ASSURANCE CONTINUITY MAINTENANCE REPORT FOR RSA Certificate Manager Version 6.7 Build 417CC

Maintenance Report Number: CCEVS-VR-06-0055a

Date of Activity: 02/11/2008

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004

Impact Analysis Report,"RSA Certificate Manager Version 6.7 Impact Analysis Report", Version 1.2, November 28, 2007

Documentation Updated:

RSA Certificate Manager Version 6.7 Security Target, Version 1.7, December 7, 2006 (Build 411) – *updated to – RSA Certificate Manager Version 6.7 Security Target*, Version 1.8, November 15, 2007 (Build 417CC)

RSA Certificate Manager 6.7 Security Functional Specification for Common Criteria Evaluation Against the CIMC PP at Security Level 3, Version 1.6, November 15, 2007

RSA Certificate Manager version 6.7 Vulnerability Assessment: Vulnerability Analysis, Strength of TOE Security Function, Misuse, Version 1.6, October 23, 2007

RSA Certificate Manager v6.7 Delivery and Operation: Installation, Generation and Start-Up Release Notes, Version 1.10, October 23, 2007

RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Test Plan, Version 1.7, October 10, 2007

RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Certificate Management, Version 1.2, October 29, 2007

RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Access Control, Version 1.1, October 8, 2007

RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Key Management, Version 1.1, October 11, 2007

Readme: RSA Certificate Manager 6.7 build 417, April 27 2007

Assurance Continuity Maintenance Report:

The vendor for the RSA Certificate Manager Version 6.7 (Build 417CC) product submitted an Impact Analysis Report (IAR) to CCEVS for approval on 25 January 2008. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Changes to TOE:

This maintenance activity consists of changes to both the previous evaluated TOE and the previous evaluated TOE environment. The Impact Assessment Report provides details on the changes; the following is a summary of the changes. Note that all changes are summarized in the "Readme" file delivered with the product.

Product Changes

Security Relevant Changes

Bugfixes:

- Correction of the wildcard capability in Web ACLs to agree with normal Unix regular expression behavior.
- Correction of the behavior when selected special character were used in a certificate request through the Enrollment User Interface.

Enhancements:

- Permit certificate replacement is selected cases where the distinguished names differ in order, as long as they contain the same public key.
- Permit certificate enrollment and client enrollment and renewal for end-users with MSIEv7 and Windows Vista.
- Permit certificate enrollment and client enrollment and renewal for end-users with Firefox 2.
- Permit certificate enrollment and client enrollment and renewal for end-users with Mozilla on Solaris 10.

Non-Security Relevant Changes

Bugfixes:

- Correction of a number of behaviors regarded to the ability to use selected special non-alphabetic characters.
- Correction of the behavior regarding the expiration date for cross-certificates (a security capability not covered by the evaluation)

- Correction of cryptographic operation behavior when using certain non-evaluated hardware security modules.
- Correction of a functional anomaly regarding deletion of non-mandatory attributes in the External Publishing UI.
- Correction of the behavior of a HealthCare attribute not used in the evaluated configuration.
- Correction of the functional behavior of a particular extension in a PKCS#10 certificate request that generated an error message.
- Correction of the search pattern evaluation behavior when using an external LDAP directory server; such servers cannot be invoked in the CC configuration.
- Correction of a bug in the One-Step CGI, which although part of the product, cannot be used in the evaluated configuration.
- Correction of LDAP filter behavior when used with particular operators in custom (non-CC) templates.
- Correction of an anomalous behavior in the upgrade process from 6.5.1 to 6.7.
- Correction of a problem in creating certificates based on certain PKCS#10 requests through the C-language RCM API; this problem did not affect RCM when operated in a CC-evaluation compliant mode.
- Correction of some cross-site scripting vulnerabilities related to special characters.
- Correction of the Vettor UI for the Firefox 2.0 browser.

Enhancements:

- Enhancement of the operation of RCM with the OneStep plugin and the RSA Key-Recovery Module, neither of which are usable in the CC configuration.
- Product optimizations for very large certificate databases used with the LDAP plugin with Oracle Internet Directory (OID) server.
- Provide mechanism for periodic email notification of soon-to-expire certificates in the database.
- Enhancement of the UI to display the length of the public-key modulus in a certificate request, when the request is being vetted.

Supporting Platform, Database, and Web Browser Changes

- Permit end-user use of MSIEv7 and Windows Vista.
- Permit end-user use of Firefox 2.
- Permit end-user use of Mozilla on Solaris 10.

The Impact Assessment Report also indicates that corresponding updates have been made to the appropriate assurance evidence, including the test matrices. This appears to indicate that sufficient testing has been performed to ensure the TOE is invoked as in previous versions.

Conclusion:

The changes to the TOE and TOE environment, as described in the Impact Assessment Report, were analyzed and found to have no effect on the security of the evaluated TOE. The non-security

relevance of the set of changes (with respect to the TOE's SFRs) leads to the conclusion that the updates included in the transition of RSA Certificate Manager version 6.7 from Build 411 to Build 417CC can be classified as a **minor change** and that certificate maintenance is the correct path to continuity of assurance.

Note that the ST indicates that the TOE excludes a number of security relevant features. It is important to note that these excluded security-relevant features **are not covered** by this maintenance action. Any additional security relevant features in the product will be required to be covered by the TOE's Security Functions at the next major change (sooner if CCEVS policy changes) based on CCEVS Policies 10 and 13 (and their addenda).