Certification Report

EAL 3 Evaluation of RSA® Access Manager v6.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-106-CR
Version:	1.0
Date:	16 November 2009
Pagination:	i to iii, 1 to 11

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 2,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. 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 Ltd. 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 16 November 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 (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:

- EMC ® is a registered trademark symbol of EMC Corporation;
- RSA® Access Manager is a registered trademark symbol of EMC Corporation;
- JAVA™, Solaris™ are trademarks of SUN Microsystems, Inc.;
- Microsoft®, Internet Explorer®, and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries;
- BEA Weblogic® Server and Oracle 10g® are registered trademarks of Oracle; and
- Apache™ is a trademark of The Apache Software Foundation.

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

TABLE OF CONTENTS

Executive Summary

The RSA® Access Manager v6.1 (hereafter referred to as Access Manager), from RSA, The Security Division of EMC, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

Access Manager is a web access management solution that enables user authorization and privilege management. It allows organizations to provide secure access to web applications within intranets, extranets, portals, and exchange infrastructures.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 5 November 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 Access Manager, 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 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 2.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Access Manager is conformant with the US Government Protection Profile Authorization Server For Basic Robustness Environments, July 25, 2007, Version 1.1.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Access Manager 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 RSA® Access Manager v6.1 (hereafter referred to as Access Manager), from RSA, The Security Division of EMC.

2 TOE Description

Access Manager is a web access management solution that enables user authorization and privilege management. It allows organizations to provide secure access to web applications within intranets, extranets, portals, and exchange infrastructures.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Access Manager is identified in Section 1.3 (TOE Overview) and Section 7 (TOE Summary Specification) 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® Access Manager v6.1 Security Target
Version: 0.8
Date: 5 November 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version3.1 Revision 2,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

Access Manager is:

- *Common Criteria Part 2 extended*, with security functional requirements based on functional components in Part 2 as well as the following explicitly stated requirements defined in the ST:
  - FDP_ACF_(EXT).1 – Security Attribute Based Access Control
  - FPT_TST_(EXT).1 – TSF Testing
- *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3;
- *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; and

- Access Manager is *conformant* with the US Government Protection Profile Authorization Server For Basic Robustness Environments, July 25, 2007, Version 1.1.

6 Security Policy

Access Manager implements a security attribute-based access control policy to control user access to protected systems based on user and group membership entitlements as well as smart rules.

In addition, Access Manager implements a security management policy that restricts the ability to determine or modify the security attribute-based access control. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Access Manager 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:

- TOE administrators are non-hostile, appropriately trained and follow all user guidance.

- The TOE has access to all the IT System data it needs to perform its functions.

- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

- Principals cannot gain access to resources protected by the TOE without passing through the TOE access control mechanisms.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.
- The TOE environment is appropriately scalable to provide support to the IT systems in the organization it is deployed.

7.3 Clarification of Scope

Physical/logical features and functionality not included in the TSF are:

- The requirement to use NIST FIPS 140-2 validated cryptographic modules for any cryptographic services is expressed as an objective on the operational environment.
- The TOE's underlying operating system must be maintained in a secure state.
- RSA Access Manager Agent and other 3rd party software components, see Security Target Section 1.3.2 for a complete list.

8 Architectural Information

Access Manager is a software-only TOE that is installed and deployed on general-purpose server hardware running a general-purpose operating system. To implement Access Manager, the administrator must install and configure at least one instance of each of these servers either on one platform or separately in distributed mode:

Entitlements Server: The Entitlements Server provides Administrative API clients (including the Administrative Console) with read/write access to the Access Manager data store. This allows the administrator to establish and revise the security policy. The administrator can configure the Entitlements Server to selectively update the cached data on your Authorization Servers. By doing so, changes made to the Access Manager data store, such as entitling a user to access a resource, take effect immediately.

Authorization Server: The Authorization Server performs the authentication and authorization checks for users at runtime. When a user tries to access a resource, the Authorization Server determines whether the authentication method validated the user and whether the user is allowed to access the resource. The Authorization Server reads the user and policy information directly from the data store. To improve runtime performance, the Authorization Server can be configured to cache a variety of data. When properly configured, the Authorization Server does not have to go to the data store to check access privileges for users who have already been allowed or denied access to a resource.

Dispatcher/Key Server: The Dispatcher/Key Server has two functions. The Dispatcher keeps track of all available Authorization Servers. By default, Agents are configured to query the Dispatcher at startup for available Authorization Servers. Agents then connect to the Authorization Servers that are available. The Key Server generates single sign-on (SSO) token encryption keys (or secret keys), which carry a limited lifetime. When a user authenticates to the Access Manager system, the Authorization Server issues a token, encrypted with one of these keys, that encapsulates the user's session state. The Agent returns this token to the user's browser in the form of a cookie. On subsequent requests, the token is sent back to the Authorization Server for decryption as needed.

RSA Access Manager Data Adapter: Access Manager uses the Data Abstraction Layer (DAL) to access user data in data stores, such as an LDAP directory or an SQL database. The user data store contains all information about users and their access privileges. Access Manager adds additional policy, resource, and administration data schemas to the directory server or database, which can be managed separately from the user data store. This allows the administrator to consolidate user and security policies into one central location, and makes administering enterprise security less time-consuming.

Access Manager Administrative Console: The Administrative Console is used to administer the TOE using a computer with a web browser. The Administrative Console is a web-based, Java Server Page (JSP) application is installed on any supported application server or servlet engine. From the Administrative Console, administrators can set-up administrative groups and roles, add resources, and define the security policies. The administrator can also use the Administrative Console to add and edit your users and groups, and store them in its data store.

On any Web or Application server to be protected the administrator must install an RSA Access Manager Agent[2]**.** RSA Access Manager Web Server Agents supplement the native security mechanisms of a web server. RSA Access Manager Web Server Agents run in the same process as the web server itself and are invoked whenever the web server needs to determine access rights for a particular Uniform Resource Locator (URL). RSA Access Manager Web Server Agents forward access requests to an Authorization Server, which passes the answers it receives back to the web server.

RSA Access Manager Application Server Agents supplement the native security on an application server, and extend single sign-on to a web application environment. This allows for the protection of web resources, such as servlets, Enterprise Java Beans (EJBs), and Java Server Pages (JSPs) with Access Manager.

9 Evaluated Configuration

The evaluated configuration for Access Manager comprises the Entitlement Server, Authorization Server, Dispatcher/Key Server, a Data Adapter, and the Administrative Console. The server(s) hardware, operating systems, and Web/Application Server Agent are not included in the evaluated configuration of the TOE, and are not provided as part of the product delivery.

[2] The Agent software was not evaluated and is not included within the TOE boundary.

Each of the components is modular, and can be installed on a server by itself, or can be installed together with other components on the same server. RSA Access Manager v6.1 supports the following 3rd party software and server operating system (OS) types:

- Microsoft Windows Server 2003 R2 SP2 (64 bit) x86
- SUN Solaris 10
- BEA Weblogic Server 10
- Oracle 10g Release 2 (10.2)
- iPlanet 6.3 (LDAP)
- Internet Explorer 6 Web Browser
- IIS Web Agent 4.8 on Windows
- Apache 2.2.4 Agent on SUN Solaris 10

10 Documentation

The RSA Access Manager documents provided to the consumer are as follows:

- RSA Access Manager 6.1 Administrator’s Guide, v6.1, August 2009;
- RSA Access Manager 6.1 Getting Started, v6.1, August 2009;
- RSA Access Manager 6.1 Planning Guide, v6.1, August 2009;
- RSA Access Manager 6.1 Servers Installation and Configuration Guide, v6.1, August 2009;
- RSA Access Manager 6.1 Common Criteria Installation and Configuration Guide, v1.0, August 2009;
- RSA Access Manager 6.1 Upgrade Guide, August 2009;
- RSA Access Manager 6.1 Release Notes, v6.1, 14 August 2009.

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the Access Manager 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 Access Manager security architectural description and determined that the initialization process was 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 were correct.

Guidance Documents: The evaluators examined the Access Manager 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 Access Manager configuration management system and associated documentation was performed. The evaluators found that the Access Manager 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 Access Manager 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 Access Manager during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by RSA for Access Manager. During the 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 Access Manager. 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 Access Manager in its operational environment.

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

12 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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[3].

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.

The evaluators selected a sample of the developer test cases and repeated them during a site visit to the developer’s QA facility using their lab resources. All test cases were easily duplicated with consistent results, thus gaining assurance in the developer testing method and practices.

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 Ltd. test goals:

[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.

- 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;

- Independent Evaluator Testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing.

12.3 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:

- Reconnaissance:
    - Port scanning for service exploration and identification.
    - Search of public domain information sources for TOE vulnerabilities.
- Bypassing:
    - Exercising access control mechanisms through user privilege and group membership.
- Misuse:
    - Preventing the unintentional disruption of proper TOE operation by the operator through invalid use of processes or configuration parameters.
    - Password policy enforcement.
- Monitoring:
    - Data protection in the intended operating environment of the TOE.

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

12.4 Conduct of Testing

Access Manager 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.

12.5 Testing Results

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

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The Access Manager documentation set includes comprehensive installation, administration, deployment, development, user, and reference guides. The developer also provides a complete solution with on-site system engineer to help the customer integrate the TOE into a corporate network. 24/7 support is also an available option.

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
DAL	Data Abstraction Layer
EAL	Evaluation Assurance Level
EJB	Enterprise Java Beans
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
JSP	Java Server Pages
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SSO	Single sign-on
SQL	Structured Query Language

Acronym/Abbreviation/ Initialization	Description
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
URL	Universal Resource Locator

16 References

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

- CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

- CC version e.g. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

- CEM version e.g. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

- US Government Protection Profile Authorization Server For Basic Robustness Environments, Version 1.1, July 25, 2007.

- RSA, The Security Division of EMC RSA® Access Manager v6.1 Security Target, 0.8, 5 November 2009

- Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of RSA, The Security Division of EMC RSA® Access Manager v6.1, Doc# 1606-000-D002, Version 1.0, 5 November 2009.