Certification Report

EAL 2+ Evaluation of

RSA Adaptive Authentication System v6.0.2.1 with Service Pack 1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-96-CR
Version: 1.1
Date: 10 February 2009
Pagination: i to iii, 1 to 14

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 R2, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2. 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 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 10 February 2009, 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 at: http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked names:

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

TABLE OF CONTENTS

Executive Summary

The RSA Adaptive Authentication System Version 6.0.2.1 with Service Pack 1 (hereafter referred to as RSA Adaptive Authentication System), from RSA, The Security Division of EMC, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 *augmented* evaluation.

The RSA Adaptive Authentication System is a risk-based authentication platform that provides additional layers of security to companies with an online presence. The RSA Adaptive Authentication System uses positive device identification and risk analysis to ensure that only genuine online customers can access their accounts. The RSA Adaptive Authentication System provides additional authentication measures during login and continuous monitoring of each transaction. If a single transaction (or series of transactions) increases 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 Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 19 January 2009 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 RSA Adaptive Authentication System, 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 3.1 R2, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2. The following augmentation is claimed:

- ALC_FLR.1 – Basic flaw remediation.

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 in the field of IT Security*

[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.

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 Evaluation Assurance Level (EAL) 2 *augmented* evaluation is the RSA Adaptive Authentication System Version 6.0.2.1 with Service Pack 1 , (hereafter referred to as RSA Adaptive Authentication System), from RSA, The Security Division of EMC.

2 TOE Description

The RSA Adaptive Authentication System is a risk-based authentication platform that provides additional layers of security to companies with an online presence. The RSA Adaptive Authentication System uses positive device identification and risk analysis to ensure that only genuine online customers can access their accounts. The RSA Adaptive Authentication System provides additional authentication measures during login and continuous monitoring of each transaction. If a single transaction (or series of transactions) increases the perceived risk level, the online customer may be challenged to provide additional authentication, or the transaction can be flagged for later review. This is accomplished via the monitoring of end user transactions as they occur. End users do not directly interface with the TOE; instead requests are made by a host application on behalf of the user. Once the host application determines if the user is valid, the host application then ascertains if the user is "enrolled" in the RSA Adaptive Authentication System. If not, the user is given the opportunity to enroll at that time. The host application then collects the necessary information and passes it to the TOE. The TOE uses this information to determine a recommended action based on its stored policies. The recommendation will either be allow, challenge, review or deny.

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 the RSA Adaptive Authentication System is identified in Section 6 of the Security Target (ST).

4 Security Target

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

Title: RSA®, The Security Division of EMC, RSA Adaptive Authentication System v6.0.2.1 with Service Pack 1 Security Target
Version: 1.0
Date: 4 February 2009

5 Common Criteria Conformance

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 R2.

The RSA Adaptive Authentication System is:

a. *Common Criteria Part 2 extended*, with functional requirements based only upon 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;
   - EXT_FCR_CDA.2 – Simple attack heuristics.

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

c. *Common Criteria EAL 2 augmented*, with all the security assurance requirements in EAL 2, as well as ALC_FLR.1.

6 Security Policy

The RSA Adaptive Authentication System 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, the RSA Adaptive Authentication System 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 the RSA Adaptive Authentication System 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 the RSA Adaptive Authentication System 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 assumptions are made about the operating environment of the TOE:

- The host machine upon which RSA Adaptive Authentication System is installed resides in a controlled access facility.
- The host machine upon which RSA Adaptive Authentication System is installed is capable of supporting all of its required functionality as well as providing a valid time stamp.
- 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 System 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.

The RSA Adaptive Authentication System 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 Architectural Information

The RSA Adaptive Authentication System is composed of several parts that are primarily written in Java. This allows the same source code to operate on the different operating systems supported. The product can be distributed across several servers or deployed with all the product components installed on a single server. RSA Adaptive Authentication System supports two types of users: Back Office users who are the administrators of the product and end users who are the online customers that will be subjected to the authentication policies. The RSA Adaptive Authentication System can be divided into five major subsystems:

Core Components. The Core Components provide the fundamental functionality of transaction risk assessment, authentication processing based on risk, and transaction policies enforcement.

Back Office Applications. Administrators of the RSA Adaptive Authentication System administer the device using a set of Back Office Applications which comprise the following:

- *Access Management Tool* provides a single interface for access to the Back Office applications. It allows administrators to create Back Office users and manage roles and permissions for the different Back Office applications.

- *Admin Tool* is used to add, remove, and save elements from security risk lists such as country or Internet Protocol (IP) blacklists, watch lists, and white lists.

- *Report Viewer* allows administrators to view daily, weekly, or monthly reports created by the RSA Data Center, but does not generate the reports.

- *Customer Service Representative (CSR) Tool* is designed to help CSRs look up and modify user account information as the user interacts with the RSA Adaptive Authentication System.

- *Policy Editor* allows Back Office users to configure and customize the necessary policies by which the RSA Adaptive Authentication System detects and challenges potentially risky end users, marks transactions for review by Fraud Analysts, allows valid end users, or denies fraudulent end users.

- *Case Management Tool* is used to review any events that have been flagged as risky by the RSA Adaptive Authentication System, and requires review by a Fraud Analyst.

Adaptive Authentication Utilities. There are a number Adaptive Authentication Utilities that run in the background or provide specific configuration tools for the RSA Adaptive Authentication System. These utilities can be used by administrators to help manage the RSA Adaptive Authentication System and troubleshoot any problems. The following utilities are included in the Adaptive Authentication Utilities:

- Health Check Servlet
- Simple Mail Transfer Protocol (SMTP) and HTTP to Voice Extensible Markup Language (VXML) or Telephony
- Aggregator Token Generator
- Log Manager
- Policy Simulator
- Billing Utility
- GeoIP Admin Tool
- GeoIP Inspector Utility

- Risk Engine Offline Task Utility
- Orgs & Groups Configuration Tool

Data and Configuration Databases. The RSA Adaptive Authentication System utilizes three primary data stores: Tools Database, Case Management Database, and the Adaptive Authentication Database. The Tools Database stores the authentication credentials and privileges for the administrators that authenticate and use the Back Office Applications. The Case Management Database contains events that have been flagged as risky by the RSA Adaptive Authentication System, and requires review by a Fraud Analyst. The Adaptive Authentication Database is the primary data store for the Core Components. It contains the policy table information for the Policy Manager and the end user credentials other than user name and password, including secret questions and responses.

External Network Interfaces. The RSA Adaptive Authentication System provides a well-defined set of Application Programming Interfaces (APIs) for Web Services Description Language (WSDL) that can be used by developers that wish to integrate the RSA Adaptive Authentication System into their applications. The Web Services external interface is used by the developer's application to access the TOE's authentication services.

9 Evaluated Configuration

The RSA Adaptive Authentication System is a software TOE that requires an application server and underlying operating system to run. The RSA Adaptive Authentication System also relies on the presence of a database application to store data and configurations. For this evaluation, the RSA Adaptive Authentication System build 1831 was installed and configured on two evaluated and tested platforms. The combination of the application server, underlying operating system, and database server is as follows:

- IBM Websphere 6.1 application server operating on SUN Solaris 10 with an Oracle 10g database.

- Apache Tomcat 5.5 application server operating on Microsoft Windows 2003 Server with a Microsoft SQL Server 2005 database.

10 Documentation

The RSA Adaptive Authentication System documentation set provided to the consumer is as follows:

- Access Management User's Guide v6.0.2.1. rev 1.2, published October 30, 2007 & Doc Number CUS-029-007-ENG

- Admin Tool User's Guide v6.0.2.1. rev 1.4, published October 29, 2007 & Doc Number CUS-020-001-ENG

- Architectural Overview v6.0.2.1. rev 1.5, published October 29, 2007 & Doc Number CUS-021-010-ENG
- Best Practices for Choosing Challenge Questions v6.0.2.1. rev 1.8, published November 1, 2007 & Doc Number CUS-032-001-PDM
- Case Management User's Guide v6.0.2.1. rev 1.7, published October 30, 2007 & Doc Number CUS-029-006-ENG
- Configuration Framework User's Guide v6.0.2.1. rev 2.5, published October 25, 2007 & Doc Number CUS-022-017-ENG
- CSR Tool User's Guide v6.0.2.1. rev 1.5, published September 7, 2007 & Doc Number CUS-029-001-ENG
- Authentify ACSP Developer's Guide v6.0.2.1. rev 1.0, published November 8, 2007 & Doc Number WSI-023-009-ENG
- EFraud Network Agent Installation & Admin Guide v6.0.2.1. rev 1.2, published October 2, 2007 & Doc Number CUS-022-016-ENG[2]
- Integration Guide v6.0.2.1. rev 1.4, published October 31, 2007 & Doc Number CUS-023-005-ENG
- Operations Handbook v6.0.2.1. rev 2.5, published November 1, 2007 & Doc Number CUS-024-002-ENG
- Policy Editor User's Guide v6.0.2.1. rev 1.6, published October 30, 2007 & Doc Number CUS-029-002-FOR
- Policy Simulator User's Guide v6.0.2.1. rev 1.2, published October 30, 2007 & Doc Number CUS-029-007-ENG
- Web Service Reference Guide v6.0.2.1. rev 1.2, published October 30, 2007 & Doc Number CUS-029-007-ENG
- AdminService & ImageService Reference Guide v6.0.2.1. rev 2.2, published August 29, 2007 & Doc Number WSI-023-004-ENG

[2] Provided as part of the RSA Adaptive Authentication documentation set but not included in the evaluated configuration.

- Release Notes v6.0.2.1. rev 1.2, published November 2, 2007 & Doc Number ENG-028-026-ENG

- Reporting & Logging v6.0.2.1. rev 1.6, published October 26, 2007 & Doc Number CUS-027-008-ENG

- Report Viewer User's Guide v6.0.2.1. rev 1.5, published September 7, 2007 & Doc Number CUS-029-004-ENG

- The RSA Risk Engine Upgrade Guide v6.0.2.1. rev 1.5, published October 26, 2007 & Doc Number FOR-021-003-FOR

- Workflows & Processes v6.0.2.1. rev 1.2, published October 26, 2007 & Doc Number CUS-032-003-PDM

- Authentify ACSP Developer's Guide v6.0.2.1. rev 1.0, published November 8, 2007 & Doc Number WSI-023-009-ENG

- Back Office Tools Installation Guide v6.0.2.1. rev 2.0, published October 30, 2007 & Doc Number CUS-022-018-ENG

- Back Office Database Installation Guide v6.0.2.1. rev 2.0, published October 30, 2007 & Doc Number CUS-022-020-ENG

- Database Installation Guide v6.0.2.1. rev 1.0, published October 30, 2007 & Doc Number CUS-022-009-ENG

11 Evaluation Analysis Activities

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

Development: The evaluators analysed the RSA Adaptive Authentication System functional specification and design documentation and determined that the design completely and accurately instantiated the security functional requirements. The evaluators analyzed the RSA Adaptive Authentication System security architectural description and determined that the initialization process was secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

Guidance documents: The evaluators examined the RSA Adaptive Authentication System 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 System configuration management system and associated documentation was performed. The evaluators found that the RSA Adaptive Authentication System configuration items were clearly and uniquely marked, and could be modified and controlled. 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 the RSA Adaptive Authentication System during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by RSA for the RSA Adaptive Authentication System. 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 RSA Adaptive Authentication System robustness was validated through independent evaluator analysis and penetration testing. The evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that no potential vulnerabilities existed for the TOE in its intended environment.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessing 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[3].

RSA employs a rigorous testing process that tests the changes and fixes in each release of the RSA Adaptive Authentication System. Comprehensive regression testing is conducted for all releases.

[3] 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 evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 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 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 by following all instructions in the developer's Installation and Administrative guidance documentation.

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

c. Identification and Authentication: The objective of this test goal is to confirm that TOE administrators are identified and authenticated;

d. User Data Protection: The objective of this test goal is to verify that the end-user access control policy is enforced;

e. Case Recording and Review: The objective of this test goal is to verify that the TOE is capable of recognizing, recording, storing, and analyzing records of users committing potentially fraudulent activities; and

f. Security Management: This objective of this test goal is to verify roles and administrative access control for the various TOE subsystems.

12.3 Independent Penetration Testing

Subsequent to independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Port scanning;
- Direct attacks to verify the TOE can self-protect itself in its intended environment; and

- Forced exception behaviour of the TOE to verify that an operator of the TOE is prevented from disrupting the proper operation of the TOE through invalid use of processes or configuration parameters.

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

12.4 Conduct of Testing

The RSA Adaptive Authentication System 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 all documented.

12.5 Testing Results

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

13 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.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the RSA Adaptive Authentication System includes comprehensive installation, administration, deployment, development, user, and reference guides.

The RSA Adaptive Authentication System is a complex system to initialize and often requires the aide of an on-site RSA systems engineer to configure and integrate into a corporate network.

Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

The RSA QA facilities were used during a portion of the testing activities. RSA Support was consulted during the initialization of the product in the EWA-Canada ITSET lab.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CSR	Customer Service Representative
EAL	Evaluation Assurance Level
EFN	eFraudNetwork™
ETR	Evaluation Technical Report
GeoIP	Geographical IP
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
QA	Quality Assurance
SMTP	Simple Mail Transport Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WSDL	Web Services Description Language
VXML	Voice Extensible Markup Language

16 References

This section lists all documentation used as source material for this report:

a. CCS-Guide-004 Version 1.1, Technical Oversight for TOE Evaluation, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 R2, September 2007.

d. RSA®, The Security Division of EMC, RSA Adaptive Authentication System v6.0.2.1 with Service Pack 1 Security Target, Version 1.0, 4 February 2009.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of RSA Adaptive Authentication System Version 6.0.2.1 with Service Pack 1 , EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-96, Document No. 1589-000-D002, Version 1.4, 19 January 2009.