EJBCA
PKI BY PRIMEKEY

Security Target for EJBCA v5.0.4

Document ID :	**D10.0**
Document Name :	**Security Target for EJBCA v5.0.4**
Status :	**Draft**
Dissemination Level :	**Public**
Document Version :	**1.2**
Version Date :	**02-07-12**
Author(s):	**Tomas Gustavsson, Pedro Borges, Nuno Ponte, Nuno Santos, Hasan Subaşi**

Abstract: This document defines the Security Target according to which the EJBCA product will be EAL 4+ Common Criteria evaluated.

History

Version	Date	Modification reason	Modified by	Approved by
0.1	26-12-2010	Initial draft	Tomas Gustavsson	Admir Abdurahmanovic
0.2	02-03-2011	Include comments received from Oppida and internal reviewers	Pedro Borges	Admir Abdurahmanovic
1.0	28-03-2012	Include comments received from Oppida	Pedro Borges	Admir Abdurahmanovic
1.1	29-04-2012	Perform changes requested by the certifier	Pedro Borges	Admir Abdurahmanovic
1.2	02-07-2012	Perform changes requested by the certifier	Pedro Borges	Admir Abdurahmanovic

Table of contents

List of figures

List of tables

1 Introduction

1.1 Description of EJBCA

EJBCA is an enterprise class PKI[1] Certificate Authority built on JEE technology, allowing the issuance and life cycle management of public key certificates compliant with the X.509 v3 [4] and CVC BSI TR-03110 [3] standards. Additionally, EJBCA can also be set up a CA independent, high performance, highly available OCSP responder service.

As the most flexible CA on the market, EJBCA PKI is the leading open source enterprise PKI. Designed to be a robust, high performance, platform independent, flexible and component based CA to be used stand-alone or integrated in other JEE applications.

Functionalities offered by EJBCA can be used through web interfaces (by end users or TOE users) or APIs (by relying applications that integrate it). More information can be found at the project website [6].

The rest of this document describes the EJBCA Target of Evaluation (TOE) that is in the scope of this Common Criteria evaluation and the corresponding Security Target (ST).

1.2 TOE Reference

ST Title	Security Target for EJBCA v5.0.4
ST Reference	D10.0
TOE Identification	EJBCA v5.0.4
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 3)
PP Conformance	Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001
Assurance Level	Evaluation Assurance Level 4 augmented with `ALC_FLR.2`

1.3 TOE Overview

The usage of Public-key Cryptography relies on the usage of digital certificates, in order to authenticate relying parties. However, given the complex nature of the issuance and management of the digital certificates lifecycle, organizations that want to carry out those types of operations usually need to use Certificate Authority applications

As an enterprise class PKI Certificate Authority, EJBCA is compliant with the X.509 v3 [4] and CVC BSI TR-03110 [3] standards, allowing the issuance of public key certificates for different purposes, such as:

- Strong authentication for users accessing your intranet/extranet/internet resources;
- Secure communication with SSL servers and SSL clients;

[1] Public Key Infrastructure.

- Smart card logon to Windows and/or Linux;
- Signing and encrypting email;
- VPN connections by issuing certificates to your VPN routers such as OpenVPN, Cisco, Juniper etc.;
- Client VPN access with certificates in users VPN clients;
- Single sign-on by using a single certificate to secure logon to Web applications;
- Creating signed documents;
- Issue citizen certificates for access to government resources, used in passports etc.;
- Create CVCAs and DVs and issue CV certificates (CVC) to Document Verifiers and Inspection Systems for EU EAC ePassports.

Additionally, and besides being robust, highly flexible and customizable, the TOE also can act as a CA independent OCSP responder service.

Technology wise, given that it is composed by a set of Java Enterprise Edition (JEE) modules, EJBCA is platform independent.

Regarding its usage, EJBCA is deployed as a regular JEE application, making most of its functionalities available through a set of customizable Web interfaces. However, applications that need to integrate or build upon EJBCA's services in order to deliver higher level features may either use its APIs or, given the TOE's open-source nature, change it to fit their specific needs.

Figure 1 depicts the layered architecture that can be observed in a system where the TOE is deployed.

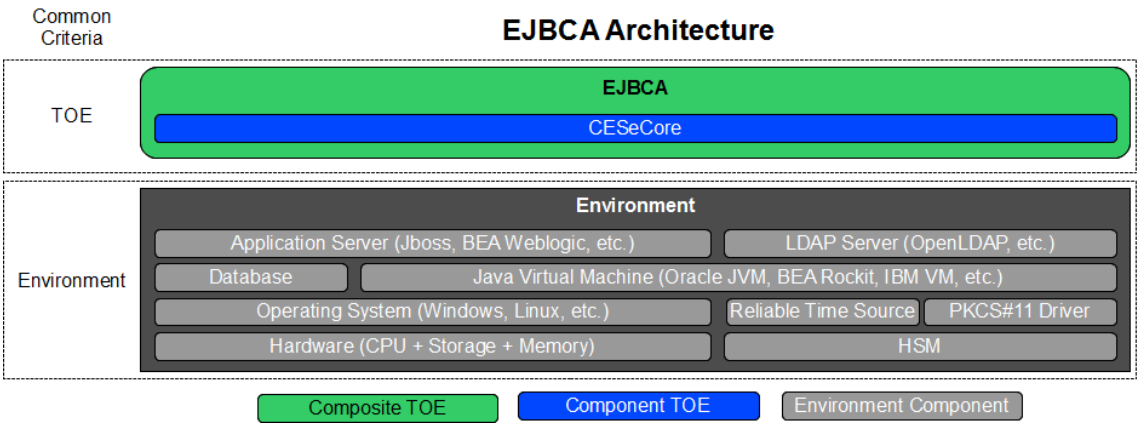

Figure 1: EJBCA Architecture

1.3.1 Components

The usage of EJBCA relies not only on its implementation, but also on several other additional components described in the following subsections.

1.3.1.1 EJBCA

The EJBCA component consists of a set of Java classes that provide such functionalities as:

- Create digital certificates and CRLs;
- OCSP support;
- Certificate Authority management;
- Key recovery;
- Profile management;
- User registration and management;
- Certificate and CRL publishing;
- Certificate and CRL retrieval;
- Backup of TOE data.

In order to achieve some of its goals and deliver the above mentioned features, the TOE relies on the usage of CESeCore, described in the following section.

1.3.1.2 CESeCore

CESeCore is a CC EAL4+ evaluated product (compliant with the CIMC SL3 PP) that implements security functionalities needed to create PKI-based applications, available through a set of APIs (either Java APIs or JEE specific APIs).

For more information about the CESeCore, please visit the project website (https://www.cesecore.eu).

1.3.1.3 Configuration artifacts

Configuration artifacts are basic TOE configuration items provided by the TOE users. The configuration artifacts define details on how the specific instance of the TOE works and consist of key-value pairs, stored in a configuration file or in a database. Examples of configuration artifacts are PKCS#11 library path for the hardware security module (HSM), key labels for cryptographic keys and modes for secure audit.

However, in order to run in an CC-certified configuration certain restrictions on the configuration artifacts may apply.

1.3.1.4 Java Virtual Machine

EJBCA is developed in the Java programming language and, as such, runs in a Java Virtual Machine (JVM). Additionally, since the JVM specifications are public, it can be implemented by independent vendors.

1.3.1.5 Application server

EJBCA can be (optionally) deployed on an JEE 5 compliant application server, which provides a number of resources and services to EJBCA, namely:

- Database connectivity services (e.g. object mappings and connection pooling);
- Component creation and management (e.g. session bean pooling and life-cycle management);
- Communication interfaces (e.g. HTTP and JEE).

These resources and services not only make development and maintenance more efficient, but also enable high performance, scalability and availability.

1.3.1.6 Database

Data persisted by EJBCA is handled by a standard relational database, where the following information is kept:

- Key pairs[2] for key recovery, along with their respective passphrase;
- Publisher configuration;
- End user registration data, along with their respective passwords;
- Service configuration;
- Approval information (events waiting for approval by TOE users);
- CA configuration (additional to the one kept in CESeCore's database);
- System configuration;
- End user hard token information and issuer configuration (e.g. information about smartcards issued to end users).

Additionally, EJBCA relies on additional information kept in the CESeCore's relational database, namely:

- Key pairs[3] and references to key pairs;
- Certificates and CRLs;
- Basic CA configuration;
- Audit logs of all security relevant operations;
- Authentication data, such as TOE user information;
- Authorization data, such as which TOE user is authorized to which resources.

EJBCA enforces access control and maintains integrity of the data for which it is required.

1.3.1.7 Cryptographic module

All cryptographic operations performed at the request of the TOE should take place in FIPS 140-1 (or higher) validated cryptographic modules, either in software or in a hardware (HSM). The interaction with the cryptographic module is performed through a standard PKCS#11 library provided by the respective vendor.

[2] Where the private key is encrypted.

[3] Where the private key is encrypted.

However, the level of FIPS 140-1 (or higher) required varies according to the type of operation performed, as depicted in Table 1.

Category of Use	FIPS 140-1[4] Level Required
Certificate and Status Signing:	
- single party signature	3
- multiparty signature	2
Integrity or Approval Authentication:	2
General Authentication	2
Long Term Private Key Protection	3
Long Term Confidentiality	2
Short Term Private key Protection	2
Short Term Confidentiality	1
Hash Generation	1
Signature Verification	1

Table 1: FIPS 140-1 (or higher) Level for Validated Cryptographic Module

1.4 TOE Description

The EJBCA TOE comprises all the security functions required by a Certification Authority, allowing the issuance of public key certificates and CRLs, the lifecycle management of those certificates and capability to provide realtime information about their revocation status, according to the OCSP protocol. Additionally, the TOE depends on several external components for it's operation.

1.4.1 Security functions

Though the security functions can be used independently of each other, the implementation of some functions depends on others. For example, the *secure audit* security function depends on *data integrity protection* and *electronic signatures creation*.

1.4.1.1 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 FIPS 140-1 (or higher) validated cryptographic modules, both using software or hardware (such as HSMs and smart cards).

[4]Or higher.

1.4.1.2 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).

1.4.1.3 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 realtime revocation status information.

1.4.1.4 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.

1.4.1.5 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 that meets CWA 14167-1 requirements for secure audit.

1.4.1.6 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.

1.4.1.7 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.

1.4.1.8 Key generation and management

The TOE is able to generate key pairs for its own usage, kept inside a FIPS 140-1 (or higher) validated cryptographic module.

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

1.4.1.10 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.).

1.4.1.11 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 passphrases) are encrypted and stored in the database.

1.4.1.12 Profile management

Since, according to [1], 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.

1.4.1.13 User registration and management

Issued digital certificates are associated to users, created during the enrolment 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.

1.4.1.14 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.

1.4.1.15 Certificate and CRL retrieval

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

1.4.2 TOE boundary

As illustrated by Figure 2, the TOE includes:

- The EJBCA component;
- The CESeCore library and its configuration files.

Excluded from the TOE is:

- Hardware and operating system platform (abstract machine);
- Application server and execution environment;
- Hardware security module (HSM);
- Database engine.

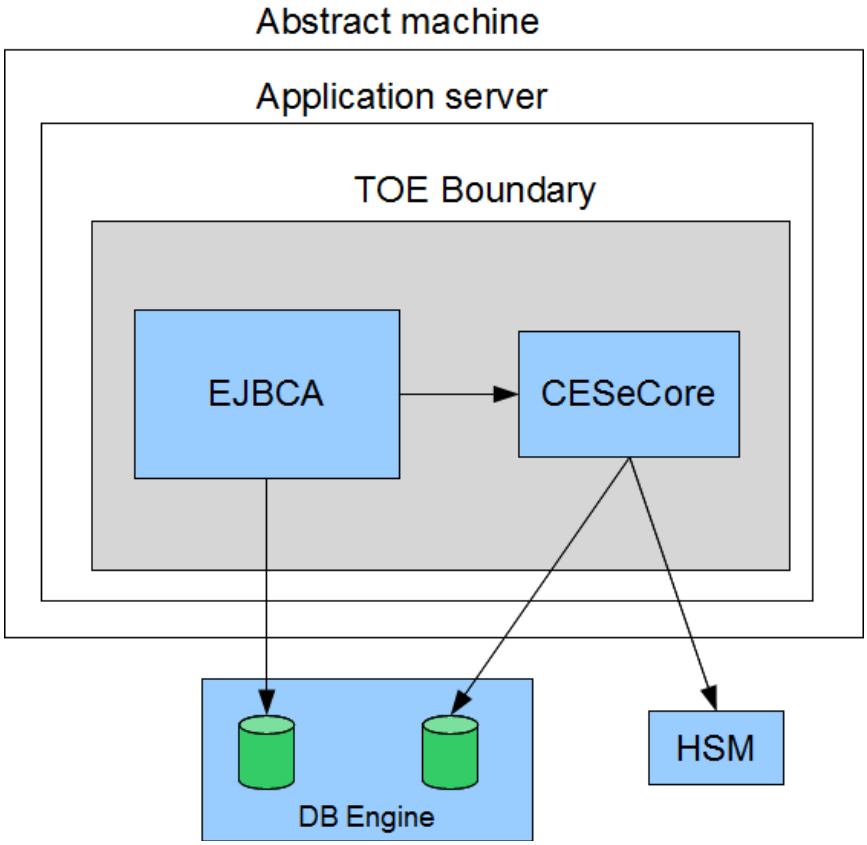

Figure 2: TOE boundary

The rationale for excluding components from the TOE is elaborated in the following sections.

1.4.2.1 Hardware and operating system platform

EJBCA is independent of hardware and operating system and is expected to work on any platform that provides a reliable time source and is capable of running a JVM. The TOE security functions do not depend on the security functions of the underlying platform.

1.4.2.2 Application server and execution environment

EJBCA is independent of the application server and execution environment where it is used, as long as the execution environment is a compliant Java VM and the application server implements the Enterprise Java Beans (EJB) standard. The TOE security functions do not depend on the security functions of the application server or execution environment.

1.4.2.3 Hardware security module

The HSM supplies its own set of security functions and is FIPS[5] 140-1 (or higher) evaluated and, as such, is regarded as a trusted device.

1.4.2.4 Database

All connections to the database are performed using the appropriate JDBC[6] drivers. Given that it is located in the same machine as the TOE, no specific mechanisms are needed to ensure the integrity and confidentiality of the information transferred to/from the database by the TOE.

1.4.3 TOE physical scope

By running on an application server inside a JVM, the TOE is independent of the underlying hardware and software platforms. Therefore, as long as a fully compliant JVM is available and may be used on such a platform, it should be possible to use the TOE.

Nevertheless, since there are several versions of the JVM specification, we have chosen to explicitly support Oracle JDK 1.6.0_27 (64 bit) in Linux and Oracle JDK 1.6.0_24 (32 bit) in Windows.

To perform the evaluation process we limit the hardware platform to the the most commonly used: Generic x86 32 or 64 bit server.

Moreover, and though it should be possible to deploy and use it in any Linux (32 or 64 bit) or Windows (32 bit) operating system, the TOE has been successfully tested in Red Hat Enterprise Linux 5.5 x86 (64 bit) and Windows Server 2008 (32 bit).

Regarding the database, any SQL[7] compliant database can be used, with successful tests already performed in the following versions:

- MySQL 5.1;
- PostgreSQL 9.0.

Additionally, EJBCA should run on any JEE 5 certified application server, having been successfully tested in the following:

- JBoss 5.1.0;
- Glassfish v2.

Finally, using the PKCS#11 interface makes it possible to use virtually any of the FIPS 140-1 (or higher) evaluated HSMs available on the market, with SafeNet Luna SA and Utimaco CryptoServer having been successfully tested.

[5] Federal Information Processing Standard.

[6] Java Database Connectivity.

[7] Structured Query Language.

2 Conformance Claims

2.1 CC Conformance Claim

The TOE conforms to:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 3), part 2 extended;
- Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 3), part 3 conformant;
- Evaluation Assurance Level 4 augmented with the `ALC_FLR.2` component.

2.2 PP conformance claim

As previously mentioned in this ST, EJBCA is demonstrably conformed to the following Protection Profiles (PP):

- Certificate Issuing and Management Components (CIMC) Security Level 3 PP, version 1.0, October 31, 2001.

2.3 Conformance Rationale

All of the assumptions, threats, policies, objectives and security requirements defined for CIMC PP Security Level 3 have been reproduced in this ST and adapted for CC v3.1. No additional assumption, threat, policy, objective or security requirement has been used.

All operations performed on the IT security requirements are within the bounds set by the CIMC PP for Security Level 3. Assignment and selection operations on security requirements are indicated in Section 6.

3 Security problem definition

3.1 Introduction

The security problem definition is extracted from the CIMC family of protection profiles and includes the following parts:

- Threats;
- Organizational security policies;
- Secure usage assumptions.

3.2 Threats

The threats are organized in four categories: authorized users, system, cryptography, and external attacks.

3.2.1 Authorized users

T.Administrative errors of omission	Administrators, Operators, Officers or Auditors fail to perform some function essential to security.
T.User abuses authorization to collect and/or send data	User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.
T.User error makes data inaccessible	User accidentally deletes user data rendering user data inaccessible.
T.Administrators, Operators, Officers and Auditors commit errors or hostile actions	An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.

3.2.2 System

T.Critical system component fails	Failure of one or more system components results in the loss of system critical functionality.
T.Malicious code exploitation	An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.
T.Message content modification	A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.
T.Flawed code	A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

3.2.3 Cryptography

T.Disclosure of private and secret keys	A private or secret key is improperly disclosed.
T.Modification of private/secret keys	A secret/private key is modified.
T.Sender denies sending information	The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

3.2.4 External attacks

T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.
T.Hacker physical access	A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

3.3 Organisational Security Policies

P.Authorized use of information	Information shall be used only for its authorized purpose(s).
P.Cryptography	FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

3.4 Assumptions

The usage assumptions are organized in three categories: personnel, connectivity and physical.

3.4.1 Personnel

Personnel assumptions about administrators and users of the system, as well as any threat agent.

A.Auditors Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Auditors.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories and variations) (Note: this assumption is not applicable to biometric authentication data.)
A.Competent Administrators, Operators, Officers and Auditors	Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
A.CPS	All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed e.g., job termination, change in responsibility).
A.Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity.
A.Notify Authorities of Security Issues	Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Social Engineering Training	General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
A.Cooperative Users	Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.

3.4.2 Connectivity

Connectivity assumptions about other IT systems that are necessary for the secure operations of the TOE.

A.Operating System	The operating system has been selected to provide the functions required by this ST to counter the perceived threats for the the CIMC Security Level 3 PP.

3.4.3 Physical

Physical assumptions about the physical location of the TOE or any attached peripheral devices.

A.Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

4 Security objectives

The security objectives are based on the CIMC family of protection profiles and include the following parts:

- High-level solution;
- Security objectives for the TOE;
- Security objectives for the operational environment;
- Security objectives for both the TOE and operational environment;
- Security objectives rationale.

4.1 High-level solution

In general terms, this TOE aims to ensure:

- That all information generated by the system (e.g. certificates, CRLs and status information) is trustworthy;
- Protection against unknown/malicious communication traffic;
- The preservation and (if needed) recovery of a coherent and viable system state, despite component failures or security incidents (e.g. malicious code);
- Non-repudiation and auditability of relevant events;
- Control over its development and deployment, by implementing a configuration management plan;
- Confidentiality of sensitive information received or generated by the TOE;
- The protection of system and data integrity (including backup information), allowing prompt detection of unauthorized modification;
- An appropriate access control policy that restricts actions of unauthenticated users, fosters segregation of duties and grants only the essential access rights required by each role;
- The sequencing of events through the usage of reliable time stamps;
- Tamper protection of audit records.

4.2 Security objectives for the TOE

The objectives are organized in four categories: authorized users, system, cryptography, and external attacks.

4.2.1 Authorized users

O.Certificates	The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.

4.2.2 System

O.Preservation/trusted recovery of secure state	Preserve the secure state of the system in the event of a secure component failure and/or recover to a secure state.
O.Sufficient backup storage and effective restoration	Provide sufficient backup storage and effective restoration to ensure that the system can be recreated.

4.2.3 Cryptography

O.Non-repudiation	Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message. (Security Levels 3 and 4) .

4.2.4 External attacks

O.Control unknown source communication traffic	Control (e.g., reroute or discard) communication traffic from an unknown source to prevent potential damage.

4.3 Security objectives for the operational environment

4.3.1 Non-IT security objectives for the environment

O.Administrators, Operators, Officers and Auditors guidance documentation	Deter Administrator, Operator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.
O.Auditors Review Audit Logs	Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.
O.Authentication Data Management	Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories and variations) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.).
O.Communications Protection	Protect the system against a physical attack on the communications capability by providing adequate physical security.
O.Competent Administrators, Operators, Officers and Auditors	Provide capable management of the TOE by assigning competent Administrators, Operators, Officers and Auditors to manage the TOE and the security of the information it contains.

O.CPS	All Administrators, Operators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.
O.Disposal of Authentication Data	Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).
O.Installation	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.
O.Malicious Code Not Signed	Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.
O.Notify Authorities of Security Issues	Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
O.Physical Protection	Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.
O.Social Engineering Training	Provide training for general users, Administrators, Operators, Officers and Auditors in techniques to thwart social engineering attacks.
O.Cooperative Users	Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE. (Security Levels 1 – 3).
O.Lifecycle security	Provide tools and techniques used during the development phase to ensure security is designed into EJBCA. Detect and resolve flaws during the operational phase. (Security Levels 2 – 4)
O.Repair identified security flaws	The vendor repairs security flaws that have been identified by a user. (Security Levels 2 – 4)
O.Require inspection for downloads	Require inspection of downloads/transfers.
O.User authorization management	Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.

4.3.2 IT security objectives for the environment

O.Cryptographic functions	The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. (Validated is defined as FIPS 140-1 or higher validated.)
O.Operating System	The operating system used is validated to provide adequate security, including domain separation and non-bypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology (available at http://checklists.nist.gov).
O.Periodically check integrity	Provide periodic integrity checks on both system and software.
O.Security roles	Maintain security-relevant roles and the association of users with those roles.
O.Validation of security function	Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.
O.Trusted Path	Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities. (Security Levels 3 and 4)

4.4 Security objectives for both the TOE and the operational environment

This section specifies the security objectives that are jointly addressed by the TOE and the environment.

O.Configuration Management	Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.
O.Data import/export	Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
O.Detect modifications of firmware, software, and backup data	Provide integrity protection to detect modifications to firmware, software, and backup data.
O.Individual accountability and audit records	Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.

O.Integrity protection of user data and software	Provide appropriate integrity protection for user data and software.
O.Limitation of administrative access	Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.
O.Maintain user attributes	Maintain a set of security attributes (which may include role membership and access privileges) associated with individual users. This is in addition to user identity.
O.Manage behavior of security functions	Provide management functions to configure, operate, and maintain the security mechanisms.
O.Object and data recovery free from malicious code	Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.
O.Procedures for preventing malicious code	Incorporate malicious code prevention procedures and mechanisms.
O.Protect stored audit records	Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.
O.Protect user and TSF data during internal transfer	Ensure the integrity of user and TSF data transferred internally within the system.
O.Respond to possible loss of stored audit records	Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.
O.Restrict actions before authentication	Restrict the actions a user may perform before the TOE authenticates the identity of the user.
O.Security-relevant configuration management	Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
O.Time stamps	Provide time stamps to ensure that the sequencing of events can be verified.
O.React to detected attacks	Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent. (Security Levels 2 - 4)

Common Criteria version 3.1 requires the strict separation between security objectives for the TOE and security objectives for the operational environment.

This section is directly extracted from the CIMC protection profile and is however considered as acceptable because:

- separation between security requirements for the TOE and security requirements for the environment is clearly defined in the rationale for objectives coverage (section 6.3);
- security requirements statement is the basis for CC 3.1 evaluation tasks (e.g. for ADV class evaluation workunits).

4.5 Security objectives rationale

The Security Problem Definition and the Security Objectives are identical to the CIMC protection profile.

5 Extended components definition

Extended components have been defined in the CIMC Protection Profile.

Extended security requirements are explicitly identified in Table 2, and thoroughly described in the PP.

Extended Security Requirements	CIMC Page Reference
FCO_NRO_CIMC.3	49
FCO_NRO_CIMC.4	51
FCS_CKM_CIMC.5	53
FDP_ACF_CIMC.2	52
FDP_ACF_CIMC.3	53
FDP_CIMC_BKP.1	44
FDP_CIMC_BKP.2	44
FDP_CIMC_CER.1	58
FDP_CIMC_CRL.1	59
FDP_CIMC_CSE.1	51
FDP_CIMC_OCSP.1	59
FDP_ETC_CIMC.5	54
FDP_SDI_CIMC.3	52
FMT_MOF_CIMC.3	55
FMT_MOF_CIMC.5	57
FMT_MOF_CIMC.6	57
FMT_MTD_CIMC.4	52
FMT_MTD_CIMC.5	53
FMT_MTD_CIMC.7	54
FPT_CIMC_TSP.1	41

Table 2: Extended Components Definition

6 Security requirements

The security requirements are based on the CIMC family of protection profiles and include the following parts:

- Security functional requirements (SFRs);
- Security assurance requirements (SARs);
- Security requirements rationale.

6.1 Security functional requirements

Table 3 lists all the TOE's functional security requirements.

Security Functional Requirement	CIMC PP Section	CC Part 2 Extended
FAU_GEN.1 Audit data generation	6.1 Security Audit	
FAU_GEN.2 User identity association	6.1 Security Audit	
FAU_SEL.1 Selective audit	6.1 Security Audit	
FAU_STG.1 Protected audit trail storage	6.1 Security Audit	
FAU_STG.4 Prevention of audit data loss	6.1 Security Audit	
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	6.6 Remote Data Entry and Export	yes
FCO_NRO_CIMC.4 Advanced verification of origin	6.6 Remote Data Entry and Export	yes
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	6.7 Key Management	yes
FDP_ACC.1 Subset access control	6.4 Access Control	
FDP_ACF.1 Security attribute based access control	6.4 Access Control	
FDP_ACF_CIMC.2 User private key confidentiality protection	6.7 Key Management	yes
FDP_ACF_CIMC.3 User secret key confidentiality protection	6.7 Key Management	yes
FDP_CIMC_BKP.1 CIMC backup and recovery	6.3 Backup and Recovery	yes
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	6.3 Backup and Recovery	yes

FDP_CIMC_CER.1 Certificate Generation	6.11 Certificate Registration	yes
FDP_CIMC_CRL.1 Certificate Revocation	6.12 Certificate Revocation	yes
FDP_CIMC_CSE.1 Certificate status export	6.6 Remote Data Entry and Export	yes
FDP_CIMC_OCSP.1 Basic Response Validation	6.12 Certificate Revocation	yes
FDP_ETC_CIMC.5 Extended user private and secret key export	6.7 Key Management	yes
FDP_ITT.1 Basic internal transfer protection (iteration 1 and 2)	6.6 Remote Data Entry and Export	
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	6.7 Key Management	yes
FDP_UCT.1 Basic data exchange confidentiality	6.6 Remote Data Entry and Export	
FIA_UAU.1 Timing of authentication	6.5 Identification and Authentication	
FIA_UID.1 Timing of identification	6.5 Identification and Authentication	
FIA_USB.1 User-subject binding	6.5 Identification and Authentication	
FMT_MOF.1 Management of security functions behaviour	6.2 Roles	
FMT_MOF_CIMC.3 Extended certificate profile management	6.8 Certificate Profile Management	yes
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	6.9 Certificate Revocation List Profile Management	yes
FMT_MOF_CIMC.6 OCSP Profile Management	6.10 Online Certificate Status Protocol (OCSP) Profile Management	yes
FMT_MTD_CIMC.4 TSF private key confidentiality protection	6.7 Key Management	yes
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	6.7 Key Management	yes
FMT_MTD_CIMC.7 Extended TSF private and secret key export	6.7 Key Management	yes
FPT_CIMC_TSP.1 Audit log signing event	6.1 Security Audit	yes

FPT_ITC.1 Inter-TSF confidentiality during transmission	6.6 Remote Data Entry and Export	
FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1 and 2)	6.6 Remote Data Entry and Export	
FPT_STM.1 Reliable time stamps	6.1 Security Audit	

Table 3: TOE Functional Security Requirements

6.1.1 Security Audit

Table 4 describes the SFRs related to security audit.

FAU_GEN.1 Audit data generation	
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the minimum level of audit; and c) The events listed in Table 5 below.
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, the information specified in the Additional Details column in Table 5 below. Additionally, the audit shall not include plaintext private or secret keys or other critical security parameters.
FAU_GEN.2 User identity association	
FAU_GEN.2.1	For audit events resulting from the actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
FAU_SEL.1 Selective audit	
FAU_SEL.1.1	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) object identity, subject identity and event type; b) date.
FAU_STG.1 Protected audit trail storage	
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to detect unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss	
FAU_STG.4.1	The TSF shall prevent audited events, except those taken by the Auditor and no other actions if the audit trail is full.
FPT_CIMC_TSP.1 Audit log signing event	
FPT_CIMC_TSP.1.1	The TSF shall periodically create an audit log signing event in which it computes a digital signature, keyed hash, or authentication code over the entries in the audit log.
FPT_CIMC_TSP.1.2	The digital signature, keyed hash, or authentication code shall be computed over, at least, every entry that has been added to the audit log since the previous audit log signing event and the digital signature, keyed hash, or authentication code from the previous audit log signed event.
FPT_CIMC_TSP.1.3	The specified frequency at which the audit log signing event occurs shall be configurable.
FPT_CIMC_TSP.1.4	The digital signature, keyed hash, or authentication code from the audit log signing event shall be included in the audit log.
FPT_STM.1 Reliable time stamps	
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Table 4: TOE Functional Security Requirements – Security Audit

Table 5 describes the auditable events and respective data.

Section/Function	Component	Event	Additional Details
6.1 Security Audit	FAU_GEN.1 Audit data generation	Any changes to the audit parameters, e.g., audit frequency, type of event audited	
		Any attempt to delete the audit log	
	FPT_CIMC_TSP.1 Audit log signing event	Audit log signing event	Digital signature, keyed hash, or authentication code shall be included in the audit log.
6.6 Remote Data Entry and Export		All security-relevant data that is entered in the system (local data entry)	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an “accept” button). This shall be included with the accepted data.

Section/Function	Component	Event	Additional Details
		All security-relevant messages that are received by the system (remote data entry)	
		All successful and unsuccessful requests for confidential and security-relevant information (Security Levels 2, 3, 4)	
5.6 Key Management	FCS_CKM.1 Cryptographic Key Generation	Whenever the TSF requests generation of a cryptographic key (except single session or one-time use symmetric keys)	The public component of any asymmetric key pair generated
		The loading of Component private keys[8]	
6.7 Key Management		All access to certificate subject private keys retained within the TOE for key recovery purposes	
		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
		The manual entry of secret keys used for authentication (Security Levels 3 and 4)	
	FDP_ETC_CIMC.4 User private and secret key export; FMT_MTD_CIMC.6 TSF private and secret key export	The export of private and secret keys (except keys used for a single session or message)	
6.11 Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
Certificate Status Change Approval		All requests to change the status of a certificate	Whether the request was accepted or rejected.
CIMC Configuration		Any security-relevant changes to the configuration of the TSF	

[8] Audit log not generated since this operation is not supported by the TOE.

Section/Function	Component	Event	Additional Details
6.8 Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	All changes to the certificate profile	The changes made to the profile
Revocation Profile Management		All changes to the revocation profile	The changes made to the profile
6.9 Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile
6.10 Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP Profile Management	All changes to the OCSP profile	The changes made to the profile
Minimal Events to be logged (as defined in CC – Part 2)	FAU_SEL.1 Selective Audit	All modifications to the audit configuration that occur while the audit collection functions are operating	
	FDP_ACF.1 Security attribute based access control	Successful requests to perform an operation on an object covered by the SFP	
	FDP_UCT.1 Basic data exchange confidentiality	The identity of any user or subject using the data exchange mechanisms	
	FIA_UAU.1 Timing of authentication	Unsuccessful use of the authentication mechanism	
	FIA_UID.1 Timing of identification	Unsuccessful use of the user identification mechanism, including the user identity provided	
	FIA_USB.1 User-subject binding	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	
	FPT_STM.1 Reliable time stamps	Changes to the time	Since this takes place at the operating system level, the TOE is not able to detect and log this type of events.

Table 5: Auditable Events and Audit Data

6.1.2 Roles

Table 6 describes the SFRs related to role management.

FMT_MOF.1 Management of security functions behaviour	
FMT_MOF.1.1	The TSF shall restrict the ability to modify the behavior of the functions listed in Table 7 to the authorized roles as specified in Table 7.

Table 6: TOE Functional Security Requirements – Roles

Table 7 describes the roles authorised to manage the security functions behaviour.

Section/Function	Component	Function/Authorized Role
6.1 Security Audit		The capability to configure the audit parameters shall be restricted to Administrators.
		The capability to change the frequency of the audit log signing event shall be restricted to Administrators. (Security Levels 2-4).
6.3 Backup and Recovery		The capability to configure the backup parameters shall be restricted to Administrators.
6.11 Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers.
		If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Officers.
Data Export and Output		The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer, Auditor, or Operator. (Security Levels 3 and 4)
Certificate Status Change Approval		Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate.
		Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.
CIMC Configuration		The capability to configure any TSF functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)
6.8 Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administrators.

Section/Function	Component	Function/Authorized Role
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
6.9 Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.
6.10 Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.

Table 7: Authorized Roles for Management of Security Functions Behaviour

6.1.3 Backup and Recovery

Table 8 describes the SFRs related to the backup and recovery operations.

FDP_CIMC_BKP.1 CIMC backup and recovery	
FDP_CIMC_BKP.1.1	The TSF shall include a backup function.
FDP_CIMC_BKP.1.2	The TSF shall provide the capability to invoke the backup function on demand.
FDP_CIMC_BKP.1.3	The data stored in the system backup shall be sufficient to recreate the state of the system at the time the backup was created using only: a) a copy of the same version of the CIMC as was used to create the backup data; b) a stored copy of the backup data; c) the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and d) the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.
FDP_CIMC_BKP.1.4	The TSF shall include a recovery function that is able to restore the state of the system from a backup. In restoring the state of the system, the recovery function is only required to create an "equivalent" system state in which information about all relevant CIMC transactions has been maintained.
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	
FDP_CIMC_BKP.2.1	The backup data shall be protected against modification through the use of digital signatures, keyed hashes, or authentication codes.
FDP_CIMC_BKP.2.2	Critical security parameters and other confidential information shall be stored in encrypted form only.

Table 8: TOE Functional Security Requirements – Backup and Recovery

6.1.4 Access Control

Table 9 describes the SFRs related to access control.

FDP_ACC.1 Subset access control	
FDP_ACC.1.1	The TSF shall enforce the CIMC TOE Access Control Policy specified in appendix A on users, profiles, view, edit, create, delete, approve.
FDP_ACF.1 Security attribute based access control	
FDP_ACF.1.1	The TSF shall enforce the CIMC TOE Access Control Policy specified in appendix A to objects based on the identity of the subject and the set of roles that the subject is authorized to assume.
FDP_ACF.1.2	The TSF shall enforce the rules specified in Table 10 to determine if an operation among controlled subjects and controlled objects is allowed.
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: no additional rules.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: no additional explicit denial rules.

Table 9: TOE Functional Security Requirements – Access Control

Table 10 describes the access controls enforced by the TOE.

Section/Function	Component	Event
Certificate Request Remote and Local Data Entry		The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry		The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked.
Data Export and Output		The export or output of confidential and security-relevant data shall only be at the request of authorized users.
5.6 Key Management	FCS_CKM.1 Cryptographic Key Generation	The capability to request the generation of Component keys (used to protect data in more than a single session or message) shall be restricted to Administrators.
6.7 Key Management		The capability to request the loading of Component private keys into cryptographic modules shall be restricted to Administrators.
6.7 Key Management		At least two Officers or one Officer and an Administrator, Auditor, or Operator shall be required to request the decryption of a certificate subject private key. (Security Levels 3 and 4)
		The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures.

Section/Function	Component	Event
Trusted Public Key Entry, Deletion, and Storage		The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators.
6.7 Key Management		The capability to request the loading of CIMC secret keys into cryptographic modules shall be restricted to Administrators.
6.7 Key Management		The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators.
6.7 Key Management		The capability to export a component private key shall be restricted to Administrators.
6.7 Key Management		The export of a certificate subject private key shall require the authorization of at least two Officers or one Officer and an Administrator, Auditor, or Operator. (Security Levels 3 and 4)
Certificate Status Change Approval		Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold.
		Only Officers shall be capable of removing a certificate from on hold status.
		Only Officers shall be capable of approving the placing of a certificate on hold.
		Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate.
		Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

Table 10: Access Controls

6.1.5 Identification and Authentication

Table 11 describes the SFRs related to identification and authentication.

FIA_UAU.1 Timing of authentication	
FIA_UAU.1.1	The TSF shall allow enrolment and public information retrieval requests on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID.1 Timing of identification	
FIA_UID.1.1	The TSF shall allow enrolment and public information retrieval requests on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding	
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: the set of roles that the user is authorized to assume.
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: the user subject object shall represent the user's identify and be mapped to the set of roles the user is authorized to assume.
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: None.

Table 11: TOE Functional Security Requirements – Identification and Authentication

6.1.6 Remote Data Entry and Export

Table 12 describes the SFRs related to remote data entry and export operations.

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	
FCO_NRO_CIMC.3.1	The TSF shall enforce the generation of evidence of origin for certificate status information and all other security-relevant information at all times.
FCO_NRO_CIMC.3.2	The TSF shall be able to relate the identity and no other attributes of the originator of the information, and the security-relevant portions of the information to which the evidence applies.
FCO_NRO_CIMC.3.3	The TSF shall verify the evidence of origin of information for all security-relevant information.
FCO_NRO_CIMC.4 Advanced verification of origin	
FCO_NRO_CIMC.4.1	The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using an authentication code, keyed hash, or digital signature algorithm.
FCO_NRO_CIMC.4.2	The TSF shall, for all other security-relevant information, only accept the information if it was signed using a digital signature algorithm.
FDP_CIMC_CSE.1 Certificate status export	
FDP_CIMC_CSE.1.1	Certificate status information shall be exported from the TOE in messages whose format complies with the X.509 standard [4] for CRLs and the OCSP standard [2] as defined by RFC 2560.
FDP_ITT.1 Basic internal transfer protection (iteration 1)	
FDP_ITT.1.1	The TSF shall enforce the CIMC TOE Access Control Policy specified in appendix A to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the TOE.
FDP_ITT.1 Basic internal transfer protection (iteration 2)	
FDP_ITT.1.1	The TSF shall enforce the CIMC TOE Access Control Policy specified in appendix A to prevent the disclosure of confidential user data when it is transmitted between physically-separated parts of the TOE.

FDP_UCT.1 Basic data exchange confidentiality	
FDP_UCT.1.1	The TSF shall enforce the CIMC TOE Access Control Policy specified in appendix A to be able to transmit user data in a manner protected from unauthorised disclosure.
FPT_ITC.1 Inter-TSF confidentiality during transmission	
FPT_ITC.1.1	The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.
FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1)	
FPT_ITT.1.1	The TSF shall protect security-relevant TSF data from modification when it is transmitted between separate parts of the TOE.
FPT_ITT.1 Basic internal TSF data transfer protection (iteration 2)	
FPT_ITT.1.1	The TSF shall protect confidential TSF data from disclosure when it is transmitted between separate parts of the TOE.

Table 12: TOE Functional Security Requirements – Remote Data Entry and Export

6.1.7 Key Management

Table 13 describes the SFRs related to key management operations.

FCS_CKM_CIMC.5 CIMC private and secret key zeroization	
FCS_CKM_CIMC.5.1	The TSF shall provide the capability to zeroize plaintext secret and private keys within the FIPS 140-1 (or higher) validated cryptographic module.
FDP_ACF_CIMC.2 User private key confidentiality protection	
FDP_ACF_CIMC.2.1	CIMS personnel private keys shall be stored in a FIPS 140-1 (or higher) validated cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-1 (or higher) validated cryptographic module.
FDP_ACF_CIMC.2.2	If certificate subject private keys are stored in the TOE, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the FIPS 140-1 (or higher) validated cryptographic module.
FDP_ACF_CIMC.3 User secret key confidentiality protection	
FDP_ACF_CIMC.3.1	User secret keys stored within the CIMC, but not within a FIPS 140-1 (or higher) validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-1 (or higher) validated cryptographic module.
FDP_ETC_CIMC.5 Extended user private and secret key export	
FDP_ETC_CIMC.5.1	Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	
FDP_SDI_CIMC.3.1	Public keys stored within the CIMC, but not within a FIPS 140-1 (or higher) validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.
FDP_SDI_CIMC.3.2	The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall generate an audit log entry, mark the key as tampered with and deny any type of key usage.
FMT_MTD_CIMC.4 TSF private key confidentiality protection	
FMT_MTD_CIMC.4.1	CIMC private keys shall be stored in a FIPS 140-1 (or higher) validated cryptographic module or stored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-1 (or higher) validated cryptographic module.
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	
FMT_MTD_CIMC.5.1	TSF secret keys stored within the TOE, but not within a FIPS 140-1 (or higher) validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-1 (or higher) validated cryptographic module.
FMT_MTD_CIMC.7 Extended TSF private and secret key export	
FMT_MTD_CIMC.7.1	Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

Table 13: TOE Functional Security Requirements – Key Management

6.1.8 Certificate and Profile Management

Table 14 describes the SFRs related to certificate and profile management.

FMT_MOF_CIMC.3 Extended certificate profile management	
FMT_MOF_CIMC.3.1	The TSF shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.
FMT_MOF_CIMC.3.2	The TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions: • the key owner's identifier; • the algorithm identifier for the subject's public/private key pair; • the identifier of the certificate issuer; • the length of time for which the certificate is valid;

FMT_MOF_CIMC.3.3	If the certificates generated are X.509 public key certificates, the TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions: • keyUsage; • basicConstraints; • certificatePolicies
FMT_MOF_CIMC.3.4	The Administrator shall specify the acceptable set of certificate extensions.
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	
FMT_MOF_CIMC.5.1	If the TSF issues CRLs, the TSF must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.
FMT_MOF_CIMC.5.2	If the TSF issues CRLs, the TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions: • issuer; • issuerAltName (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.); • nextUpdate (i.e., lifetime of a CRL).
FMT_MOF_CIMC.5.3	If the TSF issues CRLs, the Administrator shall specify the acceptable set of CRL and CRL entry extensions.
FMT_MOF_CIMC.6 OCSP Profile Management	
FMT_MOF_CIMC.6.1	If the TSF issues OCSP responses, the TSF shall implement an OCSP profile and ensure that issued OCSP responses are consistent with the OCSP profile.
FMT_MOF_CIMC.6.2	If the TSF issues OCSP responses, the TSF shall require the Administrator to specify the set of acceptable values for the responseType field (unless the CIMC can only issue responses of the basic response type).
FMT_MOF_CIMC.6.3	If the TSF is configured to allow OCSP responses of the basic response type, the TSF shall require the Administrator to specify the set of acceptable values for the ResponderID field within the basic response type.
FDP_CIMC_CER.1 Certificate Generation	
FDP_CIMC_CER.1.1	The TSF shall only generate certificates whose format complies with X.509 v3 [4] and CVC BSI TR-03110 [3] standards for public key certificates.
FDP_CIMC_CER.1.2	The TSF shall only generate certificates that are consistent with the currently defined certificate profile.
FDP_CIMC_CER.1.3	The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FDP_CIMC_CER.1.4	If the TSF generates X.509 public key certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that: a) The version field shall contain the integer 0, 1, or 2. b) If the certificate contains an issuerUniqueID or subjectUniqueID then the version field shall contain the integer 1 or 2. c) If the certificate contains extensions then the version field shall contain the integer 2. d) The serialNumber shall be unique with respect to the issuing Certification Authority. e) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore. f) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension. g) If the subject field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical subjectAltName extension. h) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a FIPS-approved or recommended algorithm.
FDP_CIMC_CRL.1 Certificate Revocation	
FDP_CIMC_CRL.1.1	A TSF that issues CRLs shall verify that all mandatory fields in any CRL issued contain values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated: 1. If the version field is present, then it shall contain a 1. 2. If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1. 3. If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension. 4. The signature and signatureAlgorithm fields shall contain the OID for a FIPS-approved digital signature algorithm. 5. The thisUpdate field shall indicate the issue date of the CRL. 6. The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

FDP_CIMC_OCSP.1 Basic Response Validation	
FDP_CIMC_OCSP.1.1	If a TSF is configured to allow OCSP responses of the basic response type, the TSF shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 2560. At a minimum, the following items shall be validated: 1. The `version` field shall contain a `0`. 2. If the `issuer` field contains a null Name (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical `issuerAltName` extension. 3. The `signatureAlgorithm` field shall contain the OID for a FIPS-approved digital signature algorithm. 4. The `thisUpdate` field shall indicate the time at which the status being indicated is known to be correct. 5. The `producedAt` field shall indicate the time at which the OCSP responder signed the response. 6. The time specified in the `nextUpdate` field (if populated) shall not precede the time specified in the `thisUpdate` field.

Table 14: TOE Functional Security Requirements – Certificate and Profile Management

6.2 Security assurance requirements

Given the adoption of CIMC Security Level 3, **EAL4 augmented with the `ALC_FLR.2`** component has been selected as the overall assurance level of this TOE, as Table 15 summarizes.

Assurance class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

Table 15: Assurance Requirements

6.3 Security requirements rationale

Since the Security Problem Definition and the Security Objectives are similar to the CIMC PP, so are the Security Requirements.

However, given that the CIMC PP is only compliant with CC version 2.1 and that this TOE claims conformity with CC version 3.1, the security requirements rationale was adapted as follows:

- Since the FPT_RVM.1 SFR does not exist any more in CC 3.1, it was replaced by the ADV_ARC.1 SAR component;
- Though CC 3.1 introduced a new dependency of FMT_MOF.1 towards FMT_SMF.1, this dependency was not satisfied in this ST because management functions are already explicitly required by components FMT_MOF_CIMC.3, FMT_MOF_CIMC.5 and FMT_MOF_CIMC.6;
- Given the changes made in CC 3.1 to the contents of EAL4, there was a need to:
  - Add the ALC_CMC.4 and ALC_CMS.4 components, in order to replace the suppressed ACM_AUT.1, ACM_CAP.4 and ACM_SCP.2 components used in CC 2.1;
  - Replace the ADO_DEL.2 component used in CC 2.1 by the ALC_DEL.1 (covering the developer's site) and the AGD_PRE.1 (covering the user's site) components;
  - Replace the ADO_IGS.1 component used in CC 2.1 by the ALC_CMC.4 (covering the developer's site) and the AGD_PRE.1 (covering the user's site) components;
  - Map the ADV_FSP.2 component used in CC 2.1 to the ADV_FSP.4 component;
  - Add the ADV_TDS.3 component, in order to replace the suppressed ADV_HLD.2 and ADV_LLD.1 components used in CC 2.1;
  - Update the name of the ADV_IMP.1 component (from "*Subset of the implementation of the TSF*" to "*Implementation representation of the TSF*"), since CC 3.1 requires that all code is provided to the evaluator (though only a subset will be examined);
  - Suppress the ADV_RCR.1 component, since its contents were distributed by several other components;
  - Suppress the ADV_SPM.1 component, since CC 3.1 regards the informal SPM as the collection of objectives in the ST;
  - Add the AGD_OPE.1 component, in order to replace the suppressed AGD_ADM.1 and AGD_USR.1 components used in CC 2.1;
  - Added the ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1 and ASE_TSS.1 components, formally introduced by CC 3.1;
  - Update the name of the ATE_DPT.1 component (from "*Testing: high-level design*" to "*Testing: basic design*");
  - Suppress the AVA_MSU.2 component, since misuse analysis was mostly moved into the AGD component families that address the documents subject to such analysis. However, aspects of this remain in VAN components, since the AGD documents are considered when performing vulnerability analysis;

- Suppress the AVA_SOF.1 component, since SOF is not longer explicitly addressed. Instead, the resistance of a security function to an attacker is covered in VAN components;
- Map the AVA_VLA.2 component used in CC 2.1 to the AVA_VAN.3 component.

6.3.1 SFR dependencies

Table 16 lists all the security functional requirements dependencies for CIMC PP Security Level 3.

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Not included but covered by FMT_MTD_CIMC.4, FMT_MTD_CIMC.5 and FMT_MTD_CIMC.6
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	FCS_CKM.4 Cryptographic key destruction	Not included because secret keys are stored within the HSM and the operation of erasing is done internally by the HSM
	FDP_ACF.1 Security attribute based access control	Included

Component	Dependencies	Which is:
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Not included because no default profile is present in the TOE
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	FMT_MOF.1 Management of security functions behavior	Included
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	None	
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included

Component	Dependencies	Which is:
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	Not included because this product uses basic encryption to ensure basic data exchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path at this Security Level.
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Not included because the list of attributes is not configurable
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Not included because the list of supported roles is not restricted by the TOE
	FMT_SMF.1 Specification of Management Functions	Not included but covered by FMT_MOF_CIMC.3, FMT_MOF_CIMC.5 and FMT_MOF_CIMC.6
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Not included because the list of supported roles is not restricted by the TOE
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Not included because the list of supported roles is not restricted by the TOE
FMT_MOF_CIMC.6 OCSP profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Not included because the list of supported roles is not restricted by the TOE

Component	Dependencies	Which is:
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FMT_MTD_CIMC.6 TSF private and secret key export	Included
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1 Audit data generation	Included
	FMT_MOF.1 Management of security functions behavior	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	

Table 16: Summary of SFR dependencies for Security Level 3

6.3.2 SAR dependencies

Table 17 lists all the security assurance requirements dependencies for Security Level 3.

Component	Dependencies	Which is:
ADV_ARC.1 Security architecture description	ADV_FSP.1 Basic functional specification	Included (hierarchical to ADV_FSP.4)
	ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
ADV_FSP.4 Complete functional specification	ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)

Component	Dependencies	Which is:
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
ADV_IMP.1 Implementation representation of the TSF	ADV_TDS.3 Basic modular design	Included
	ALC_TAT.1 Well-defined development tools	Included
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_FSP.4 Complete functional specification	Included
	(indirect) ADV_IMP.1 Implementation representation of the TSF	Included
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
ADV_TDS.3 Basic modular design	ADV_FSP.4 Complete functional specification	Included
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
AGD_OPE.1 Operational user guidance	ADV_FSP.1 Basic functional specification	Included (hierarchical to ADV_FSP.4)
AGD_PRE.1 Preparative procedures	No dependencies	Not applicable
ALC_CMC.4 Production support, acceptance procedures and automation	ALC_CMS.1 TOE CM coverage	Included (hierarchical to ALC_CMS.4)
	ALC_DVS.1 Identification of security measures	Included
	ALC_LCD.1 Developer defined life-cycle model	Included

Component	Dependencies	Which is:
ALC_CMS.4 Problem tracking CM coverage	No dependencies	Not applicable
ALC_DEL.1 Delivery procedures	No dependencies	Not applicable
ALC_DVS.1 Identification of security measures	No dependencies	Not applicable
ALC_FLR.2 Flaw reporting procedures	No dependencies	Not applicable
ALC_LCD.1 Developer defined life-cycle model	No dependencies	Not applicable
ALC_TAT.1 Well-defined development tools	ADV_IMP.1 Implementation representation of the TSF	Included
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_FSP.4 Complete functional specification	Included
	(indirect) ADV_TDS.1 Basic Design	Included (hierarchical to ADV_TDS.3)
	(indirect) ADV_TDS.3 Basic modular design	Included
	(indirect) ALC_TAT.1 Well-defined development tools	Included
ASE_CCL.1 Conformance claims	ASE_ECD.1 Extended components definition	Included
	ASE_INT.1 ST introduction	Included
	ASE_REQ.1 Stated security requirements	Included (hierarchical to ASE_REQ.2)
ASE_ECD.1 Extended components definition	No dependencies	Not applicable
ASE_INT.1 ST introduction	No dependencies	Not applicable
ASE_OBJ.2 Security objectives	ASE_SPD.1 Security problem definition	Included

Component	Dependencies	Which is:
ASE_REQ.2 Derived security requirements	ASE_ECD.1 Extended components definition	Included
	ASE_OBJ.2 Security objectives	Included
	(indirect) ASE_SPD.1 Security problem definition	Included
ASE_SPD.1 Security problem definition	No dependencies	Not applicable
ASE_TSS.1 TOE summary specification	ADV_FSP.1 Basic functional specification	Included (hierarchical to ADV_FSP.4)
	ASE_INT.1 ST introduction	Included
	ASE_REQ.1 Stated security requirements	Included (hierarchical to ASE_REQ.2)
	(indirect) ASE_ECD.1 Extended components definition	Included
ATE_COV.2 Analysis of coverage	ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	ATE_FUN.1 Functional testing	Included
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
	(indirect) ATE.COV.1 Evidence of coverage	Included
ATE_DPT.1 Testing: basic design	ADV_ARC.1 Security architecture description	Included
	ADV_TDS.2 Architectural design	Included (hierarchical to ADV_TDS.3)
	ATE_FUN.1 Functional testing	Included
	(indirect) ADV_FSP.1 Basic functional specification	Included (hierarchical to ADV_FSP.4)

Component	Dependencies	Which is:
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_FSP.3 Functional specification with complete summary	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
	(indirect) ATE_COV.1 Evidence of coverage	Included (hierarchical to ATE_COV.2)
ATE_FUN.1 Functional testing	ATE_COV.1 Evidence of coverage	Included (hierarchical to ATE_COV.2)
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
	(indirect) ATE_FUN.1 Functional testing	Included
ATE_IND.2 Independent testing - sample	ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	AGD_OPE.1 Operational user guidance	Included
	AGD_PRE.1 Preparative procedures	Included
	ATE_COV.1 Evidence of coverage	Included (hierarchical to ATE_COV.2)
	ATE_FUN.1 Functional testing	Included
	(indirect) ADV_FSP.1 Informal functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
AVA_VAN.3 Focused vulnerability analysis	ADV_ARC.1 Security architecture description	Included

Component	Dependencies	Which is:
	ADV_FSP.4 Complete functional specification	Included
	ADV_IMP.1 Implementation representation of the TSF	Included
	ADV_TDS.3 Basic modular design	Included
	AGD_OPE.1 Operational user guidance	Included
	AGD_PRE.1 Preparative procedures	Included
	ATE_DPT.1 Testing: basic design	Included
	(indirect) ADV_FSP.1 Basic functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_FSP.2 Security-enforcing functional specification	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_FSP.3 Functional specification with complete summary	Included (hierarchical to ADV_FSP.4)
	(indirect) ADV_TDS.1 Basic design	Included (hierarchical to ADV_TDS.3)
	(indirect) ADV_TDS.2 Architectural design	Included (hierarchical to ADV_TDS.3)
	(indirect) ALC_TAT.1 Well-defined development tools	Included
	(indirect) ATE_COV.1 **Evidence of coverage**	Included (hierarchical to ATE_COV.2)
	(indirect) ATE_FUN.1 **Functional testing**	Included

Table 17: Summary of SAR dependencies for Security Level 3

7 TOE Summary Specifications

7.1 Security Audit

A complete deployment of EJBCA generates the following log types:

- *applicational logs*, produced by the TOE for problem tracking or maintenance purposes. Since these logs are solely for monitoring and maintenance purposes, they are not cryptographically protected;
- *audit logs*, produced by the TOE for security relevant events. Each log entry contains audit relevant data and is cryptographically protected by the TOE;
- *system logs*, produced by the IT environment supporting the TOE (e.g., Operating System, Database, HSM).

Audit logs are of particular importance for security audits as reliable supporting evidence of operations. Log entries are produced whenever security relevant events (described in section 6.1.1) occur during execution of operations in the TOE and contain the following information:

- Date/time;
- TOE User: Identification of the TOE user that originated the event;
- Security Service: Type of service that generated the log entry (e.g. certificate issuance, key generation, etc.);
- Module;
- Event Type: Description of the event (e.g. information, error, warning);
- Result: Description of the result type (OK or error);
- Other relevant details.

Since EJBCA fully relies on CESeCore's security audit functionalities, the audit logs are stored in CESeCore's database and can be exported to file either periodically or at request of an Auditor. The integrity of the audit logs stored in the database and on the export files is cryptographically protected, that not only ensure data authenticity, but also prevents undetected log entry deletion.

Additionally, CESeCore provides an interface to query, view and check the audit logs stored in the its database.

An error that prevents the persistence of audit logs causes the TOE to prevent audited events except those carried out by the Auditor, in order to avoid the execution of operations without properly recording related audit data.

Date and time accuracy of audit logs is guaranteed by requiring the IT environment to have system time synchronized with a reliable time source. The time source is considered reliable if is synchronized to within 1 second of Co-ordinated Universal Time (UTC).

Table 18 details the rationale applied to the usage of security audit security requirements.

FAU_GEN.1 Audit data generation	Audit logs are generated along the occurrence of the events and immediately committed and stored in the database that is part of the IT environment.
FAU_GEN.2 User identity association	Audit logs include information about the TOE user identity, either by reference (if it is an authenticated user) or by value (if it is an unauthenticated user).
FAU_SEL.1 Selective audit	The TOE provides a searching interface where audit logs can be queried by applying a configurable composition of criteria.
FAU_STG.1 Protected audit trail storage	Audit logs are cryptographically protected against tampering and deletion.
FAU_STG.4 Prevention of audit data loss	Only events triggered by Auditors are allowed to be executed when the IT environment cannot store any more audit logs.
FPT_CIMC_TSP.1 Audit log signing event	Audit logs are cryptographically protected against tampering and deletion.
FPT_STM.1 Reliable time stamps	Time is obtained from the IT environment which must have its system time synchronized with a reliable time source.

Table 18: Rationale for the Security Audit Security Requirements

7.2 Roles

As detailed in section 7.4, access control to the TOE is based on the concept of TOE users associated to roles. Each of the defined roles is configured with a set of permissions and/or restrictions about the operations and objects that it can (or cannot) access.

EJBCA uses the same role set as CESeCore, which is defined in Appendix A.

Creation of additional customized roles is allowed in order to be able to comply with specific security policies.

Table 19 details the rationale applied to the usage of roles security requirements.

FMT_MOF.1 Management of security functions behaviour	The Access Control uses the defined Roles the evaluate whether the TOE user shall be granted access to the requested object or operation.

Table 19: Rationale for the Roles Security Requirements

7.3 Backup and Recovery

EJBCA provides backup and recovery functionalities in order to allow the reconstruction of the system in the event of a system failure, data loss or other serious error. Despite being based on the same type of functionality made available by CESeCore, EJBCA includes extensions necessary to cover its additional configuration files.

With that purpose, the TOE's interfaces can be used by an Operator to backup and restore the following data:

- TOE configuration files;
- Cryptographic material stored outside of the HSM and DB;
- Other information relevant for the recovery of the CESeCore system.

The integrity of the backup data is assured through the usage of digital signature, keyed hash or authentication code mechanisms (configurable). Regarding the protection of critical security parameters and other confidential information, it is ensured using encryption.

Additionally, and since in large scale deployments the information kept on the database can reach hundreds of gigabytes, both EJBCA and CESeCore's databases should be backed up using appropriate and database-specific tools, taking advantage of the partitioning and security mechanisms they support.

Finally, the TOE's interfaces may also be used by the Auditor to backup audit log entries.

Table 20 details the rationale applied to the usage of backup and recovery security requirements.

`FDP_CIMC_BKP.1 CIMC backup and recovery`	The TOE's interfaces can be used to trigger the backup process in order to export all relevant data existing in an EJBCA deployment. Additionally, those interfaces can also be used to restore the system state at the respective time of a given backup.
`FDP_CIMC_BKP.2 Extended CIMC backup and recovery`	The integrity of the backup data is protected by using digital signature, keyed hash or authentication code mechanisms (configurable). Critical security parameters and other confidential information are protected through encryption.

Table 20: Rationale for the Backup and Recovery Security Requirements

7.4 Access Control

Since EJBCA fully relies on CESeCore's access control mechanisms, the TOE's resources are protected using access control lists, based on four key components:

- `access rule` – accept or decline access to a resource, can be recursive or not;
- `resource` – a resource to which access is controlled. Resources have a hierarchical format (e.g. `/ca_functionality/store_certificate`);
- `user` – an entity that have access rights to a resource;

- `role` – a role that a user is allowed to take on. Since access rules are defined on a role, so for a user to have access rights he must be assigned roles.

When a controlled resource is accessed, the TOE verifies that the caller meets the appropriate access rules for the resource and, if not, denies access and generates an error. If there are no access rules associated to the resource, access is denied.

The TOE access control system maps authentication information to a user entity in the TOE database. The entity is then associated to a role in order to acquire privileges.

Appendix A details the roles supported by the TOE.

The roles have different access rights on different resources. Additionally, there are many resources organized in a hierarchical way, which allows for higher level access rights to be applied recursively on sub-access rights.

Table 21 details the rationale applied to the usage of access control security requirements.

`FDP_ACC.1 Subset access control`	Access control lists can be used to specify the acceptable subsets of security functions applicable to specified resources.
`FDP_ACF.1 Security attribute based access control`	TOE users are assigned roles that are granted a set of access control rules on a set of resources.

Table 21: Rationale for the Access Control Security Requirements

7.5 Identification and Authentication

Enrolment and public information access operations may be carried out before user identification. However, non-authenticated requests need to be approved later by an authenticated Officer before being processed by the TOE. Access to non-public operations in the TOE is restricted to users authenticated using mutually authenticated SSL or username/password.

Table 22 details the rationale applied to the usage of identification and authentication security requirements.

`FIA_UAU.1 Timing of authentication`	Authentication is not required to perform the following operations: • fetch CA[9] certificates, OCSP certificates, CRLs; • check certificate status (given the issuer DN and the serial number). Additionally, it is also possible to list and fetch user certificates (given the subject DN) for certificates that are registered as public.

[9]Certification Authority.

FIA_UID.1 Timing of identification	Identification is not required to perform the following operations: • fetch CA certificates, OCSP certificates, CRLs; • check certificate status (given the issuer DN and the serial number). Additionally, it is also possible to list and fetch user certificates (given the subject DN) for certificates that are registered as public. Nonetheless, if audit logs are configured to be stored for those events, the request source IP is registered.
FIA_USB.1 User-subject binding	User security attributes are associated to the TOE user identity and authentication credentials, allowing a unique match.

Table 22: Rationale for the Identification and Authentication Security Requirements

7.6 Remote Data Entry and Export

Regarding data entry, the TOE is capable of handling and processing:

- registration data, either electronically provided by an external application (e.g. Registration Authority) or an Operator. In either case, the information is provided securely to the TOE;
- CSRs formatted in PKCS#10 or CRMF;
- status information requests that comply with the RFC 2560;
- other security-relevant operations carried out by an Administrator, Officer, Operator or Auditor. In either case, the information is securely provided to the TOE.

Additionally, data exported by the TOE observes the following standards:

- X.509 v3: public key certificates and CRLs;
- CVC BSI TR-03110: public key certificates;
- RFC 2560: OCSP responses
- PKCS#12: user private keys and respective public key certificate chain.

Finally, and regarding communication between the TOE and external components/systems:

- TOE ↔ HSM: This type of communication should be protected using the equipment's security mechanisms;
- TOE ↔ Database: Since the database is installed in the same machine, there is no need to adopt specific controls to protect the connection with it. However, whenever possible, advantage should be taken of the database's security mechanisms (e.g. encrypted channel supported by MySQL and PostgreSQL).

Table 23 details the rationale applied to the usage of remote data entry and export security requirements.

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	Digital signatures are used as a basis for ensuring proof of origin, given the compliance with with X.509 v3 and RFC 2560. Since the TOE includes an internal RA, TOE users can carry out relevant operations through a secure interface. Additionally, when EJBCA is integrated with external RAs, requests are only accepted from authenticated and authorised sources, taking advantage of the security mechanisms (e.g. authentication codes, digital signatures, etc.) of protocols like CMP.
FCO_NRO_CIMC.4 Advanced verification of origin	Requests received from external RAs are only accepted from authenticated and authorised sources, taking advantage of the security mechanisms (e.g. authentication codes, digital signatures, etc.) of protocols like CMP.
FDP_CIMC_CSE.1 Certificate status export	Certificate status information is provided by the TOE through CRLs compliant with X.509 v3 and OCSP responses compliant with RFC 2560 (as a result of the reception and processing of a valid OCSP request).
FDP_ITT.1 Basic internal transfer protection (iteration 1 and 2)	Since there are no physically-separated parts of the TOE, there is no need to employ specific security mechanisms.
FDP_UCT.1 Basic data exchange confidentiality	The communications between the TOE and the HSM should be protected using the equipment's security mechanisms. The communications between the TOE and the database should be protected by, whenever possible, taking advantage of the database's security mechanisms (e.g. encrypted channel supported by MySQL and PostgreSQL).
FPT_ITC.1 Inter-TSF confidentiality during transmission	Since the database is installed in the same machine, there is no need to adopt specific controls to protect the connection with it. However, whenever possible, advantage should be taken of the database's security mechanisms (e.g. encrypted channel supported by MySQL and PostgreSQL).
FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1 and 2)	Since there are no physically-separated parts of the TOE, there is no need to employ specific security mechanisms.

Table 23: Rationale for the Remote Data Entry and Export Security Requirements

7.7 Key Management

EJBCA's key management functionalities rely both on CESeCore and a FIPS 140-1 (or higher) validated cryptographic modules (both software and hardware based) for its key management functions. Moreover, if for end user keys it could be enough to ensure their protection just by storing them encrypted in the TOE's database, others (like the certificate signing key) have to be generated/kept inside a FIPS 140-1 (or higher) Level 3, which is also responsible for their secure backup and recovery. If kept by the TOE, user related secrets (e.g. passphrases) are encrypted before storing them in the database.

Table 24 details the rationale applied to the usage of key management security requirements.

FCS_CKM_CIMC.5 CIMC private and secret key zeroization	The TOE relies on software and hardware (FIPS 140-1 or higher, Level 3 validated) cryptographic security modules for key zeroization.
FDP_ACF_CIMC.2 User private key confidentiality protection	CIMS personnel private keys are not stored by the TOE. Certificate subject private keys that can be subject to key recovery are stored (encrypted) by the TOE.
FDP_ACF_CIMC.3 User secret key confidentiality protection	User secret keys are not stored outside FIPS 140-1 (or higher) validated cryptographic module.
FDP_ETC_CIMC.5 Extended user private and secret key export	User private keys can only be exported from the TOE in encrypted format (e.g. PKCS#12).
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	The integrity and authenticity of public keys stored by the TOE outside of a FIPS 140-1 (or higher) validated cryptographic module is protected by the usage of a digital signature, namely of the digital certificate structure in which it has been included. Every time each public key needs to be used to perform any cryptographic operation, its protective digital signature will be verified and, in case of failure, an audit log entry will be generated and the key will be marked as tampered with, becoming unusable for all types of operations.
FMT_MTD_CIMC.4 TSF private key confidentiality protection	All TSF private keys are stored on the FIPS 140-1 (or higher) validated cryptographic module.
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	All TSF secret keys are stored in the HSM.
FMT_MTD_CIMC.7 Extended TSF private and secret key export	The TOE does not support TSF key export, the FIPS 140-1 (or higher) HSM is responsible for their backup and recovery.

Table 24: Rationale for the Key Management Security Requirements

7.8 Certificate and Profile Management

Taking advantage of CESeCore's capabilities, the TOE contains functions to generate X.509 certificates and CRLs according to the standards:

- ISO/ITU X.509 [4];
- IETF RFC 5280 [1]
- BSI TR-03110 [3].

In addition to this, EJBCA extends CESeCore's functionalities by supporting a complete set of RA operations.

The TOE maintains a database of all issued certificates and their current state, in order to serve status information. Status information of certificates is made available through CRLs (RFC 5280 [1]), OCSP (RFC 2560 [2] and RFC 5019 [5]). Issued CRLs are also stored in the database.

Certificate, CRL and OCSP profiles can only be configured by authorized administrators.

The TOE contains functions for issuing, revoking, suspending, re-activating, renewing and reporting status of certificates. These services are provided through service APIs and subject to appropriate access control to ensure that only authorized administrators access security sensitive operations.

Table 25 details the rationale applied to the usage of certificate and profile management security requirements.

`FMT_MOF_CIMC.3 Extended certificate profile management`	Certificate profiles restrict or define key characteristics, algorithms and extensions (`keyUsage`, `basicContraints`, `certificatePolicies` and other other relevant extensions). Subject profiles restrict acceptable values for subject identity.
`FMT_MOF_CIMC.5 Extended certificate revocation list profile management`	CRL profile is configured as part of the CA configuration. Detailed settings for CRL validity and extensions are available.
`FMT_MOF_CIMC.6 OCSP profile management`	The OCSP responder only issues responses of the basic response type. Configuration of `responderID` is done by selecting which type should be used and which CAs should respond to OCSP queries.
`FDP_CIMC_CER.1 Certificate generation`	The TOE generates certificates according to the X.509, RFC 5280 and BSI TR-03110 standards.
`FDP_CIMC_CRL.1 Certificate revocation list validation`	The TOE generates CRLs according to the X.509 and RFC 5280 standards.
`FDP_CIMC_OCSP.1 OCSP basic response validation`	The TOE OCSP responder generates responses according to the RFC 2650 standard.

Table 25: Rationale for the Certificate and Profile Management Security Requirements

References

[1] http://tools.ietf.org/pdf/rfc5280.pdf, *RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[2] http://tools.ietf.org/pdf/rfc2560.pdf, *RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

[3] BSI, *Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI)*.

[4] http://www.itu.int/rec/T-REC-X.509-200508-I/en. *ITU-T X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[5] http://tools.ietf.org/pdf/rfc5019.pdf. *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*.

[6] http://www.ejbca.org/. *EJBCA Project Website*.

Glossary

AGD	Guidance Documents CC components
API	Application Programming Interface
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CIMC	Certificate Issuing and Management Components Protection Profile
CIMS	Certificate Issuing Management System
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
CVC	Card Verifiable Certificates
CWA	CEN Workshop Agreement
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EJB	Enterprise Java Bean
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IT	Information Technology
JDBC	Java Database Connectivity
JEE	Java Enterprise Edition
JVM	Java Virtual Machine
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKCS#10	Certification Request Syntax Standard
PKCS#11	Cryptographic Token Interface Standard
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Functions
SFP	Security Functions Policy
SFR	Security Functional Requirement
SOF	Strength of TOE Security Functions CC components (deprecated since CC 3.1)
SPM	Security Policy Modelling CC components (deprecated since CC 3.1)
SQL	Structured Query Language

SSCD	Secure Signature Creation Device
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAN	Vulnerability Analysis CC components
VM	Virtual Machine

A CIMC TOE Access Control Policy

This appendix describes the characteristics of the access control policy that the TOE will enforce and manage.

The system will grant subjects access to objects and operations made over it based upon:

a) The identity of the subject that requested the access;

b) The role(s) associated to that subject;

c) The details of the access request.

Subject identification includes individuals assigned to one or more roles with different access authorizations.

Access to objects is defined by the simple access types used on access rules:

- `Accept`;
- `Decline`;
- `Unused`.

Access rules can be organized hierarchically and `Accept` and `Decline` access types can be applied recursively or not. Default value is `Unused` and default recursive behaviour is "not recursive".

The default access decision for an `Unused` access rule is to deny access, unless there is a hierarchically superior access rule with value `Access` that applies recursively.

The TOE will support predefined roles:

- **Administrator:** role authorized to install, configure and maintain the TOE, establish and maintain user accounts, configure profiles, access rights and audit parameters and manage Component keys;
- **Auditor:** role authorized to view and maintain audit logs;
- **Officer:** role authorized to request or approve certificates or certificate revocations;
- **Operator:** role authorized to perform system backup and recovery.