National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Red Hat, Inc., 1801 Varsity Drive, Raleigh, North Carolina 27606

Red Hat Certificate System 8.1

Report Number: **CCEVS-VR-10359-2012**
Dated: **March 8, 2012**
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

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Red Hat Certificate System 8.1 (RHCS 8.1) provided by Red Hat, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in February 2012. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

RHCS 8.1 is a certificate issuing and management system offering the following general services to users and/or administrators:

- Certificate Enrollment,
- Certificate Renewal,
- Certificate Revocation,
- Certificate Retrieval,
- Certification and Certificate Revocation List (CRL) Management,
- Key Archival and Retrieval Service,
- Token Management System, and
- Online Certificate Status Protocol (OCSP) Responder Service.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions 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 provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional

requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Red Hat Certificate System 8.1 Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Red Hat Certificate System 8.1
Protection Profile	Certificate Issuing and Management Components (CIMC) In Basic Robustness Environments Protection Profile (PP), Version 1.0, April 27, 2009

Item	Identifier
ST:	Red Hat Certificate System 8.1 Security Target, Version 1.0, February 15, 2012
Evaluation Technical Report	Evaluation Technical Report For the Red Hat Certificate System 8.1 (Proprietary), Version 2.0, January 27, 2012
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Red Hat, Inc
Developer	Red Hat, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Architecture

The RHCS 8.1 TOE is an operating system application written in Java, C++, C, and Perl using associated network (Network Security Services; NSS) and java (Java Security Services; JSS) security service libraries. The RHCS 8.1 TOE is designed to integrate with a directory server such as Red Hat Directory Server to provide an internal data store and a HTTP engine (Tomcat or Apache, depending on the TOE component) to provide a network interface. The underlying JSS and NSS are designed to support the use of hardware devices that perform standards-oriented cryptographic operations. All of the components represent a RHCS 8.1 system. A RHCS 8.1 system is designed to be hosted within a RHEL 5.6+, with Security-Enhanced Linux (SELinux) policies specifically designed to protect the subsystems of the TOE, and to be connected to networks, including the Internet, and to offer these services using standard HTTP/SSL protocols.

A RHCS 8.1 system is composed of the following key components (the first of which is the TOE and the others are key supporting components in the TOE's environment):

- Certificate System (CS)

  The CS includes five configurable subsystems that work together to manage enterprise PKI deployments, including:

  - Certificate Authority (CA) - the subsystem that provides certificate management functionality for issuing, renewing, revoking, and publishing certificates and creating and publishing Certificate Revocation Lists (CRLs).
  - Data Recovery Manager (DRM) - an optional subsystem that provides private encryption key storage and retrieval. Also, in a

Token Management System setup, generates key pairs for the clients when server-side key generation option is turned on.

- Online Certificate Status Protocol (OCSP) Manager - an optional subsystem that provides OCSP responder services, based on stored CA's CRLs to distribute the load for certificate status verification.
- Token Key Service (TKS) - manages one or more master keys required to set up secure channels from the tokens directly to the token processing system. The secure channels provided by TKS allows Global Platform compliant smart cards (tokens) to be identified with high level of confidence and subsequently communicate securely with the RHCS servers for operations such as certificate enrollments, renewals, server-side key generation requests, key archival and recovery, etc.
- Token Processing System (TPS) - one unique function of the TPS is to provide communication between Global Platform-compliant smart cards and the RHCS systems by means of *APDU* (Application Protocol Data Unit). It provides the registration authority functionality in the token management infrastructure and with the assistance of the TKS, establishes secure channels between the smart cards and the back-end subsystems.

The CS subsystems (CA, DRM, OCSP Manager, TKS, and TPS) are highly integrated with each other depending on the deployment scenario. OCSP and CA instances work together on CRL publishing and certificate verification. CA and DRM instances work together for key recovery and archival. Smart card tokens, processed through the Enterprise Security Client (ESC) user interface, are managed by the TPS. The TPS, however, is designed to work with at least two essential subsystem instances, a TKS to manage shared secrets between the tokens and TMS and a CA to process certificate enrollment operations. A TPS can also be configured to use a DRM for server-side key generation and key archival and recovery, with the assistance of TKS to deliver private keys securely to the tokens (smart cards).

The CA, DRM, OCSP Manager, and TKS are implemented in Java, utilize a Tomcat HTTP engine (see below), and share a common framework (also written in Java) for management, logging, authentication, access control, self tests, and notifications. The TPS is written as a native RHEL 5.6+ C++ application and utilizes an Apache HTTP engine.

- HTTP Engines (Tomcat (*for CA, DRM, OCSP Manager, and TKS*) & Apache (*for TPS*))

The web engine provides the HTML-based UI (presentation) and HTTP-based protocol handling. It does not perform authentication and authorization other than providing and/or enforcing SSL. It performs basic

certificate validation and delegates all the application-specific authentication and authorization to CS via a callback mechanism.

- Internal Database (Red Hat Directory Server - RHDS 8.1)

  The internal database stores information such as certificates, requests, officer/administrator information, and other information such as access control information. The CS communicates with the internal database securely through SSL client authentication.

The following architectural diagrams show the interactions between various CS configurations and various internal and external systems. Internally, the CS communicates with an internal database where certificate records, request records, system user records are stored. The CS also accesses the cryptographic operations (directly or indirectly) via NSS. Externally, the HTTP engine manages the presentation-level interaction between the CS and users including end-users, security officers, and administrators. The CS may optionally publish certificates to a corporate directory server.

In addition to the HTTP Engine and Internal Database, the CS also relies on access to processing capabilities, file storage, as well as hardware cryptographic modules provided by its IT environment.

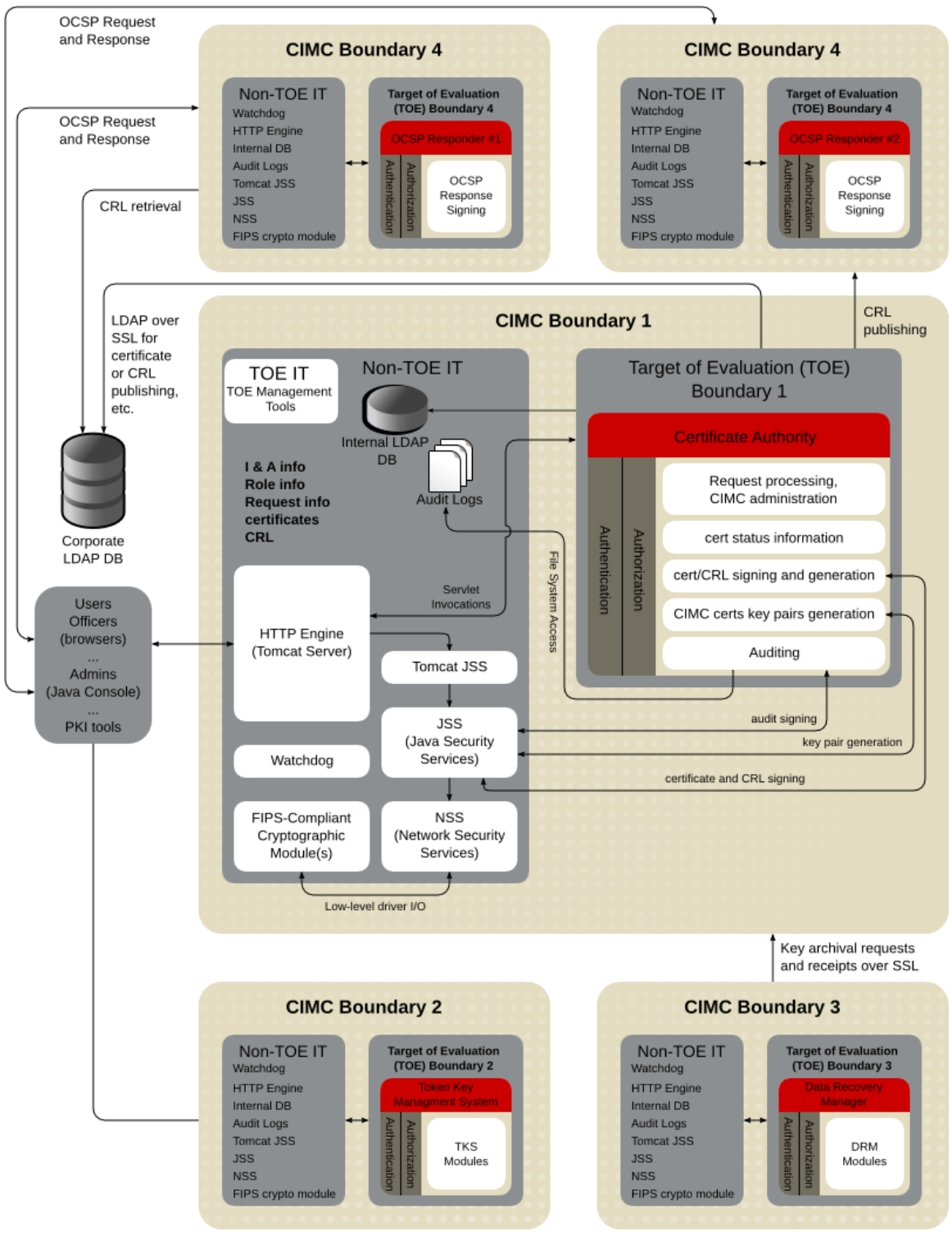

Figure 1 RHCS 8.1 System Overview

The Non-TOE IT environments are similar among all CIMC boundaries. Please refer to CIMC Boundary 1 in Figure 1 and Figure 2 to see complete details for all other Non-TOE IT within other CIMC boundaries. Figure 2 shows the TPS component and its connections to the other RHCS 8.1 components.

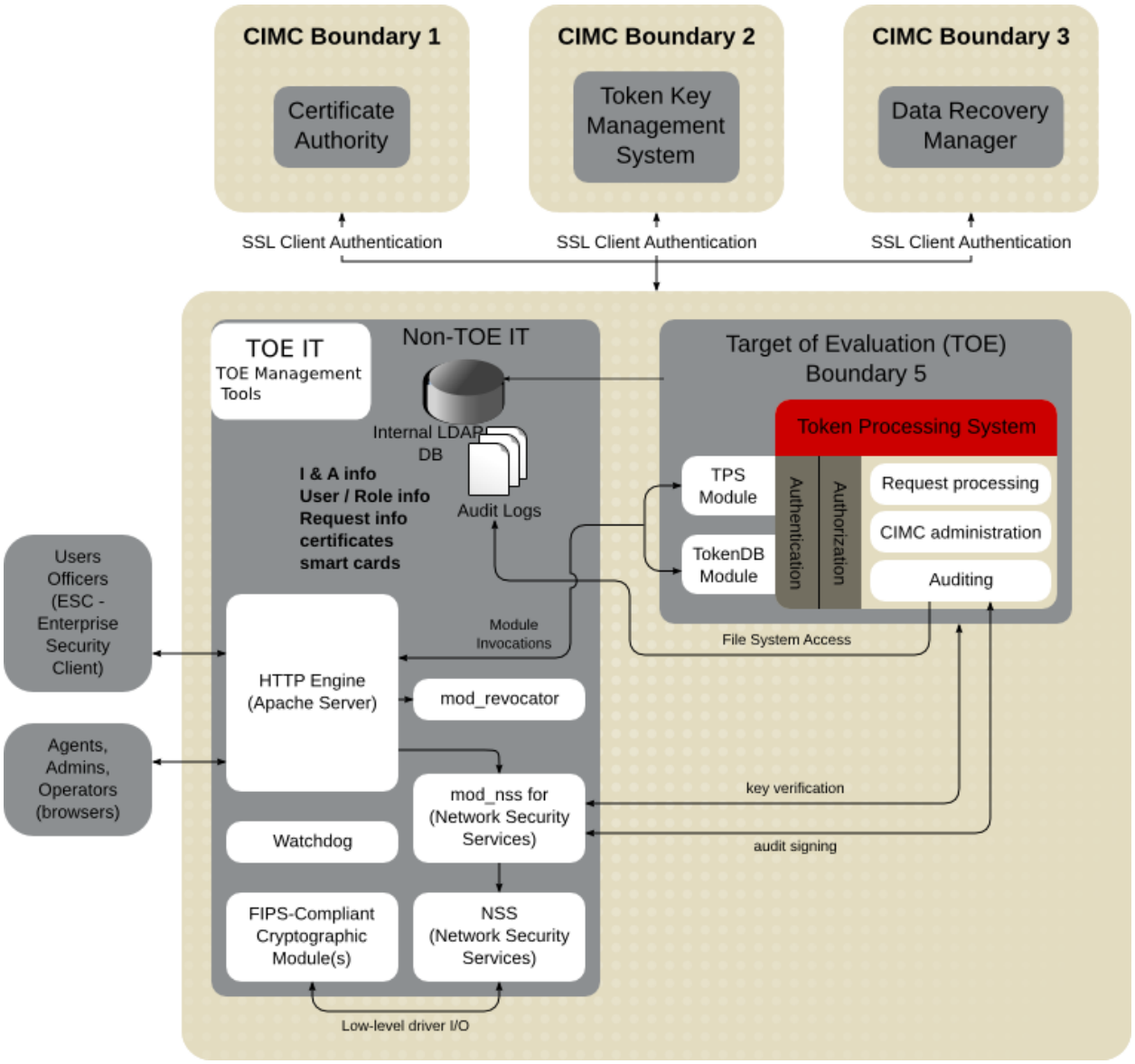

Figure 2 Token Management System

While a complete RHCS 8.1 *system* includes all of the components within the CIMC boundaries indicated in Figure 1 and Figure 2, the RHCS 8.1 *TOE* includes the components within the labeled TOE Boundaries. Specifically, the TOE consists of the CA, OCSP Manager, DRM, TKS, and TPS subsystems (some of which are optional depending on the

PKI application). The RHCS 8.1 TOE includes a Java GUI-based administration tool called the 'Console' that is used for administrative tasks such as managing users and maintaining the (CA, OCSP Manager, DRM, and TKS) subsystems and performing daily operational and managerial duties for those subsystems. Additionally, the RHCS 8.1 TOE includes a number of command-line utilities (see the Red Hat Certificate System 8.1 Command-Line Tools Guide for a complete list and more information), for example:

- The AuditVerify tool is used to verify that signed audit logs were signed with the private signing key and that the audit logs have not been compromised. Auditors can verify the authenticity of signed audit logs using the AuditVerify tool. This tool uses the public key of the signed audit log signing certificate to verify the digital signatures embedded in a signed audit log file. The tool response indicates either that the signed audit log was successfully verified or that the signed audit log was not successfully verified. An unsuccessful verification warns the auditor that the signature failed to verify, indicating the log file may have been tampered with (compromised).
- The PIN Generator generates unique PINs for end-entity entries in an LDAP directory. The tool stores these PINs as hashed values in the same directory against the corresponding user entries. It also copies the PINs to a text file so that the PINs can be sent to the end entities.
- The TKS utility manages keys, including keys stored on tokens, the TKS master key, and related keys and databases. It offers the following functions: deleting a key from a token; inputting shares to generate a new transport key; displaying the key check value (KCV) of the specified key; listing a specified key or all keys; generating a new master key; creating a new key database; changing the key database password; renaming a symmetric key; listing all security modules; generating a new transport key; unwrapping a wrapped master key; and wrapping a new master key.
- The CMC Request, Enrollment, Responses, and Revocation utilities to create CMC requests request from PKCS #10 or CRMF requests; to sign a certificate request with an agent's certificate; parse CMC responses received by the utility; and sign a revocation request with an agent's certificate, respectively.
- The CRMF Pop Request utility is a tool to send a Certificate Request Message Format (CRMF) request to a Certificate System CA with the request encoded with proof of possession (POP) data that can be verified by the CA server. If a client provides POP information with a request, the server can verify that the requester possesses the private key for the new certificate.
- The HTTP Client utility sends a CMC request (created with the CMC Request utility) or a PKCS #10 request to a CA.
- The OCSP request utility creates an OCSP request conforming to RFC 2560, submits it to the OCSP server, and saves the OCSP response in a file.

- The PKCS #10 utility generates a public key pair in the security database, constructs a PKCS#10 certificate request with the public key, and outputs the request to a file.
- The Revocation Automation utility sends revocation requests to the CA agent interface to revoke certificates.

3.2 Physical Boundaries

The components of the TOE include:

- Primary Certificate System components:
  - Certificate Authority (CA)
  - Data Recovery Manager (DRM)
  - Online Certificate Status Protocol (OCSP) Manager
  - Token Key Service (TKS)
  - Token Processing System (TPS)
- Command-line tools:
  - PKI setup tools
    - pkiarch/pkidist/pkiflavor/pkiname/pkiperl
    - pkicreate/pkiremove/pkicommon
    - pkisilent
    - p7tool
    - pkihost
    - revoker
  - TOE management tools
    - AtoB (ASCII to Binary)
    - AuditVerify
    - BtoA (Binary to ASCII)
    - CMCEnroll
    - CMCRequest
    - CMCResponse
    - CMCRevoke
    - CRMFPopClient (CRMF Pop Request)
    - ExtJoiner (Extension Joiner)

- GenExtKeyUsage (Key Usage Extension)
- GenIssuerAltNameExt (Issuer Alternative Name Extension)
- GenSubjectAltNameExt (Subject Alternative Name Extension)
- HttpClient
- OCSPClient
- PKCS10Client (PKCS #10 Client)
- PKCS12Export
- PrettyPrintCert (Pretty Print Certificate)
- PrettyPrintCrl (Pretty Print Certificate Revocation List)
- TokenInfo
- setpin (PIN Generator)
- sslget
- tkstool

The components of the TOE environment include:

- Red Hat Enterprise Linux (RHEL) 5.6+ – provides basic execution, data storage support, and network connectivity services.
- Open Java Development Kit (JDK)/Java Runtime Environment (JRE) 1.6+.
- Java Security Services (JSS) 4.6+ – provide security services to applications (e.g., encryption).
- Network Security Services (NSS) 3.12+ – provide security services to applications (e.g., encryption).
- Tomcat 5.5.23+ (and) and Apache 2.2.3+ – provide web-based (HTTP/HTTPS) interfaces being clients and the TOE.
- Tomcatjss, mod_nss (1.0.8+), and mod_revocator (1.0.3+) (shipped with RHEL) – provide network security services to applications (e.g., encryption).
- Red Hat Directory Server 8.2+ – provides the internal directory (database storage) for the TOE.
- Firefox 3.x+ – provides a browser for web services access.
- Hardware Security Module (HSM) – Thales nCipher netHSM – provides the FIPS-certified cryptographic services related to certificate management for the TOE.
- Enterprise Security Client (ESC) – provides the client to access token services available via the TPS.

- mozldap-tools (6.0.5+) and perl-Mozilla-LDAP (1.5.2-4+) – provides useful ldap tools (search, modify, delete).
- nss-tools (3.12+) – provides tools used to debug and develop NSS applications.
- Nuxwdog (1.0.0-14+) – provides watchdog daemon services that can stop and start the server.
- PKI Console - java-based GUI tool used for administration of CA, DRM, OCSP, and TKS instances.

4 Security Policy

The RHCS 8.1 TOE is designed to offer security functions generally expected of Certificate Issuing and Management Systems. While administrators of the TOE may have access to available command-line utilities, other users are limited to services offered via the web-based HTTP/HTTPS interfaces. The RHCS 8.1 TOE offers the security functions summarized in the following subsections.

4.1 Identification & Authentication

RHCS 8.1 ensures that users are identified and authenticated before they can access any other security relevant services.

4.2 Access Control

RHCS 8.1 provides the ability to define an access control list for each service it provides. These access control lists are used to ensure that users can only access services they have been authorized to use.

4.3 Security Management

RHCS 8.1 uses the access control functions to control the actions of administrative personnel. In order to accomplish this, predefined access control lists are assigned to the applicable services.

4.4 Security Audit

RHCS 8.1 has the capability to audit security relevant events. Audit records are generated when audit events occur, including the responsible user, date, time, and other details. Audit records are collected into audit buffers that are signed, to protect against possible tampering of the audit records, and then copied into non-volatile audit logs.

4.5 Remote Data Entry & Export

RHCS 8.1 protects data import and export operations using SSL sessions and secure channels in the case of TMS.

4.6 Key Management

RHCS 8.1 includes a number of key management functions. In particular, RHCS 8.1 protects security critical keys and other information by either encrypting it or storing it within a hardware cryptographic module. RHCS 8.1 also uses digital signatures when appropriate to ensure the integrity of key management related information.

4.7 Certificate Management

RHCS 8.1 includes a number of certificate management functions. In particular, RHCS 8.1 allows administrators to control, limit, or mandate values in certificates, certificate revocation lists (CRLs), and online certificate status protocol (OCSP) responses that are generated.

4.8 Strength of Functions

RHCS 8.1 is designed to make appropriate use of a FIPS 140-2 certified Hardware Security Module (HSM) for critical cryptographic operations.

5 Assumptions

The following assumptions were made during the evaluation of RHCS 8.1:

- Audit logs are required for security-relevant events and must be reviewed by the Auditors.
- 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.)
- Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
- All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
- Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
- Malicious code destined for the TOE is not signed by a trusted entity.
- 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.
- General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
- 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.

- The system is adequately physically protected against loss of communications i.e., availability of communications.
- The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.
- 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.[1]

6 Documentation

The end user documentation has been consolidated at http://docs.redhat.com/docs/en-US/Red_Hat_Certificate_System_Common_Criteria_Certification/index.html.

The documentation for the evaluated version is *Red Hat Certificate System Common Criteria Certification 8.1,* dated January 31, 2012 and includes the following documents:

- Admin Guide:
- Agent Guide:
- Command-Line Tools Guide:
- Deploy and Install Guide:
- Managing Smart Cards with the Enterprise Security Client:
- Using End User Services:
- Release Notes.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Red Hat Certificate System 8.1, Version 2.0, February 15, 2012.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

1. Identification & Authentication
2. Access Control
3. Security Management
4. Security Audit
5. Remote Data Entry & Export

[1] This assumption has been copied directly from the CIMC PP. In the context of this ST, "appropriate Security Level identified in this family of PPs" reflects Security Level 3 as represented by this ST.

6. Key Management
7. Certificate Management
8. Strength of Functions

7.2 Evaluation Team Independent Testing

The evaluation team installed the product according the Common Criteria Guide, ran a sample of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing boundary conditions not tested by Red Hat. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Red Hat Certificate System 8.1. To use the product in the evaluated configuration, the product must be configured as specified in the **Defining the Common Criteria Environment** appendix of the **Deploy and Install Guide**. The document is available at the Red Hat website at http://docs.redhat.com/docs/en-US/Red_Hat_Certificate_System_Common_Criteria_Certification/8.1/html/Deploy_and_Install_Guide/common-criteria-appendix.html.

9 Results of the Evaluation

The evaluation was conducted in accordance with the CC and the CEM and the policies/procedures documented on the NIAP CCEVS web site (www.niap.ccevs.org). The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. 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. 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. In the Final Evaluation Technical Report (ETR), all Fail or Inconclusive work unit verdicts have been resolved by the developer and the evaluation team. The details of the evaluation are recorded in the CCTL's proprietary Evaluation Technical Report (ETR).

The evaluation confirmed that the Red Hat Certificate System 8.1 product is compliant with the CC functional requirements (Part 2 extended) and assurance requirements (Part 3

conformant) for EAL4 augmented with ACL_FLR.2. The product was evaluated and tested against the claims presented in the Security Target dated February 15, 2012. The evaluation team performed independent functional and vulnerability tests which included repetition of a sample of the vendor's tests, and the evaluation team's assessment of the evaluation evidence demonstrated that the claims in the ST were met. The validation oversight reviews support the evaluation team's conclusion that Red Hat Certificate System 8.1 meets the claims stated in the Security Target.

10 Validator Comments/Recommendations.

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Red Hat Certificate System 8.1 Security Target, Version 1.0, February 15, 2012*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Red Hat Certificate System 8.1 Part 2 (Proprietary)*, Version 2.0, January 27, 2012.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Red Hat Certificate System 8.1, ETR Part 2 Supplement (SAIC and HP Proprietary)*, Version 2.0, January 27, 2012.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Red Hat Certificate System 8.1 Security Target, Version 1.0, February 15, 2012.