CSEC

**Swedish Certification Body for IT Security**

# Certification Report - PrimeKey EJBCA Enterprise v7.4.1.1

**Issue: 1.0, 2021-Apr-16**

*Authorisation: Jerry Johansson, Lead Certifier , CSEC*

Table of Contents

# 1 Executive Summary

The TOE is PrimeKey EJBCA Enterprise v7.4.1.1, a java software application, implementing a certificate authority. The main purpose of the TOE is to issue and maintain the life-cycle of public key certificates.

The TOE has been evaluated with support of the following in the environment:

| | |
|---|---|
| Application server: | Wildfly 14.0.1 |
| Java virtual machine | Oracle OpenJDK 1.8.0:242 |
| Relational database | MariaDB 10.2.13 |
| Operating system | CentOS Linux 7 (kernel 3.10.0-1062.9.1.el7) |
| HSM | Utimaco CryptoServer SE52 |

The customers download the TOE from a private URL on PrimeKey's website.

The [ST] claims exact conformance to the Protection Profile for Certification Authorities, version 2.1 [PPCA]. The following technical decisions were found applicable and have been considered during the evaluation: TD0276, TD0278, TD0286, TD0287, TD0294, TD0328, TD0348, TD0353, TD0375, TD0415, TD0500, and TD0522.

The Security Target contains eight threats, one Organisational Security Policy (OSP), and three assumptions, which have been considered during the evaluation.

The evaluation has been performed by Combitech AB in their premises in Växjö, Sweden, and in the developer's premises in Solna, Sweden. The evaluation was completed on the 29th of March 2021.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed in accordance with the assurance package described in the Protection Profile for Certification Authorities [PPCA].

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology in accordance with the assurance package described in [PPCA].

The technical information in this report is based on the Security Target [ST] and the Final Evaluation Report (FER) produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

# 2 Identification

| Certification Identification | |
|---|---|
| Certification ID | CSEC2019005 |
| Name and version of the certified IT product | PrimeKey EJBCA Enterprise v7.4.1.1 (r35494) |
| Security Target Identification | Security Target for EJBCA v7.4.1, PrimeKey Solutions AB, 2021-03-29, document version 1.2 |
| Protection Profile | Protection Profile for Certificate Authorities, NIAP, 2017-12-01, v2.1 |
| Assurance package | As specified in the PP |
| Sponsor | PrimeKey Solutions AB |
| Developer | PrimeKey Solutions AB |
| ITSEF | Combitech AB |
| Common Criteria version | version 3.1 revision 5 |
| CEM version | version 3.1 revision 5 |
| QMS version | 1.24.1 |
| Scheme Notes Release | 18.0 |
| Recognition Scope | CCRA |
| Certification date | 2021-04-XX |

# 3 Security Policy

The TOE provides the following security functionality:

- Electronic Signatures Creation
- Create Digital Certificates and CRLs
- OCSP Support
- Data Integrity Protection
- Secure Audit
- Authentication and Authorization
- Token Management
- Key Generation and Management
- Backup of TOE Data
- Certificate Authority Management
- Key Recovery
- Profile Management
- User Registration and Management
- Certificate and CRL Publishing
- Certificate and CRL Retrieval

The TOE permits custom roles. The TOE provides templates for the roles defined in the [PPCA].

## 3.1 Electronic Signatures Creation

Creation of electronic signatures is a vital part of PKI applications. Electronic signatures can be created in a number of ways, low level and high level. The TOE will provide means to obtain a private key reference (compliant with the standard JCA) that can be used by relying applications for signing of specific document types. Signatures can be created in cryptographic modules, either using software or hardware (such as HSMs and smart cards).

## 3.2 Create Digital Certificates and CRLs

PKI management systems need to be able to create and process certificates and CRLs. These sets of security functions are aimed at systems that need to create and sign certificates and CRLs. The functions are also used by PKI enabled client systems that need to generate and process certificate services requests (CSRs) using standard formats such as PKCS#10 and CRMF (Certificate Request Message Format).

## 3.3 OCSP Support

Though CRLs may be enough for some digital certificate usage scenarios, business-critical applications tend to require a more flexible and up to date source of revocation information. Therefore, the TOE natively supports OCSP request parsing and response generation, providing real-time revocation status information.

## 3.4 Data Integrity Protection

The functions for data integrity protection are used to ensure that data, in transit or in storage, cannot be tampered without detection. Integrity protection can be ensured using several techniques, where the most common are message authentication codes and digital signatures.

## 3.5 Secure 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 in accordance with CWA 14167-1.

## 3.6 Authentication and Authorization

Authentication and authorization are the most basic security functions needed in order for an application to provide services to TOE users.

Authentication is the process of identifying the TOE users. Authentication can be performed in many ways and the TOE provides a framework that can be extended by relying applications in order to meet their specific authentication needs

Authorization approves or rejects a request for accessing a specific resource. In order to control authorization, the TOE also keeps a database of access rules. The access rules are connected to the authorization system so that TOE user's access to resources can be controlled. Some access rules are already built-in in the TOE but they can be changed by the relying application.

Additionally, access control is also enforced through role separation, based on a combination of access rules.

## 3.7 Token Management

The private keys used by the TOE to perform cryptographic operations are kept inside tokens, which can be activated/deactivated in order to allow/prevent using the keys they hold.

## 3.8 Key Generation and Management

The TOE is able to generate key pairs for its own usage, kept inside a cryptographic module.

## 3.9 Backup of TOE Data

The various security functions of the TOE manage different types of data, including configuration data and recoverable key pairs. Disaster recovery procedures require that it must be possible to restore a security system in a determined state recovered from existing backups. Therefore, the backup functions of the TOE make it possible not only to perform secure backup operations, but also to restore the contents of those backups at another installation. The security functions of the backup makes it possible to ensure that the backup, and thus the restored system, cannot be compromised and that confidential data is not revealed.

Additionally, and given its dependency towards CESeCore, the backups generated by the TOE also include the information needed to recover CESeCore's state.

## 3.10 Certificate Authority Management

As an enterprise class Certificate Authority software, EJBCA allows the configuration of several CAs in the same TOE instance, providing a flexible solution for organizations that need to deploy more than one CA (e.g. one CA for issuing signature certificates, another to issue SSL certificates, etc.).

## 3.11 Key Recovery

The TOE is able to generate extractable key pairs for use in encryption certificates that, in case of loss of the respective encryption key, may be recovered by a TOE Officer. While kept by the TOE, these key pairs (and respective pass phrases) are encrypted and stored in the database.

## 3.12 Profile Management

Since the contents of the X.509 certificates and CRLs can be extended to include additional relevant information, the TOE supports the configuration of profiles that define the fields and default values that should be included in the issued certificates and CRLs. For each existing CA, it is possible to configure one CRL profile and one or more certificate profiles.

## 3.13 User Registration and Management

Issued digital certificates are associated to users, created during the enrollment process. In addition to collect his certificate(s), authenticated users can regain access to his key pairs kept by the TOE for key recovery purposes (after approval by a TOE user).

Additionally, certain users can be assigned one or more roles that grant them access to specific features of the TOE, like certificate suspension/revocation/activation, key recovery approval, configuration, administration, or user management.

## 3.14 Certificate and CRL Publishing

In order to make them widely available to external users and applications, the TOE supports the configuration of domain-specific publishers that are responsible to relay issued digital certificates and CRLs to third-party repositories where they can be accessed or used.

## 3.15 Certificate and CRL Retrieval

Besides being able to publish them in the relevant repositories, the TOE also allows the lookup and retrieval of specific certificates and CRLs.

# 4 Assumptions and Clarification of Scope

The Security Target contains eight threats, one Organisational Security Policy (OSP), and three assumptions, which have been considered during the evaluation.

The threats, OSPs, and assumptions are described in the [ST], chapter 3.

# 5 Architectural Information

The TOE is the java software component EJBCA, containing the security library CESeCore.

The operational environment must provide a Java VM, an EJB application server, a relational database, an operating system, and server hardware.

Section 1.4 in the [ST] provides further details.

# 6 Documentation

Guidance to set up the TOE in the evaluated configuration is provided in:

EJBCA Common Criteria Guidance Supplement [CCG], PrimeKey Solutions AB, 2021-03-02, version 1.1

Other, more general, guidance is avilable from:

https://doc.primekey.com/ejbca

# 7 IT Product Testing

## 7.1 Evaluator Testing

All tests required by the Protection Profile for Certificate Authorities were performed on an earlier version of the TOE. A few test cases failed and were fixed, either in the guidance documentation or with code changes, in version 7.4.1.1. For the updated version a representative selection of 22% of the test cases, including all previously failed test cases, were re-run sucessfully in September 2020.

The test environment includes the following supporting products:

Application server: Wildfly 14.0.1

Java VM: Oracle OpenJDK 1.8.0_242

Database: MariaDB 10.2.13

Operating system: CentOS Linux 7 with kernel 3.10.0-1062.9.1.el7

HSM: Utimaco CryptoServer SE52

## 7.2 Penetration Testing

The vulnerability assessment did not reveal any potential vulnerabilities, but the independent test suite contains numerous negative tests.

# 8 Evaluated Configuration

The guidance in [CCG] contains instructions how to set up the TOE in the evaluated configuration.

In the evaluated configuration, the environment provides the following software:

| | |
|---|---|
| Application server: | Wildfly 14.0.1 |
| Java virtual machine | Oracle OpenJDK 1.8.0:242 |
| Relational database | MariaDB 10.2.13 |
| Operating system | CentOS Linux 7 (kernel 3.10.0-1062.9.1.el7) |

The environment also shall provide the following cryptographic hardware:

| | |
|---|---|
| HSM | Utimaco CryptoServer SE52 |

# 9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] and in accordance with [PPCA].

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC] and the [PPCA].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

| *Assurance Class/Family* | *Short name* | *Verdict* |
|---|---|---|
| Development | ADV | PASS |
| Functional Specification | ADV_FSP.1 | PASS |
| Guidance Documents | AGD | PASS |
| Operational User Guidance | AGD_OPE.1 | PASS |
| Preparative Procedures | AGD_PRE.1 | PASS |
| Life-cycle Support | ALC | PASS |
| CM Capabilities | ALC_CMC.1 | PASS |
| CM Scope | ALC_CMS.1 | PASS |
| Security Target Evaluation | ASE | PASS |
| ST Introduction | ASE_INT.1 | PASS |
| Conformance Claims | ASE_CCL.1 | PASS |
| Security Problem Definition | ASE_SPD.1 | PASS |
| Security Objectives | ASE_OBJ.1 | PASS |
| Extended Components Definition | ASE_ECD.1 | PASS |
| Security Requirements | ASE_REQ.1 | PASS |
| TOE Summary Specification | ASE_TSS.1 | PASS |
| Tests | ATE | PP compliant |
| Independent Testing | ATE_IND.1 | PP compliant |
| Vulnerability Assessment | AVA | PASS |
| Vulnerability Analysis | AVA_VAN.1 | PASS |

# 10 Evaluator Comments and Recommendations

None.

# 11 Glossary

| | |
|---|---|
| CA | Certificate Authority |
| CC | Common Criteria |
| CEM | Common Methodology for Information Technology Security |
| CRL | Certificate Revocation List |
| CRMF | Certificate Request Message Format |
| EJB | Enterprise Java Bean |
| HSM | High Security Module |
| ITSEF | IT Security Evaluation Facility |
| JEE | Java Enterprise Edition |
| OCSP | On-line Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| ST | Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation |
| TOE | Target of Evaluation |
| VM | Virtual Machine |
| X.509 | Standard for the content of certain types of electronic certificates |

# 12 Bibliography

ST Security Target for EJBCA v7.4.1, PrimeKey Solutions AB, 2021-03-29, document version 1.2

CCG EJBCA Common Criteria Guidance Supplement, PrimeKey Solutions AB, 2021-03-02, version 1.1

PPCA Protection Profile for Certification Authorities, NIAP, 2017-12-01, document version 2.1

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2019-11-30, document version 32.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2020-11-03, document version 10.0

# Appendix A Scheme Versions

## A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was entered into the registry 2019-05-10:

| | |
|---|---|
| QMS 1.22.2 | valid from 2019-05-02 |
| QMS 1.22.3 | valid from 2019-05-20 |
| QMS 1.23 | valid from 2019-10-14 |
| QMS 1.23 | valid from 2019-10-14 |
| QMS 1.23.1 | valid from 2020-03-06 |
| QMS 1.23.2 | valid from 2020-05-11 |
| QMS 1.24 | valid from 2020-11-19 |
| QMS 1.24.1 | valid from 2020-12-03 |

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.24.1”.

The certifier concluded that, from QMS 1.22.2 to the current QMS 1.24.1, there are no changes with impact on the result of the certification

## A.2 Scheme Notes

The following Scheme Notes has been considered during the evaluation:

Scheme Note 15 Testing, v5.0:
Clarifications on testing.

Scheme Note 18 Highlighted requirements on the Security Target, v3.0:
Clarifications concerning requirements on the Security Target.

Scheme Note 22 Vulnerability assessment, v3.0:
Clarifications regarding the vulnerability assessment.
Mandatory update of the vulnerability database search, if older than 30 days
at the end of the evaluation.