National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

EJBCA Enterprise 9.3.3

Report Number: CCEVS-VR-VID11530-2026

Dated: January 23, 2026

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

Sheldon Durrant
Lisa Mitchell
Linda Morrison
Randy Heimann

The MITRE Corporation (FFRDC)

Robert Wojcik

John Hopkins Applied Physics Lab

Common Criteria Testing Laboratory

Diego Sierra Liras

DEKRA Cybersecurity Certification Laboratory,

Sterling, Virginia, USA

Table of Contents

Contents

1 Executive Summary

This Validation Report (VR) documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of EJBCA Enterprise 9.3.3, provided by Keyfactor. 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 DEKRA Cybersecurity Certification Common Criteria Testing Laboratory (CCTL) in Sterling, Virginia, United States of America, and was completed in January 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by DEKRA. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *Protection Profile for Certification Authorities*, Version 2.1, 2017-12-01 [PP_CA].

The TOE, EJBCA Enterprise 9.3.3, is a certification authority (CA) product. The TOE's primary purpose is issuance and life cycle management of public key certificates of the type specified in the X.509 v3, C-ITS Enrollment CA IEEE 1609.2, and CVC BSI TR-03110 standards. Additionally, EJBCA can also be set up as a high performance, highly available OCSP responder service, Validation Authority (VA).

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 5) for conformance to the *Common Criteria for IT Security Evaluation* (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the [PP_CA].

This VR 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 (ETR) is consistent with the evidence provided.

The Validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the [PP_CA] Assurance Activities. 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 *Security Target for EJBCA Enterprise 9.3.3*, Version 1.4, January 2026, 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). CCTLs evaluate products against Protection Profile containing Assurance Activities that are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance List (PCL).

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 results 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	EJBCA Enterprise 9.3.3
Protection Profile	*Protection Profile for Certification Authorities*, Version 2.1, 2017-12-01
Security Target	*Security Target for EJBCA Enterprise 9.3.3*, Version 1.4, January 2026
Evaluation Technical Report	*Evaluation Technical Report for EJBCA Enterprise 9.3.3 Volume 1: Evaluation of the ST*, Version 0.2, January 20, 2026 *Evaluation Technical Report for EJBCA Enterprise 9.3.3 Volume 2: Evaluation of the TOE*, Version 0.2, January 20, 2026
CC Version	*Common Criteria for Information Technology Security* Evaluation,

	Version 3.1 Revision 5
CEM Version	*Common Methodology for Information Technology Security Evaluation*, Version 3.1, Release 5, April 2017
Conformance Result	CC Part 2 extended; CC Part 3 conformant
Sponsor & Developer	KEYFACTOR
Common Criteria Testing Lab (CCTL)	DEKRA Cybersecurity Certification, Sterling, Virginia, USA
CCEVS Validators	Sheldon Durrant, Lisa Mitchell, Linda Morrison, Randy Heimann, Robert Wojcik

3 Architectural Information

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

3.1 TOE Introduction

The TOE, EJBCA Enterprise 9.3.3, is certification authority (CA) product. The TOE's primary purpose is issuance and life cycle management of public key certificates of the type specified in the X.509 v3, C-ITS Enrollment CA IEEE 1609.2, and CVC BSI TR-03110 standards. Additionally, EJBCA can also be set up as a high performance, highly available OCSP responder service, Validation Authority (VA).

3.2 Physical Boundaries

The TOE is obtained as a Docker container image from customer-specific HTTPS repositories operated by Keyfactor, at the private registry repo.keyfactor.com/images/ejbca-ee.

The EJBCA documentation is available for download to support customers via the Keyfactor Support Portal, which is currently hosted on Zendesk.

The Administrator Guide can also be consulted on the official Keyfactor documentation site at: https://docs.keyfactor.com/ejbca/9.3.3/

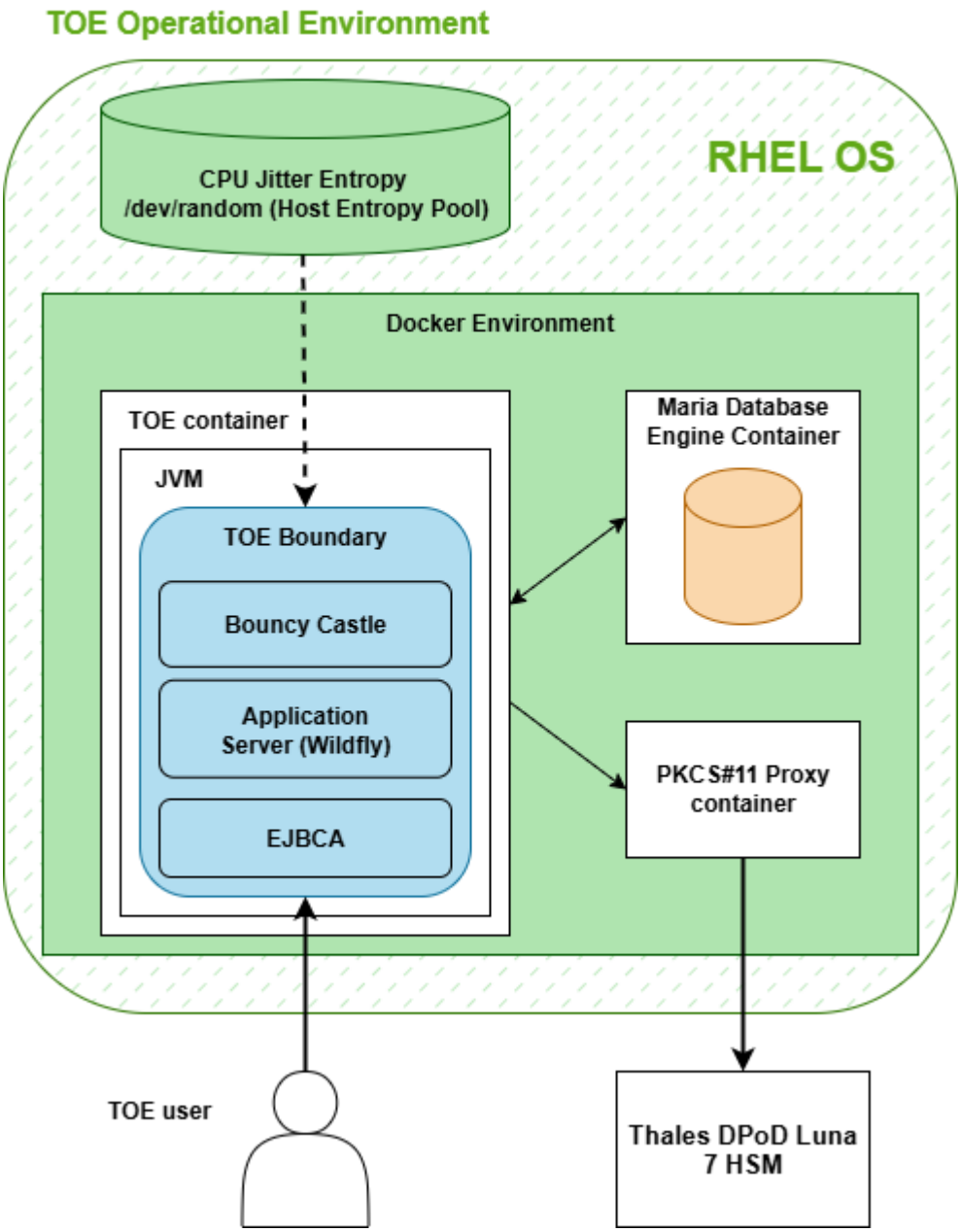
Item	**Identifier**	**Format**
CC supplementary Guidance	*EJBCA Enterprise 9.3.3 Common Criteria Guidance Supplement*, v1.1, January 2026	PDF
Administrator operational guidance	*EJBCA 9.3.3 Administrator Guide version 1.0*	PDF
TOE	EJBCA Enterprise 9.3.3	Docker container

As illustrated by the figure below, the TOE includes:

- The EJBCA component;
- Application server (WildFly)

Excluded from the TOE is:

- Hardware and operating system platform (abstract machine);
- Execution environment (Java Virtual Machine);
- Hardware security module (HSM); and
- Database engine



As illustrated in the figure above, the TOE establishes the following communications:

- The TOE acts as a server for TOE users, who interact with it via web interfaces using HTTPS/TLS channels.
- The TOE establishes a JDBC connection with a MariaDB database instance. This connection is protected within the confines of the operating system and container environment.
- The TOE interacts with the PKCS#11 proxy module via standard PKCS#11 API calls. This connection is protected within the confines of the operating system and container environment.

Excluded from the TOE scope:

- The PKCS#11 proxy container establishes a PKCS#11 protocol channel with the Thales DPoD Luna 7 HSM, which is considered part of the operational environment.

4 Security Policy

The TOE enforces the following security functions as described in the ST.

4.1 Security Audit

One very common requirement on sensitive systems is to provide secure audit records. Though creating audit records is simple, ensuring that they are not tampered with is much more difficult. By using the security audit functions of the TOE, an application will be able to create audit trails that meet ETSI EN 319 401 and ETSI EN 319 411 requirements for secure audit.

The TOE generates the audit records listed in Table 12, Table 13 and Table 14 of the ST. The event formatting is described in the guidance documentation. The TOE can associate each auditable event with the identity of the user that caused the event. It provides the ability to apply searches of audit data based on serial numbers associated with the event. The TOE provides an 'Auditors' group and stipulates that an auditor can view the signed audit logs.

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 generates an error message in the event of an error that prevents the TOE from creating new audit records.

The certificates and CRLs repository is provided by the database in the operational environment. PKCS#11 is used as interface. Audit events are stored in both the operating system and the database on the TOE platform.

4.2 Communication

The TOE provides certificate-based proof of origin for the certificates it issues by digitally signing each certificate in accordance with RFC 5280. In addition, the TOE provides proof of origin for the certificate status information it issues by digitally signing CRLs (RFC 5280) and OCSP responses (RFC 6960). The TOE uses the HSM to perform the digital signature operations for certificates, CRLs, and OCSP responses using the signature algorithm configured for the issuing CA key (e.g., RSA or ECDSA with the corresponding hash).

4.3 Cryptographic Support

The TOE relies upon the HSM in the operational environment for cryptographic operations involving persistent private keys, such as key-pair generation, certificate signing, OCSP responses, and protocol response messages (e.g., EST), performed through the PKCS#11 API using calls like C_GenerateKeyPair and C_Sign.

Secure communications are managed by the TOE’s WildFly application server, which establishes HTTPS/TLS channels by integrating the Bouncy Castle cryptographic module as its JSSE provider. This architecture employs a hybrid cryptographic model to optimize both performance and security.

- The Bouncy Castle module handles the high-volume TLS session operations in software. This includes the negotiation of cipher suites, symmetric encryption (e.g., AES-GCM), hashing for message integrity (HMAC), and the generation of ephemeral keys for key establishment. The Bouncy Castle HMAC-DRBG(SHA-512) is used for this purpose, and in the evaluated configuration, it is seeded with entropy obtained from the RHEL host operating system's /dev/random pool. This pool is continuously supplied by the Kernel CPU Time Jitter RNG, which is the entropy source validated under ESV Certificate #E54.
- In contrast, all cryptographic operations requiring the server's persistent private key, such as the digital signature performed during the TLS handshake to authenticate the server, are delegated to the Thales DPoD

Luna 7 HSM (CMVP #4327 and ESV E#98) using the SafeNet Accelerated Cryptographic Library validated under ACVP (SHS 4533, A1170, A11712, RSA 3042, ECDSA 1526) via a PKCS#11 provider. The PKCS#11 provider is the Java software component that connects EJBCA to the HSM's PKCS#11 interface, so EJBCA's key generation and signing requests are executed in the HSM via PKCS#11 calls such as C_GenerateKeyPair and C_Sign. The server's persistent TLS authentication key is generated and stored securely within the HSM and never leaves its boundary.

4.4 User data protection

The TOE provides certificate profile functionality and certificate generation services conforming to IETF RFC 5280. A CA account can have one or more profiles which are configured by an administrator using the TOE's web interface. Using that interface the administrator can assign a name (Certificate Profile ID), extensions, and default properties to the profile.

The TOE supports the approval of certificates issued according to a configured certificate profile through the web interface, the RA management interface or EST. Only user roles given 'Approve End Entity Actions' permission can approve certificates via the web interface (which is the only interface through which manual issuance occurs).

The TOE provides certificate status information through CRLs and OCSP responses. The TOE clears sensitive data from buffers before releasing the buffers.

The TOE does not store any personally identifiable information, that does not also appear in a certificate. The TOE does handle the TLS session object.

The TSF, in conjunction with the HSM, ensures that sensitive data is securely protected or erased when it is no longer needed, so that any previous content cannot be recovered. This applies to secret and ephemeral keys.

4.5 Identification and authentication

The TOE supports Enrollment over Secure Transport (EST) protocol as described in RFC 7030 to receive and act upon certificate enrollment requests using the simple enrollment method described in RFC 7030 Section 4.2.

Certificate enrollment requests are authenticated using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2.

The TOE provides a certificate-based mechanism via web interface. For certificate authentication the TOE uses the HSM to validate certificates. The TOE uses X.509v3 certificates, as defined by RFC 5280, to authenticate privileged users, subscribers, RAs, and DBAccess clients over HTTPS. Certificates can also be used for EST access authentication.

When the TSF cannot determine the current revocation status of a certificate the administrator is allowed to choose whether to accept the certificate or not.

The TSF allows the following actions prior to requiring a non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- Obtain certificate status information;
- Enrollment and public information retrieval requests.

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.

Administrative roles are fully configurable. The TOE provides default role templates corresponding to the roles defined in the Protection Profile. The corresponding TOE role names are:

- Administrator – Super Administrator
- Auditor – Auditor
- CA Operations Staff – CA Administrators
- RA Staff - RA Administrators
- Authorized Organizational Representative - Supervisor

4.7 Protection of the TSF

The TOE protects itself after a secure component failure that will result in an error message giving the Administrator the possibility to perform a secure restart. The TOE utilizes a HSM and relies upon the HSM to secure and protect the keys stored by the TOE in the HSM, and to offer services to allow operations using the HSM protected certificates.

The TOE obtains the current time from its operational environment.

4.8 TOE Access

The TOE allows 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. 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.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in [PP_CA]. That information has not been reproduced here and [PP_CA] should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in [PP_CA] as described for this TOE in the ST. 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.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within [PP_CA].
- 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 Guides identified in Section 6, additional customer documentation for the specific TOE model was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 Section 6 of the Security Target and their operation with respect to the TOE is described in Section 7 of the Security Target. Any other functionality provided by EJBCA Enterprise needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The TOE supports several features that are not part of the evaluated functionality. These features are not tested and are excluded from the scope of the evaluation: The TOE shall be deployed in a general computing platform. Deployment models that include hosting on or delivering services from cloud environments are excluded from the evaluated configuration.

6 Documentation

The vendor provides a standard set of guidance documents that covers the core functionality of the product. These documents were used during the evaluation of the TOE:

- *EJBCA 9.3.3 Administrator Guide* version 1.0
- *EJBCA Enterprise 9.3.3 Common Criteria Guidance Supplement*, v1.1, January 2026

To use the TOE in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above. Consumers are encouraged to download this documentation from the NIAP website.

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 TOE as evaluated.

7 IT Product Testing

This section describes the testing efforts of the Evaluation team. The information is derived from the EJBCA Enterprise 9.3.3 Test Report document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

7.1 Developer Testing

PP_CA v2.1 evaluations do not require developer testing evidence for assurance activities.

7.2 Evaluator Team Testing

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to PP_CA v2.1.

The Evaluation team established a test configuration comprising EJBCA Enterprise 9.3.3. Section 1.3 of the AAR provides a description of the test configuration the CCTL used to test the TOE, including a description of the test environment and a list of tools used.

A test plan was developed in accordance with the Testing Assurance Activities specified in the PP_CA v2.1.

The formal testing activity was conducted between September 8 2025 and January 20 2026 with the TOE installed in the DEKRA lab located at 405 Glenn Dr, Suite 12, Sterling, VA 20164.

- The Evaluator successfully performed the following activities during independent testing:
    - Placed TOE into evaluated configuration by following the preparative procedures.
    - Successfully executed the PP_CA v2.1 Assurance-defined tests.
    - Planned and executed a series of vulnerability/penetration tests.

It was determined after examining the Test Report and full set of test results provided by the evaluators that the testing requirements for PP_CA v2.1 were fulfilled.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the EJBCA Enterprise 9.3.3 software installed upon a general-purpose server platform. The following table lists all the components in the evaluated configuration.

Part	Description
Abstract Machine	Dell EMC PowerEdge R440 with Xeon Silver 4216
Abstract Machine Operating System	Red Hat Enterprise Linux 9.4 (kernel: 5.14.0-427.13.1.el9_4) RHEL Kernel CPU Time Jitter RNG Entropy Source version 2.2.0 (ESV E#54)
Container	Docker version 27.1.2
Container Operating System	Alma Linux 9.6
JEE 10 compliant application server	WildFly 35.0.1
Java Virtual Machine (JVM)	Oracle OpenJDK 17.0.16
Relational Database	MariaDB 11.5.2
HSM	Thales DPoD Luna 7 FIPS 140-2 validated (CMVP #4327 and ESV E#98) , using the SafeNet Accelerated Cryptographic Library validated under ACVP (SHS 4533, A1170, A11712, RSA 3042, ECDSA 1526)

To use the product in the evaluated configuration, the product must be configured as specified in *the EJBCA Enterprise 9.3.3 Common Criteria Guidance Supplement*, v1.1.

8.2 Excluded Functionality

The TOE shall be deployed in a general computing platform. Deployment models that include hosting on, or delivering service from, cloud environments are excluded from the evaluated configurations.

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 Evaluation 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 team determined the TOE to be Part 2 extended and Part 3 conformant, and meets the SARs contained in the PP. Additionally the Evaluation team performed the Evaluation Activities specified in the [PP_CA].

The following evaluation results are extracted from the proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluator ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the Evaluation team performed an assessment of the Evaluation Activities specified in the [PP_CA] to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

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 specified in the [PP_CA]. 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 ST and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the [PP_CA] 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 Assurance Activities, 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 specified in the [PP_CA]. 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. The Evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. 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 Assurance Activities, 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 specified in the [PP_CA], as well as the Assurance Activities specified for ALC_CMC.1 and ALC_CMS.1. The Evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

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 specified in the [PP_CA]. The Evaluation team ran the set of tests specified by the Assurance Activities in the PP_CA and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the [PP_CA], and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team performed a search of the following online sources:

- The National Vulnerability Database at https://nvd.nist.gov/vuln
- The CVE Details website at https://www.cvedetails.com/vulnerability-search.php

The searches were performed several times, most recently January 14, 2026, using the search terms listed in Section 3.5.1 of the AAR and CEM work unit specified in the [PP_CA]. The Evaluation team did not discover any applicable vulnerabilities. The Evaluation team also performed vulnerability testing and did not discover any issues with the TOE.

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 addressed the vulnerability analysis Assurance Activities in the [PP_CA] and 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 test activities 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 performed the Assurance Activities in the [PP_CA] and followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance documents listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated by NIAP.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The excluded functionality is specified in section 8.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

Per NIAP Scheme Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Security Target

The security target for this product's evaluation is *Security Target for EJBCA Enterprise 9.3.3*, Version 1.4, January 2026.

12 Acronyms

Acronym	Definition
CA	Certification Authority
CC	Common Criteria
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CM	Configuration Management
CSP	Critical Security Parameter
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PCL	Product Compliant List

PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	TOE Summary Specification
VR	Validation Report

13 Bibliography

The Validation team used the following documents to produce this VR:

CCEVS Documents

1. *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, Version 3.1 Revision 5.
2. *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements*, Version 3.1 Revision 5.
4. *Common Evaluation Methodology for Information Technology Security Evaluatio*n, Version 3.1 Revision 5.
5. *Protection Profile for Certification Authorities*, Version 2.1, 2017-12-01

Evaluation documents

1. *Security Target for EJBCA Enterprise 9.3.3*, Version 1.4, January 2026
2. *EJBCA Enterprise 9.3.3 Common Criteria Guidance Supplement*, v1.1, January 2026
3. *EJBCA 9.3.3 Administrator Guide version 1.0*
4. *EJBCA 9.3.3 Third-Party Libraries Vulnerability Analysis Report*, Version 0.2, January 14, 2026
5. *EJBCA 9.3.3 Enterprise Assurance Activity Report*, Version 1.1 January 20, 2026
6. *EJBCA 9.3.3 Enterprise Evaluator Test Report VID 11530*, Version 1.1, January 20, 2026
7. *Evaluation Technical Report for EJBCA Enterprise 9.3.3 Volume 1: Evaluation of the ST*, Version 0.2, January 20, 2026
8. *Evaluation Technical Report for EJBCA Enterprise 9.3.3 Volume 2: Evaluation of the TOE*, Version 0.2, January 20, 2026