National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

RSA Certificate Manager Version 6.7

Report Number: **CCEVS-VR-06-0055**
Dated: **11 December 2006**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Ron Bottomly
Shaun Gilmore
Common Criteria Evaluation and Validation Scheme

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table Of Contents

1 Executive Summary

The evaluation of the RSA Certificate Manager Version 6.7 commenced on 11-01-06 and was completed on 11-12-06. The RSA Certificate Manager Version 6.7 evaluation was performed by Science Applications International Corporation (SAIC) in the United States. The evaluation was conducted in accordance with the requirements drawn from the Common Criteria CCv2.3, Part 2, and Part 3 Evaluation Assurance Level (EAL4+) requirements. However, given that an earlier version of the product (RSA Keon CA System Version 6.5) was previously evaluated, this evaluation was largely conducted through analysis of changes in order to substantiate the continued validity of many of the previous evaluation findings.

The RSA Certificate Manager product identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the RSA Certificate Manager Version 6.7. The evaluation has been conducted in accordance with the provision of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. This Validation Report is not an endorsement of the RSA Certificate Manager Version 6.7 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

Science Applications International Corporation (SAIC) is certified by the NIAP validation body for laboratory accreditation. The CCTL has presented CEM work units and rationale that are consistent with the CC [Common Criteria], the CEM [Common Evaluation Methodology] and CCEVS publication number 4 Guidance to CCEVS Approved Common Criteria Testing Laboratories. The CCTL evaluation team concluded the requirements from Common Criteria CCv2.1, Part 2 and Part 3 Evaluation Assurance Level (EAL4) requirements have been met.

1.1 Evaluation Details

Dates of Evaluation: 11-01-06 to 11-12-06
Evaluated Product: RSA Certificate Manager Version 6.7
Developer: RSA Security, Inc.
CCTL: SAIC Inc. Columbia, MD
Validation Team: Ron Bottomly, Shaun Gilmore
Evaluation Class: EAL4 augmented with ALC_FLR.2
PP Conformance: Certificate Issuing and Management Components (CIMC) Protection Profile Version 1.0 (Security Level 3) 31 October 2001

1.2 Interpretations

Version 2.3 of the CC has no international interpretations and all NIAP interpretations affecting this evaluation have been included based on their application during the previous evaluation. The applicable NIAP interpretations are as follows:

NIAP Interpretations	
I-0407	Empty Selections Or Assignments
I-0409	Other Properties In FMT_MSA.3 Should Be Specified By Assignment
I-0410	Auditing of Subject Identity For Unsuccessful Logins
I-0415	User Attributes To Be Bound Should Be Specified
I-0416	Association of Access Control Attributes With Subjects and Objects
I-0418	Evaluation of The TOE Summary Specification: Part 1 Vs Part 3
I-0422	Clarification Of "Audit Records"
I-0423	Some Modifications To The Audit Trail Are Authorized
I-0425	Settable Failure Limits Are Permitted
I-0426	Content Of PP Claims Rationale
I-0427	Identification of Standards
I-0429	Selecting One Or More

1.3 Threats to Security

Name (T = Threat)	**Threat**
T.Administrative errors of omission	Administrators, Operators, Officers or Auditors fail to perform some function essential to security.
T.Administrators, Operators, Officers and Auditors commit errors or hostile actions	An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.
T.Critical system component fails	Failure of one or more system components results in the loss of system critical functionality.
T.Disclosure of private and secret keys	A private or secret key is improperly disclosed.
T.Flawed code	A system or applications developer delivers code that does not perform according to specifications or contains security flaws.
T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access

	control causing potential violations of integrity, confidentiality, or availability.
T.Hacker physical access	A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.
T.Malicious code exploitation	An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.
T.Message content modification	A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.
T.Modification of private/secret keys	A secret/private key is modified.
T.Sender denies sending information	The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.
T.User abuses authorization to collect and/or send data	User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.
T.User error makes data inaccessible	User accidentally deletes user data rendering user data inaccessible.

2. Identification

ST – RSA Certificate Manager V6.7 Security Target Version 1.7, 07 December 2006
TOE Identification – RSA Certificate Manager Version 6.7 (build 411)
CC Conformance – Common Criteria for Information Technology Security Evaluation, Version 2.3, Part 2 – August 2005, CC Version 2.3 Part 2 – extended, Common Criteria for Information Technology Security Evaluation, Version 2.3, Part 3 – August 2005, CC Version 2.3 Part 3 – augmented.
PP Conformance – Certificate Issuing and Management Components (CIMC) Protection Profile Version 1.0(Security Level 3) October 31, 2001.
Assurance Level - Evaluation Assurance Level 4 augmented with ALC_FLR.2 as required by CIMC PP SL3
Keywords – Public Key Infrastructure, PKI, Certificate Issuing and Management Component, CIMC. Certificate Authority, CA.

2.1 IT Security Environment

The CIMC PP levies requirements on the TOE as well as the IT Environment. In the case of this TOE the IT Environment is the Operating System on which the software is running. The TOE relies on configuration files and audit capabilities which are protected by the Operating System (IT Environment). The IT Environment provides an interface to configuration files used to control and configure the TOE's functionality. The IT Environment provides TLS facilities leveraged by the TOE to secure the communications between internal and external components of the TOE. The IT Environment defines three roles to control access to the system: Administrator, Officer (or Vettor), and Auditor.

2.2 Operating System

The TSP is enforced by the TOE, and the Security Functional Requirements (SFRs) are completely satisfied by TOE functions (with the exception of those with environmental dependencies). The Certificate Manager runs on Sun Solaris 9. The operating system which the TOE interfaces, is assumed to be trusted, meaning it can be relied upon to correctly execute the TOE functions. Sun Solaris 9 has received Common Criteria EAL4 validation.

2.3 Hardware Security Module

A hardware security module, HSM, is part of the TOE IT Environment. The Certificate Manager relies on an HSM to provide all FIPS 140-1 or 140-2 approved cryptography and key management; during the evaluation nCipher HSMs were used. The HSM is accessed via libraries installed in the physical machine on which the Certificate Manager is installed. There are two FIPS certified nCipher HSM products identified in the Security Target – the nShield and the netHSM. Both offer the same interface and functions to the Certificate Manager via the libraries installed on Solaris. The nShield was included in the original evaluation and this evaluation added the netHSM. It should be noted that the evaluation team tested only with the netHSM product given that it is a supporting component in the environment and the nShield was demonstrated to provide the necessary support to the Certificate Manager during the original evaluation. Many of the TOE components rely on the HSM to provide all the security-relevant cryptographic services necessary for the TOE to perform its functions.

2.4 Hardware Platform

The Certificate Manager software for Sun Solaris 9 requires the following minimum system requirements:

- Sun Enterprise Ultra 10S or greater
- At least 300 MB of memory (RAM)
- Minimum free hard disk space of at least 100 MB free for basic program installation. Additional space would be needed for the storage of certificates.

3. Security Policy

3.1 Secure Audit Log Server

The TOE collects data for internal user actions, provided the ability to review audit log, and restricts access to the audit logs. The TOE tracks any actions taken to a certificate (creation, revocation, deletion), authentication attempts, changes to user's roles and access.

3.2 Access Control

The TOE enforces user roles and access control whenever users access TOE-provided functions. To enforce its security policy, the TOE relies on the roles set per user and the access control list set per function. Both roles and access control lists are set by the Administrator. Access Control is primarily enforced by restricting the options presented to users on the Web management interface. The user's certificate is verified during the initial establishment of the TLS connection to the Web server from a browser. Access to TOE resources are controlled by the access control list (ACL) for each directory structure and Web page.

3.3 Backup and Recovery

The TOE provides configurable backup functionality, as well as system recovery features, to allow the operators to restore the CA System and maintain the storage of logs and current certificates stored.

3.4 Secure Import/Export

The TOE is responsible for importing and exporting certificates, public keys, and other data. The TOE protects these data transfers through a trusted path using the TLS protocol.

3.5 Cryptographic Support and Key Management

The TOE provides access to the hardware security module (HSM). The TOE relies on the HSM in the IT Environment for key generation, signing and encryption, and key destruction through zeroization. The HSM, the nCipher nShield or netHSM – is a FIPS 140-1 or 140-2 (respectively) validated module as mandated by the CIMC PP requirements. No private or secret keys are stored in the TOE; the TOE accesses the HSM to perform operations with the keys stored on the HSM.

3.6 Certificate Management

The TOE manages and securely stores all certificates that have been signed using the private key of any of the internal CAs. The TOE provides for functionality to issue, suspend, reinstate, reissue, renew, revoke and delete certificates, and generate CRLs. All these certificate services are provided in a secure manner, protecting the integrity of the certificate administrative data. Additionally, the TOE enforces proof of origin and verification of origin of certificate status information at all times.

3.7 Identification and Authentication

The TOE requires identification and authentication before performing any security-relevant functions. The TOE maintains a secure database of authorized operators of the TOE, including

all certificate information and roles that can be assumed. Users of the TOE are authenticated during the establishment of the mutually authenticated TLS connection.

4. Assumptions

4.1 Personnel Assumptions

A.Auditors Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Auditors.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)
A.Competent Administrators, Operators, Officers and Auditors	Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
A.Cooperative Users	Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.
A.CPS	All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility)
A.Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity.
A.Notify Authorities of Security Issues	Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data
A.Social Engineering Training	General Users, administrators, operators, officers and auditors are trained to techniques to thwart social engineering attacks.

4.2 Physical Assumptions

A.Communication Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

4.2 Logical Assumptions

A.Operating System	The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the appropriate security level identified in this family of PPs.

5. Architectural Information

The TOE boundary includes multiple components that make up the RSA Certificate Manager and are relied on for the correct enforcement of the TSP. As the TOE is not a hardware product the physical boundary is not easily represented. The boundary of the TOE should be drawn to encompass all RSA-provided Certificate Manager Software, the configuration files associated with the Certificate Manager component of the TOE, the audit files that are created by the Certificate Manager component, the Log Server executable, and Command Line Tool executables. At the perimeter of the TOE Boundary are sub-components of the TOE that interact with non-TOE components. The Web Front End User Interface via web browser provides the user of the system access to configure and operate the TOE. Additionally the Web Front End interacts with the HSM for cryptographic services provided by the HSM. The Log Server, the PKI Server, and the Command Line Tools also interact with the HSM for cryptographic services provided by the HSM. Additionally, as all these programs are running on an Operating System, at a detailed level all software programs in the TOE are interfacing with the Operating System for low level calls.

6. Test Documentation

The test documentation includes a top-level test plan (RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation against the CIMC PP Test Plan) and a series of test procedures documents:

- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Certificate Management

- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Management of Security Functions Behavior
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Import and export of data
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Certificate Status Export
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Certificate Revocation List
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Backup and Recovery
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Access Control
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Identification & Authentication
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Key Management
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Protected Audit Trail Storage
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Prevention of Audit Data Loss
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Reliable Time Stamps And Audit Log Signing Event
- RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Audit Data Generation

7. IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL4 evaluation, augmented with ALC_FLR.2.

7.1 Developer Testing

RSA's approach to testing is security function oriented. A set of test procedures has been developed, each of which corresponds to a single security function – though some security functions are addressed by multiple test procedures. Each test procedure is subdivided into test scenarios and/or test cases that target specific security behavior associated with a security function.

The test procedures are designed to be exercised manually, using the web client interfaces and command line interfaces of the TOE as well as the command-line interfaces of the IT environment and the use of some custom testing tools designed for use both on the client

machines and the hosting Solaris operating system. The test procedures are documented with some additional columns for note taking and recording results – to produce a log of the actual testing results.

7.2 Evaluation Team Independent and Penetration Testing

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

8. Evaluated Configuration

The evaluation team executed the entire set of vendor test procedures on a RSA Certificate Manager configured per the evaluated configuration. The following figure served as the model used by the evaluation team during testing. However, the evaluation team utilized a single set of hardware and instantiated multiple Certificate Manager instances within that hardware using different ports to differentiate the instances.

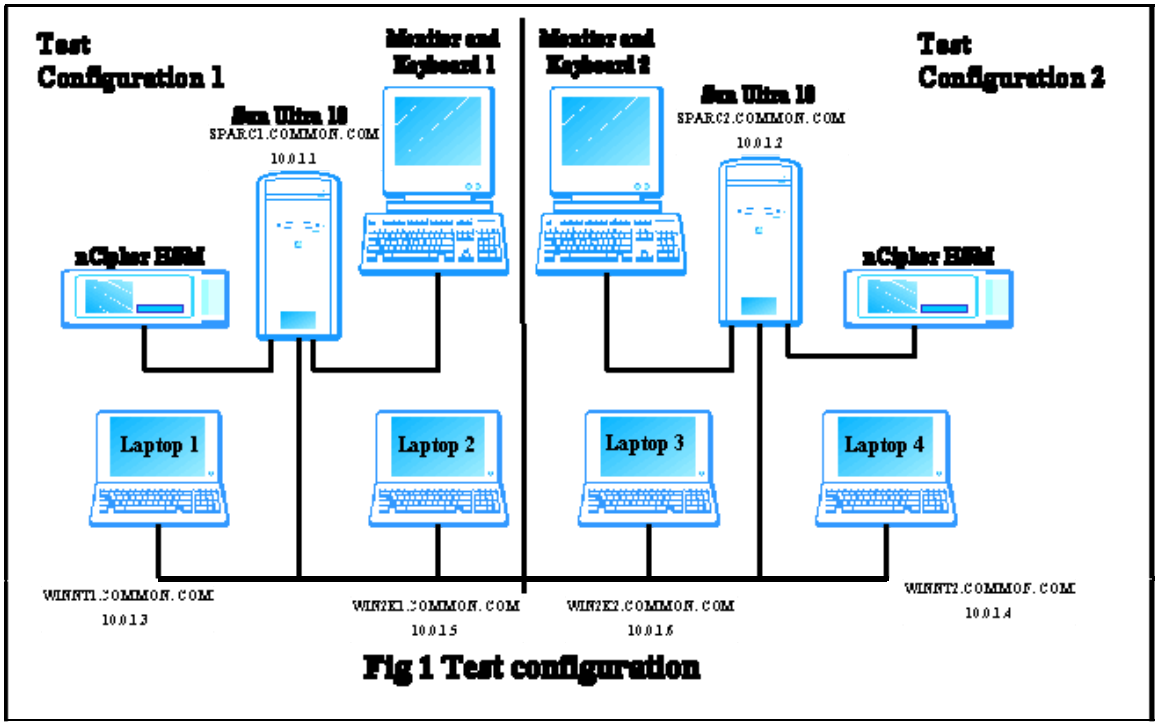

Fig 1 Test configuration

8.1 Evaluated Hardware

Regardless of the figure above, the following Hardware is used to create the test configurations:

- Sun Ultra 60 system
- 1 Intel-based workstation
- 1 Intel-based laptop
- 1 10/100 network switch
- 1 nCipher netHSM unit with FIPS 140-2 level 3 capabilities
    - As noted earlier, though the Security Target identifies both nSHield and netHSM as suitable HSMs, testing was conducted only using the netHSM. The nSHield was tested during the original evaluation and since it is in the IT environment and appears to be accessed using the same interface in the Solaris operating system the nSHield was not specifically tested during this re-evaluation effort.
- nCipher smart cards
- 1 DNS server (provided from the SAIC lab)
- 1 SMTP server (provided from the SAIC lab)

8.2 Evaluated Software

The following Software is required to be installed on the machines used for the test:

- Sun Ultra 60 system:
    - Solaris 9 (or 2.9) Operating System
    - nCipher netHSM Software Version 10.02 for Solaris
    - RSA Certificate Manager V6.7
- Laptop
    - Windows XP SP2
    - Microsoft Internet Explorer 7 with JavaScript enabled
- Workstation
    - Windows XP SP2
    - Microsoft Internet Explorer 6 with JavaScript enabled

9. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4, assurance component, augmented with ALC_FLR.2. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the

Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.
>
> A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 ([1], [2], and [3]) and CEM version 2.3 ([4]). The Evaluation Team determined the RSA Certificate Manager TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for the RSA Certificate Manager V6.7 Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> Section 6.1: Each verdict for each CEM work unit in the ASE ETR is a "Pass" therefore, the RSA Certificate Manager Version 6.7 Security Target, Version 1.7, 07 December 2006 is a CC compliant ST.
>
> Section 6.2: The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "Pass". Therefore, when configured according to the following guidance Documentation:
>
> - RSA Certificate Manager 6.7 Installation Guide, First printing: October 2006
> - RSA Certificate Manager v6.7 Delivery and Operation Installation, Generation and Start-Up Release Notes, Version 1.8, November 16 ,2006 (and associated references)
> - RSA Certificate Manager 6.7 Administrator's Guide
> - RSA Certificate Manager 6.7 Vettor's Guide
> - RSA Certificate Manager version 6.7 Guidance Documents Administrator's Guide Release Notes, 1.1
>
> The Certificate Manager Version 6.7 TOE satisfies the RSA Certificate Manager version 6.7 Security Target, Version 1.6, 16 November 2006.

10. Validation Comments/Recommendations

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The Validation Team, therefore, concludes that the evaluation and Pass result for the TOE identified below is complete and correct:

RSA Certificate Manager Version 6.7 (build 411)

Note that the validators have the following comments about the evaluation effort that, while accepted in this case, should be addressed in any subsequent evaluation efforts:

1. Residual audit bugs – During the course of evaluation it was discovered that when audit events are recorded as a result of failed attempts to Update a CA (UpdateCA event) or to automatically e-mail a certificate expiry notification (CertExpiryNotice event) the specific internal return code recorded in the audit event is incorrect. While these operations cannot fail for a security-relevant reason (e.g., access denied) due to the product design, the incorrect information could be misleading to an expert user of the product. Note that other than the specific return code, the events properly reflect the event, its more general success or failure, the responsible user, the time/date, etc.
2. Analysis in lieu of testing – Given some level of difficulty involved in developing test procedures for audit events resulting from failed operations, the developer and evaluators analyzed the applicable source code to analytically determine that the correct audit events would be generated. While it may be the case that some of the failure cases could not be practically generated without modifying the product, there should be test cases for every case where it is possible. Given that this analysis identified the residual audit bugs indicated above and also actual testing revealed other related bugs that have been fixed, it is especially important that the test procedures become more comprehensive to mitigate the occurrence of such bugs in the future.

11. Glossary

See the Glossary of definitions already defined by the ST, CC or CEM.

12. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, August 2005, Version 2.3.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, August 2005, Version 2.3.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, August 2005, Version 2.3.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, August 2005, Version 2.3.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

[Security Target] RSA Certificate Manager Version 6.7 Security Target, version 1.7, 07 December 2006.

[ETR] Evaluation Technical Report For the RSA Certificate Manager Version 6.7 Part 1 (Non-Proprietary) Version 0.1, November 19, 2002.