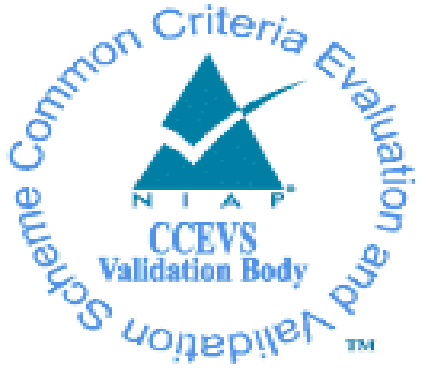
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report for the
Red Hat® Certificate System 10.4

Report Number: CCEVS-VR-VID11468-2024
Dated: August 23, 2024
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Anne Gugel
Randy Heimann
Lisa Mitchell
Linda Morrison
Robert Wojcik

Common Criteria Testing Laboratory

Kevin Cummins
Ryan Hagedorn
Cornelius Haley
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Red Hat Certificate System 10.4 solution 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 (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in August 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the Protection Profile for Certification Authorities, Version 2.1, 01 December 2017.

The Target of Evaluation (TOE) is the Red Hat Certificate System 10.4.

The 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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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, 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Red Hat® Certificate System 10.4 Security Target, Version 0.6, August 19, 2024 and analysis performed by the validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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) 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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 10.4
Protection Profile	Protection Profile for Certification Authorities, Version 2.1, 01 December 2017
ST	Red Hat® Certificate System 10.4 Security Target, Version 0.6, August 19, 2024
Evaluation Technical Report	Evaluation Technical Report for Red Hat Certificate System 10.4, Version 0.3, August 19, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Red Hat, Inc.
Developer	Red Hat, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Anne Gugel, Randy Heimann, Lisa Mitchell, Linda Morrison, Robert Wojcik

3 Architectural Information

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

The Target of Evaluation (TOE) is Red Hat Certificate System 10.4.

3.1 TOE Description

Red Hat® Certificate System (RHCS) is an enterprise software system that offers a scalable, secure framework to establish and maintain trusted identities and keep communications private.

RHCS provides certificate life-cycle management: issue, renew, suspend, revoke, archive/recover/manage single and dual-key X.509v3 certificates needed to handle strong authentication, single sign-on, and secure communications.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The RHCS TOE is an entity that issues and manages public-key certificates. It is an application written in Java, C++, C, and Python. The TOE also uses Java (Java Security Services; JSS) security service library. The TOE uses JSS as an API layer to invoke Network Security Services (NSS) cryptographic library operations. The JSS library itself is simply a software layer, it is NSS that is the actual cryptographic library.

The TOE also uses the OpenSSL cryptographic library for operations related to validating TOE updates. The TOE uses the kernel cryptographic API to initialize a DRBG that is then used by NSS and OpenSSL.

The RHCS is a software TOE that relies upon and incorporates different components in its Operational Environment. RHCS runs within Red Hat Enterprise Linux (RHEL 8.6), an operating system that protects the subsystems of the TOE with Security-Enhanced Linux (SELinux) policies and which provides secure network connections (using the TOE's Tomcat's HTTP/TLS to allow remote administration). The TOE and RHEL execute on a Dell PowerEdge R440 with an Intel(R) Xeon(R) Silver 4216 processor.

The TOE integrates with a directory server in its Operational Environment, such as Red Hat Directory Server, to provide an internal data store. The underlying NSS in the RHEL operating system component of the TOE supports the use of PKCS#11 hardware devices that perform standards-oriented cryptographic operations. All of the Operational Environment components along with the TOE components represent an RHCS system.

An RHCS system is composed of the following key components:

- Red Hat Certificate System (RHCS) - The Certificate System (CS) includes five configurable subsystems that work together to manage enterprise PKI deployments.
- Red Hat Enterprise Linux (RHEL) – The operating system (OS) in which RHCS and other components execute. The OS includes the software cryptographic module NSS, which supplies cryptographic functionality for TLS/HTTPS. The OS also includes the OpenSSL software which supplies cryptographic functionality for RHEL's package manager, RPM, which verifies update packages.
- Hardware Security Module (HSM) - –An HSM provides the FIPS-certified cryptographic services related to certificate management for the TOE. The HSM

provides secure key storage for private keys as well as cryptographic services to allow secure use of stored keys (for example, using a stored key to sign a CRL). The tested configuration includes the Entrust nShield Connect XC model number NH2075. This HSM is the nShield Connect XC series which contains internal FIPS module with firmware version 12.72.1 (FIPS CMVP 4334) running on a Freescale T1022 with cryptographic acceleration. While the evaluation tested using this Entrust HSM, any HSM that is at least FIPS 140-2 validated, provides PKCS#11 cryptographic services, hardware protection for keys and supports the required algorithms is considered equivalent.

- HTTP Engines (Tomcat (*for all subsystems: CA, KRA, OCSP Responder, TPS, and TKS*)) - The web engine provides the HTML-based UI (presentation), REST interface, and HTTP-based protocol handling. It does not perform authentication and authorization other than providing and/or enforcing TLS. 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 11.5) - The internal database stores information such as certificates, requests, officer/administrator/auditor information, and other information such as access control information. The CS communicates with the internal database securely through TLS client authentication.

The RHCS is composed of the following subsystems running on one or more host systems. A subsystem can reside on its own host system or be combined with other subsystems on a single host system. While only the first three subsystems along with command line tools (installed as part of the RHCS packages) are responsible for enforcing the requirements of the CAPP21 Protection Profile requirements (i.e., they comprise the TSF), one may use the other subsystems in an evaluated configuration to provide additional functionality beyond the scope of the CAPP21. All RHCS subsystems share common frameworks such as authentication, authorization, and auditing, as well as utilize the same Operational Environment components.

- 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).
- Online Certificate Status Protocol (OCSP) Responder - a subsystem that provides OCSP responder services, based on stored CA's CRLs to distribute the load for certificate status verification.
- Key Recovery Authority (KRA) - a subsystem that provides private encryption key storage and retrieval. In a Token Management System, the KRA’s HSM generates key pairs for the clients when server-side key generation option is turned on.
- 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

subsystems 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 RHCS subsystems (i.e., CA, KRA, OCSP Responder, TKS, and TPS) are highly integrated. OCSP and CA subsystems work together on CRL publishing and certificate verification. CA and KRA subsystems 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, works with at least two essential subsystems, a TKS to manage shared secrets between the tokens and the collective Token Management System (TMS) and a CA to process certificate enrollment operations. A TPS can also be configured to use a KRA 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, KRA, OCSP Responder, TPS, 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 framework.

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

In addition to the HTTP Engine and Internal Database, the RHCS also relies on access to processing capabilities, file storage, as well as hardware and software cryptographic modules provided by its Operational Environment.

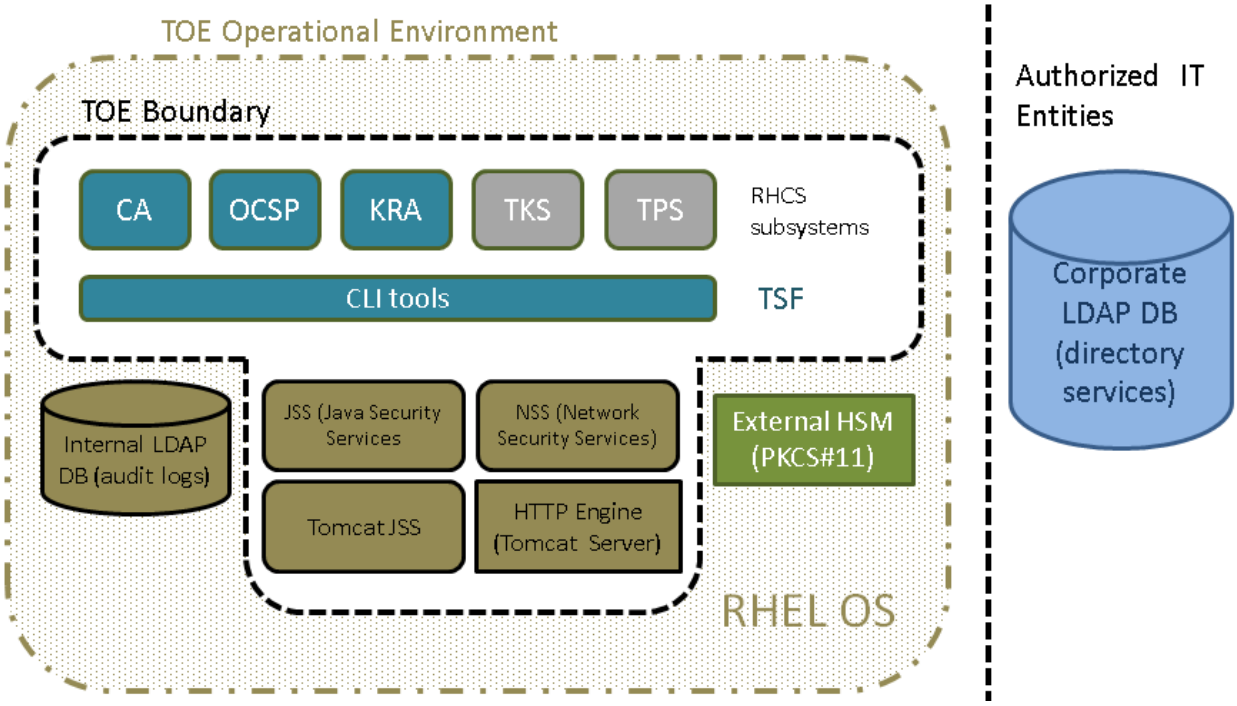


Figure 3-1 RHCS System Architecture

Figure 3-1 above depicts the architecture of the different parts of the TOE (including its RHCS [the upper portion] and RHEL [the lower, brown portion] components), the TOE's Operational Environment (OE), and external, authorized IT entities. Note that RHCS includes technology preview code (e.g., EST) and support for Automatic Certificate Management Environment (ACME) which is not evaluated, and which must not be used in the evaluated configuration.

While a complete RHCS *system* includes all the components indicated in Figure 3-1 the RHCS *TOE* includes the components within the TOE boundary. Specifically, the TOE's RHCS components consists of the CA, OCSP Responder, KRA, TKS, and TPS subsystems along with the command line utilities included with RHCS. The TOE's RHEL components include the NSS software cryptographic module and Tomcat server. The TSF portion of the TOE consists of the CA, OCSP, and KRA subsystems, while the TOE's OE includes other components within RHEL (the internal LDAP DB, watchdog daemon, and an HSM). The TOE OE's provides a Java GUI-based administration tool (called the "pkiconsole"). Administrators use this "console" for administrative tasks such as managing users and maintaining the different (CA, OCSP Manager, KRA, and TKS) subsystems and performing daily operational and managerial duties for those subsystems.

3.4 Physical Boundaries

As depicted in Figure 3-1, the TOE exists as a collection of application programs interacting with other components to implement its security functions. The TOE applications run within an IT environment based on RHEL (with configured SELinux policies) and including a Java

runtime environment (invoking NSS), a Tomcat HTTP Engine, and a directory server (e.g., Red Hat Directory Server) and watchdog daemon.

The TOE supports LDAP interfaces and also HTTP-based interfaces. The LDAP interfaces are used to connect to the internal LDAP Server (e.g., Red Hat Directory Server) used by RHCS exclusively as a private data store, and also to connect to a Corporate LDAP server for publishing purposes, if configured. The HTTP-based interfaces allow users, administrators, agents, and auditors to connect to RHCS to access its security functions and to manage RHCS.

Since the TOE is a collection of application programs, its logical and physical boundaries largely coincide. The TOE requires basic execution, data storage support, and network connectivity services from its IT environment. The external interfaces are limited to LDAP (over TLS), HTTP/TLS, and the use of command-line utility programs.

LDAP connections are supported only when initiated by RHCS. The HTTP/TLS interfaces are used to offer functions via service-oriented web pages to RHCS users, agents, auditors, and administrators. The command-line utility programs make use of these other interfaces, data files (e.g. for configuration or audit review), and in some cases do not interact with the rest of the TOE at all.

Note that many administrative functions (for the CA, KRA, OCSP, and TKS subsystems) are performed using a console application included with RHCS. This application interacts with the RHCS using HTTP/TLS, but instead of using XML/HTML it uses proprietary name/value pairs to better facilitate the administrator functions available. The TPS subsystem is managed via changes in configuration files (using RHEL OS tools) and through a web browser using HTTP/TLS. Some command-line tools are also available either utilizing the same name value pair mechanism or through the REST interface.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. User data protection
5. Identification and authentication
6. Security management
7. Protection of the TSF
8. TOE access
9. Trusted path/channels

4.1 Security audit

The TOE generates logs for a range of security relevant events and relies upon its Operational Environment (OE) for generation of operating system events. The TOE provides secure storage of audit events and further provides separate audit storage for certificate related events. The TOE provides no administrator or auditor method for deletion or removal of

events, and the TOE shuts down in the event of an error that prevents the TOE from creating new audit records.

4.2 Communication

The TOE provides proof of origin for issued certificates through CRLs and OCSP responses. The TOE also verifies certificate related messages using signed CMC requests and responses.

4.3 Cryptographic support

The TOE relies upon its OE for all cryptography and uses the OE-provided cryptography in support of certificate issuance and related CA operations, in support of HTTPS, TLSS, and TLSC operations.

4.4 User data protection

The TOE provides certificate profile functionality and certificate generation services conforming to IETF RFC 5280. The TOE provides certificate status information through CRLs and OCSP responses. The TOE clears sensitive data from buffers before releasing the buffers.

4.5 Identification and authentication

The TOE handles Certificate Management over CMS as both a client and server. The TOE performs certificate path validation in conformance with IETF RFC 5280.

4.6 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target as well as other functions commonly found in certificate authorities. The TOE provides its available functions to CA administrators, CA operations staff, Administrators/Officers, and Auditors.

4.7 Protection of the TSF

The RHCS TOE protects itself and relies on supporting protections from other components. At a high level, the TOE utilizes a separate and distinct hardware cryptographic engine for critical cryptographic operations; the TOE makes effective use of SELinux security mechanisms to protect itself and its underlying data and executables; the TOE command-line tools do not operate on or modify live TOE data, but rather use the documented security interfaces of the TOE to interact with the TOE; the TOE security functions are modular to isolate them from potential errors in other components; and the TOE interfaces are well-defined and restricted using a common certificate-based access control mechanism to distinguish among and limit the functions of administrator roles.

The TOE protects itself primarily using its identification & authentication and access control functions. With these functions, it ensures that users are properly authenticated, and they are

authorized to perform the functions made available by the TOE. Users that cannot be authenticated or that are not authorized will be denied access to applicable TOE functions.

The TOE relies on the components identified above for security and non-security functions. The primary security functions involve protecting the TOE as it is executing or at rest within its host, in facilitating secure inter-component communication, and providing FIPS-compliant cryptographic services.

The host operating system and Java implementation are relied upon to provide a distinct and separate execution environment for the TOE applications. In order to make effective use of the operating system, all RHCS components are packaged utilizing standard Red Hat package management (RPM). As such, whenever the TOE components are installed, they are stored with "root" user and group ownership and utilize standard Linux directory, file, and executable UNIX permissions. When an RHCS TOE instance is generated from these installed components, a "pkiuser" user and group identifier is used for ownership of *most* portions of the installed instances. The notable exceptions are (1) that an instance's start/stop script is ONLY granted "root" ownership with read/write/execute permission available only to root and (2) that the signed audit log files contained under the signedAudit directory contain a group privilege of "pkiaudit" to allow separation of roles between auditors and administrators. Files owned by "pkiuser" containing potentially sensitive information (e. g., log files, configuration files such as CS.cfg, and NSS security database files) contain no privileges for "other" users (e.g., file permissions of 00660 or 00600). Also, the entire contents of each PKI instance's signed audit directory are not accessible to "other" users. In practice, access to the "root" account is limited to administrators and the "pkiuser" account is configured so that it is not used by any human user, but rather is used by TOE components.

While previous versions of the TOE operated in an unconfined SELinux domain, a SELinux policy was created specifically to enhance the protection of RHCS. This policy includes the following characteristics:

1. The files and directories delivered for each of the subsystems are labeled with specific SELinux contexts (*pki_ca_exec_t, pki_ca_var_lib_t, pki_ca_var_log_t,* etc. for a CA for example).
2. The ports used by each subsystem are labeled with specific SELinux contexts (*pki_ca_port, pki_tps_port,* etc.).
3. The CS subsystem processes are also constrained to run within specific SELinux domains (*pki_ca_t, pki_ra_t, pki_ocsp_t,* etc.). When processes are started, they start in the *unconfined_t* domain, but transition into their assigned domain.
4. Each SELinux domain has rules written to specify the actions that are authorized for the domain. As an example, the *pki_ca_t* domain has rules written to allow write-access files with context *pki_ca_var_log_t*. Moreover, it has rules to allow processes running within the domain to connect to ports of type *pki_ca_port* (as well as others).
5. All accesses not specified in the policy are denied.

Ultimately, the operating system with SELinux extensions is configured to protect the TOE and its stored data using the core access control mechanisms and SELinux domain protection mechanisms.

The TOE also relies on its security provider (NSS) and web engines primarily to facilitate secure (TLS/HTTPS) communications between TOE components and also with TOE clients.

While the TOE can support a number of cipher suites with RSA and ECC key exchange, limiting TLS ciphers to FIPS compliant algorithms is encouraged.

Finally, the TOE depends on a FIPS validated HSM to provide the underlying cryptographic support necessary to allow the TOE to securely act as a certificate authority (signing/issuing certificates and revocation information [CRL and OCSP]). The TOE accesses the HSM via a corresponding library installed on the host operating system. The HSM stores critical keys so that they are not externally accessible. It provides access to its embedded keys in order to generate new keys, encrypt/decrypt data, produce signatures, etc. In practice, the TOE is the sole user or client of the HSM attached directly to its host operating system.

4.8 TOE access

The TOE offers an administrator configurable timeout after which to lock remote interactive sessions as well as allowing remote users to terminate their interactive session. The TOE also has the capability to display an advisory message (banner) when users access the TOE for use.

4.9 Trusted path/channels

The TOE protects interactive communication with administrators on the HTTPS (WebUI) interface, the set of TLS protected command line tools, and the pkiconsole application that utilizes HTTPS protected REST API interfaces. In each case, both integrity and disclosure protection are ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, the attempted connection will not be established.

The TOE protects communication with network peers, such as a directory services, using TLS connections to prevent unintended disclosure or modification of data.

5 Assumptions & Clarification of Scope

Assumptions
The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Certification Authorities, Version 2.1, 01 December 2017

That information has not been reproduced here and the CAPP21 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the CAPP21 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Protection Profile for Certification Authorities and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Certificate Authority models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CAPP21 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Red Hat Certificate System 10.4 - Administration Guide (Common Criteria Edition), 2024-08-14
- Red Hat Certificate System 10.4 - Planning, Installation, and Deployment Guide (Common Criteria Edition), 2024-08-14

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

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 proprietary Detailed Test Report for Red Hat

Certificate System 10.4, Version 0.3, August 19, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the CAPP21 including the tests associated with optional requirements. The AAR identifies the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration consists of the Red Hat Certificate System 10.4 running Red Hat Enterprise Linux (RHEL 8.6) on a Dell PowerEdge R440 with an Intel(R) Xeon(R) Silver 4216 processor. An Entrust nShield Connect XC series Hardware Security Module was used for hardware based cryptographic security functions.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

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 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Red Hat Certificate System 10.4 TOE to be Part 2 extended, and to meet the SARs contained in the CAPP21.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Red Hat Certificate System 10.4 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CAPP21 related to the examination of the information contained in the TSS.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the CAPP21 and recorded the results in a Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- cve.org CVE Database (https://www.cve.org/)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

on 7/23/2024 (from 1/1/2018) with the following search terms: "RHCS", "RHEL", "Thales", "nShield", "Certificate Authority", "(NSS)", "TLS", "pki-core", "Intel+Xeon+Silver".

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated. Special care should be taken with regard to

the selection of an appropriate Hardware Security Module for use with the TOE, ensuring that it is the same as, or equivalent to, the HSM used in the evaluated configuration.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included with the product, or within the operational environment, was not assessed as part of this evaluation and no further conclusions can be drawn about their effectiveness. This functionality and its impact on the product when deployed in the operational environment needs to be assessed separately in the context of the larger architecture that the product is a part of. No versions of the TOE models or firmware versions, either earlier or later, were evaluated.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: Red Hat® Certificate System 10.4 Security Target, Version 0.6, August 19, 2024.

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 for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Certification Authorities, Version 2.1, 01 December 2017.

[5] Red Hat® Certificate System 10.4 Security Target, Version 0.6, August 19, 2024 (ST).

[6] Red Hat Certificate System 10.4 - Administration Guide (Common Criteria Edition), 2024-08-14.

[7] Red Hat Certificate System 10.4 - Planning, Installation, and Deployment Guide (Common Criteria Edition), 2024-08-14.

[8] Assurance Activity Report for Red Hat Certificate System 10.4, Version 0.3, August 19, 2024 (AAR).

[9] Detailed Test Report for Red Hat Certificate System 10.4, Version 0.3, August 19, 2024 (DTR).

[10] Evaluation Technical Report for Red Hat Certificate System 10.4, Version 0.3, August 19, 2024 (ETR).