Security Target for EJBCA v7.4.2

Document ID :	**1.3.6.1.4.1.22408.1.3.1.1.1**
Document Name :	**Security Target for EJBCA v7.4.2**
Status :	**Approved**
Dissemination Level :	**Public**
Document Version :	**1.7**
Version Date :	**2023-11-01**
Author(s):	**Anders Staaf**

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

History

Version	Date	Modification reason	Modified by
1.0	2020-09-28	Minor updates and QA	Anders Staaf
1.1	2021-03-02	Addressed the certifier's comments.	Anders Staaf
1.2	2021-03-29	A minor update for the version of Oracle OpenJDK.	Anders Staaf
1.3	2021-05-17	Added compliance to EAL1+.	Anders Staaf
1.4	2021-09-09	Minor updates, addressed by the NIAP review of the "Assurance Activity Report – EJBCA 7.4.1.1", version 1.9, CAB- 21-1490-6223-411	Anders Staaf
1.5	2021-09-24	Minor update in section 7.1 for FAU_STG.4.1	Anders Staaf
1.6	2023-09-07	Version of TOE is updated.	Magnus Ahlbin
1.7	2023-11-01	Version of TOE is updated.	Magnus Ahlbin

Contents

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 of the type specified in the X.509 v3 [4] and CVC BSI TR-03110 [3] standards. Additionally, EJBCA can also be set up as a high performance, highly available OCSP responder service, Verification Authority (VA).

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 v7.4.2
ST Reference	1.7
TOE Identification	EJBCA Enterprise v7.4.2
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 5)
PP Conformance	Protection Profile for Certification Authorities, Version 2.1, 2017-12-01, National Information Assurance Partnership

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.

The TOE is a Certificate Authority (CA). As an enterprise class PKI Certificate Authority, EJBCA issues and manage the life cycle of public key certificates of the type specified in 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;
- Smart card logon to Windows and/or Linux;

[1] Public Key Infrastructure.

- 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.

1.4. TOE Description

1.4.1. TOE Physical Scope

As illustrated by Figure 1, the TOE includes:

- The EJBCA component; and
- 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); and
- Database engine.

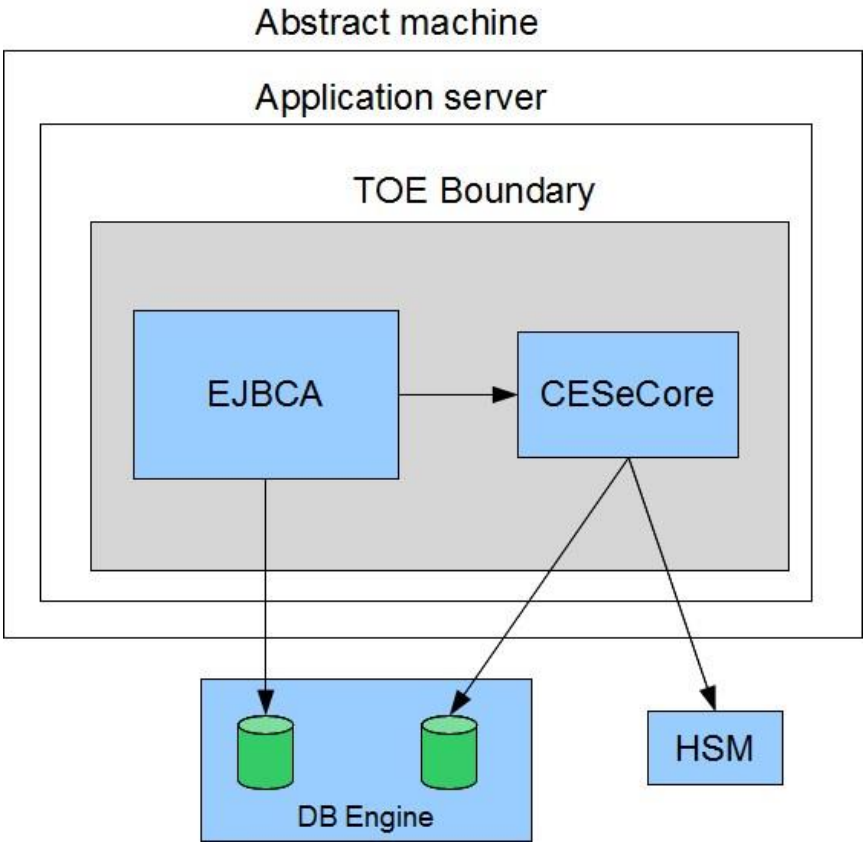

Figure 1, TOE boundary

1.4.2. TOE Components

The usage of EJBCA relies not only on its implementation, but also on several other additional components described in section 1.4.3.

1.4.2.1. 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.
- Connecting to other EJBCA nodes acting as Registration Authority (RA) or Validation Authority (VA).

In order to achieve some of its goals and deliver the above mentioned features, the CESeCore, described in the following section, is used as a part of TOE. .

1.4.2.2. CESeCore

CESeCore is a part of the TOE. CESeCore follows the CIMC SL3 Protection Profile and implements security functionalities needed to create PKI-based applications, available through a set of APIs (either Java APIs or JEE specific APIs).

1.4.3. TOE Environment

The non-TOE hardware/software/firmware required by the TOE is described below. The rationale for excluding components from the TOE is elaborated in the following sections.

1.4.3.1. Application Server

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.

EJBCA can (optionally) be deployed on a JEE 7 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.

EJBCA should run on any JEE 7 certified application server. The TOE works, at least, with the following components:

- JBoss EAP 7.2;
- Wildfly 10, 11, and 14

See section 1.4.3.7 for the evaluated configuration.

1.4.3.2. 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.

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.

Since there are several versions of the JVM specification, Oracle OpenJDK 1.8.0_242 for Linux and Windows has been explicitly chosen for the evaluated configuration.

1.4.3.3. 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;

[2] Where the private key is encrypted.

- End user registration data, along with their respective passwords;
- Roles and access rules for administrative users
- Service configuration;
- Approval information (events waiting for approval by TOE users);
- Information about Approval Profiles
- CA configuration (additional to the one kept in CESeCore's database);
- System configuration;
- Configuration pertaining to various protocols and APIs
- End user hard token information and issuer configuration (e.g. information about smartcards issued to end users).
- Information about configured downstream peers, e.g. VAs and RAs

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.

All connections to the database are performed using the appropriate JDBC[4] drivers. Given that it is located in the same physical 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.

Any SQL[5] compliant database can be used. The TOE works, at least, with the following components:

- MySQL 5.7;
- MariaDB 10.2.13

See section 1.4.3.7 for the evaluated configuration.

1.4.3.4. Hardware Security Module

All cryptographic operations performed at the request of the TOE should take place in a cryptographic module, either in software or in hardware. The interaction with the cryptographic module is performed through a standard PKCS#11 library provided by the respective vendor.

[3] Where the private key is encrypted.
[4] Java Database Connectivity
[5] Structured Query Language

Using the PKCS#11 interface makes it possible to use virtually any of the HSMs available on the market. A FIPS 140-2 validated HSM is recommended.

The TOE works, at least, with the following components:

- SafeNet Luna SA
- Utimaco CryptoServer, FIPS 140-2 validated (CMVP #2814/CMVP #3925)

1.4.3.5. 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 a CC-certified configuration certain restrictions on the configuration artifacts may apply. Those restrictions are defined in ref. 7, *EJBCA Common Criteria Guidance Supplement*.

1.4.3.6. Hardware and Operating System

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.

The hardware platform is limited to a generic x86 64 bit server for the evaluated configuration.

Although it is be possible to deploy and use the TOE on any Linux or Windows operating system, the TOE has been verified on CentOS Linux 7, Red Hat Enterprise Linux 7, and Windows Server 2016.

1.4.3.7. Evaluated Configuration

Part	Description
JEE 7 compliant application server	Wildfly 14.0.1
Java Virtual Machine (JVM)	Oracle OpenJDK 1.8.0_242
Relational Database	MariaDB 10.2.13
HSM	Utimaco CryptoServer SE52 (CMVP #2814 and #3925)
Operating system	CentOS Linux 7 (kernel: 3.10.0-1062.9.1.el7)

Table 1, Evaluated Configuration

1.4.4. TOE Logical Scope

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 real-time information about their revocation status, according to the OCSP protocol. Additionally, the TOE depends on several external components for its operation.

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.

1.4.4.1. Electronic Signatures Creation

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

1.4.4.2. 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).

1.4.4.3. OCSP Support

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

1.4.4.4. 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.

1.4.4.5. 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.

1.4.4.6. 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.

1.4.4.7. 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.

1.4.4.8. Key Generation and Management

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

1.4.4.9. Backup of TOE Data

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

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

1.4.4.10. 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.).

1.4.4.11. Key Recovery

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

1.4.4.12. 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.

1.4.4.13. User Registration and Management

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

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

1.4.4.14. 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.

1.4.4.15. Certificate and CRL Retrieval

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

1.4.5. TOE Roles

Administrative roles are fully configurable. The TOE provides default role templates corresponding to the roles defined in the Protection Profile, ref. 8. The corresponding TOE role names are:

Administrator – Super Administrator

Auditor – Auditor

CA Operations Staff – CA Administrators

RA Staff - RA Administrators

Authorized Organizational Representative - Supervisor

1.4.6. TOE Delivery Method

The TOE is downloaded from customer specific HTTPS-sites owned by PrimeKey, e.g. https://download.primekey.se/.

2. Conformance Claims

2.1. CC Conformance Claim

The TOE conforms to:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 5), part 2 extended;
- Common Criteria for Information Technology Security Evaluation, Version 3.1 (revision 5), part 3 conformant;
    - ADV_FSP.1 Basic Functional Specification
    - AGD_OPE.1 Operational User Guidance
    - AGD_PRE.1 Preparative Procedures
    - ALC_CMC.1 Labeling of the TOE
    - ALC_CMS.1 TOE CM Coverage
    - ASE_CCL.1 Conformance claims
    - ASE_ECD.1 Extended components definition
    - ASE_INT.1 ST Introduction
    - ASE_OBJ.1 Security Objectives
    - ASE_REQ.1 Security Requirements
    - ASE_SPD.1 Security problem definition
    - ASE_TSS.1 TOE summary specification
    - ATE_IND.1 Independent Testing – Conformance
    - AVA_VAN.1 Vulnerability Survey

2.2. PP conformance claim

The ST demonstrates exact conformance to the following Protection Profile (PP):

- Protection Profile for Certification Authorities, Version 2.1, 2017-12-01, National Information Assurance Partnership, ref. 8.

2.3. Applicable Technical Decisions

The following technical decisions are applicable to the PP_CA_V2.1:

- TD0522 – Updates to Certificate Revocation (FIA_X509_EXT.1)
- TD0500 – Cryptographic selections and updates for CAPP
- TD0415 – Trusted Update Test 4 Conditional
- TD0375 – FMT_MOF.1(4) selection
- TD0353 – Guidance for Certificate Profiles
- TD0348 – FCS_TLSS_EXT.2.4 for TLS 1.2 or higher
- TD0328 – Split Knowledge Procedures distinction
- TD0294 – Correction of TLS SFRs in CA PP ver 2.1
- TD0287 – FAU_STG.4 Testing
- TD0286 – Audit Events for FPT_RCV.1
- TD0278 – Clarification of Role for Managing Manual Certificate Requests
- TD0276 – X.509 Code Signing on TOE Updates

2.4. Conformance Rationale

All of the assumptions, threats, policies, objectives and security requirements defined for Protection Profile for Certification Authorities have been reproduced in this ST. No additional assumption, threat, policy, objective or security requirement has been used.

Table 2 lists all security function requirements that have or have not been included. M – Mandatory, O – Optional, S – Selectable.

Security Functional Requirement	M	O	S	Incl.	Rationale
FAU_ADP_EXT.1 Audit Dependencies	X			Y	Mandatory
FAU_GCR_EXT.1 Generation of Certificate Repository	X			Y	Mandatory
FAU_GEN.1 Audit Data Generation	X			Y	Mandatory
FAU_GEN.2 User Identity Association	X			Y	Mandatory
FAU_SAR.1 Audit Review			X	Y	Audit review is performed by an auditor through an interface provided by the TSF.
FAU_SAR.3 Selectable Audit Review			X	Y	Audit review is performed by an auditor through an interface provided by the TSF.

Security Functional Requirement	M	O	S	Incl.	Rationale
FAU_SCR_EXT.1 Certificate Repository Review			X	N	The ability to search on certificate fields provided entirely by the OE OE.CERTIFICATE_REPOSITORY_SEARCH objective is included instead.
FAU_SEL.1 Selective Audit			X	Y	The TSF provides operations (as specified in FAU_ADP_EXT.1) to include the pre-selection of audit records.
FAU_STG.1(1) Protected Audit Trail Storage			X	N	Audit records are not stored within the TOE boundary but in the database.
FAU_STG.1(2) Protected Audit Trail Storage (Archive Data)			X	N	No audit data stored within the TOE boundary is expected to persist intact beyond the validity of certificates issued by the CA.
FAU_STG.4 Prevention of Audit Data Loss	X			Y	Applies to the TOE regardless of whether the audit trail is stored within the TOE boundary (e.g. the audit trail is full) or on an external system in the Operational Environment (e.g. the connection to a remote audit repository is broken).
FAU_STG_EXT.1 External Audit Trail Storage			X	Y	The TSF initiates the storage of the audit data (that is, it generates audit data that will be stored by the OE).
FAU_STG_EXT.2 Audit Data Retention			X	N	The Operational Environment provides mechanisms for retention of audit records.
FCO_NRO_EXT.2 Certificate-Based Proof of Origin	X			Y	Mandatory
FCO_NRR_EXT.2 Certificate-Based Proof of Receipt			X	Y	EST is claimed.

Security Functional Requirement	M	O	S	Incl.	Rationale
FCS_CDP_EXT.1 Cryptographic Dependencies	X			Y	Mandatory
FCS_CKM.1 Cryptographic Key Generation			X	Y	The Operational Environment is used to generate the keys.
FCS_CKM.2 Cryptographic Key Establishment			X	Y	The TOE perform key establishment.
FCS_CKM_EXT.1(1) Symmetric Key Generation for DEKs			X	N	FDP_SDP_EXT.1 is not included.
FCS_CKM_EXT.1(2) Key Generation Key Encryption Keys			X	N	Keys are stored in a hardware cryptographic module.
FCS_CKM_EXT.1(3) Key Generation for Key Encryption Keys (TOE Key Archival)			X	N	FPT_SKY_EXT.1 is not included.
FCS_CKM_EXT.1(4) Generation of Key Shares			X	N	Used by FPT_SKY_EXT.1 is not included.
FCS_CKM_EXT.4 Cryptographic Key Destruction			X	Y	TOE destructs key material and CSP.
FCS_CKM_EXT.5 Public Key Integrity			X	N	FDP_STG_EXT.1 is not included.
FCS_CKM_EXT.6 TOE Key Archival			X	N	Key sharing mechanism is included in FPT_SKY_EXT.1 Split Knowledge Procedures
FCS_CKM_EXT.7 Key Generation for KEKs			X	N	The Key Encryption Key generation is performed in a hardware cryptographic module.
FCS_CKM_EXT.8 Key Hierarchy Entropy			X	N	The entropy is provided by the operational environment.
FCS_COP.1(1) Cryptographic Operation (AES Encryption/Decryption)			X	Y	AES is used for HTTPS/TLS.
FCS_COP.1(2) Cryptographic Operation (Cryptographic Signature)			X	Y	Digital signatures are used (e.g. HTTPS/TLS).
FCS_COP.1(3) Cryptographic Operation (Cryptographic Hashing)			X	Y	Hashing is used (e.g. HTTPS/TLS).
FCS_COP.1(4) Cryptographic Operation (Keyed-Hash Message Authentication)			X	Y	Keyed mac is used (e.g. HTTPS/TLS).
FCS_COP.1(5) Cryptographic Operation (Password-Based Key Derivation Function)		X		N	FPT_SKY_EXT.2 is not included.

Security Functional Requirement	M	O	S	Incl.	Rationale
FCS_HTTPS_EXT.1 HTTPS Protocol			X	Y	HTTPS/TLS is used for administration GUI.
FCS_IPSEC_EXT.1 IPsec Protocol			X	N	IPSec is not used.
FCS_RBG_EXT.1 Cryptographic Random Bit Generation			X	Y	RBG is used for key generation.
FCS_STG_EXT.1 Cryptographic Key Storage	X			Y	Mandatory
FCS_TLSC_EXT.1 TLS Client Protocol			X	N	Only TLS with mutual authentication is used.
FCS_TLSC_EXT.2 TLS Client Protocol with Mutual Authentication			X	Y	Used for RA communication.
FCS_TLSS_EXT.1 TLS Server Protocol			X	N	Only TLS with mutual authentication is used
FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication			X	Y	Used for administration GUI communication.
FDP_CER_EXT.1 Certificate Profiles	X			Y	Mandatory
FDP_CER_EXT.2 Certificate Request Matching	X			Y	Mandatory
FDP_CER_EXT.3 Certificate Issuance Approval	X			Y	Mandatory
FDP_CER_EXT.4 Non-X.509v3 Certificate Generation		X		N	Only X.509 v3 needs to be claimed.
FDP_CRL_EXT.1 Certificate Revocation List Validation			X	Y	CRL validation is supported.
FDP_CSI_EXT.1 Certificate Status Information	X			Y	Mandatory
FDP_ITT.1 Basic Internal Transfer Protection			X	Y	TLS and TLS/HTTPS are used.
FDP_OCSPG_EXT.1 OCSP Basic Response Generation			X	Y	OCSP is supported.
FDP_RIP.1 Subset Residual Information Protection	X			Y	Mandatory
FDP_SDP_EXT.1 User Sensitive Data Protection		X		N	User Sensitive Data is not encrypted.
FDP_STG_EXT.1 Public Key Protection		X		N	Public key protection is performed entirely by the DB in the Operational Environment.
FIA_AFL.1 Authentication Failure Handling			X	N	Unsuccessful authentication attempts are not detected.

Security Functional Requirement	M	O	S	Incl.	Rationale
FIA_CMCC_EXT.1 Certificate Management over CMS (CMC) Client			X	N	CMC is not supported.
FIA_CMCS_EXT.1 Certificate Management over CMS (CMC) Server			X	N	CMC is not supported.
FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client			X	N	Only EST Server not client is included.
FIA_ESTS_EXT.1 Enrollment over Secure Transport (EST) Server			X	Y	EST Server is included.
FIA_PMG_EXT.1 Password Management			X	Y	Password management is supported for end entities.
FIA_PSK_EXT.1 Pre-Shared Key Composition			X	N	Pre-Shared Keys are not supported.
FIA_X509_EXT.1 Certificate Validation	X			Y	Mandatory
FIA_X509_EXT.2 Certificate-Based Authentication	X			Y	Mandatory
FIA_X509_EXT.3 X509 Certificate Request			X	Y	CSR is supported.
FIA_UAU.7 Protected Authentication Feedback			X	Y	Obscured feedback when entering password is supported.
FIA_UAU_EXT.1 Authentication Mechanism	X			Y	Mandatory
FIA_UIA_EXT.1 User Identification and Authentication	X			Y	Mandatory
FMT_MOF.1(1) Management of Security Functions Behavior (Administrator Functions)	X			Y	Mandatory
FMT_MOF.1(2) Management of Security Functions Behavior (CA/RA Functions)	X			Y	Mandatory
FMT_MOF.1(3) Management of Security Functions Behavior (CA Operations Functions)	X			Y	Mandatory
FMT_MOF.1(4) Management of Security Functions Behavior (Admin/Officer Functions)	X			Y	Mandatory
FMT_MOF.1(5) Management of Security Functions Behavior (Auditor Functions)	X			Y	Mandatory
FMT_MTD.1 Management of TSF Data	X			Y	Mandatory
FMT_SMF.1 Specification of Management Functions	X			Y	Mandatory
FMT_SMR.2 Restrictions on Security Roles	X			Y	Mandatory

Security Functional Requirement	M	O	S	Incl.	Rationale
FPT_APW_EXT.1 Protection of Privileged User Passwords			X	Y	Password are protected when stored.
FPT_FLS.1 Failure with Preservation of Secure State	X			Y	Mandatory
FPT_ITT.1 Basic Internal TSF Data Transfer Protection			X	Y	TLS and TLS/HTTPS are used.
FPT_KST_EXT.1 No Plaintext Key Export	X			Y	Mandatory
FPT_KST_EXT.2 TSF Key Protection	X			Y	Mandatory
FPT_NPE_EXT.1 NPE Constraints		X		Y	Non-person entity constraints can be configured.
FPT_RCV.1 Manual Trusted Recovery	X			Y	Mandatory
FPT_SKP_EXT.1 Protection of Keys	X			Y	Mandatory
FPT_SKY_EXT.1 Split Knowledge Procedures		X		N	Split knowledge procedures are performed entirely in the operational environment.
FPT_SKY_EXT.2 Key Share Access			X	N	Key share access is performed entirely in the operational environment.
FPT_STM.1 Reliable Time Stamps	X			Y	Mandatory
FPT_TST_EXT.1 TOE Integrity Test		X		N	TSF is a virtual application.
FPT_TST_EXT.2 Integrity Test		X		N	The operational environment verifies the integrity of the TOE databases.
FPT_TUD_EXT.1 Trusted Update	X			Y	Mandatory
FTA_SSL.3 TSF-Initiated Termination		X		N	The TOE does not terminate remote interactive sessions. Session is managed by the browser, which will automatically ended after a period of inactivity.
FTA_SSL.4 User-Initiated Termination	X			Y	Mandatory
FTA_SSL_EXT.1 TSF-Initiated Session Locking		X		N	The TOE does not lock or terminate local interactive sessions.
FTA_TAB.1 Default TOE Access Banners	X			Y	Mandatory
FTP_ITC.1 Inter-TSF Trusted Channel			X	Y	Trusted channels are used.

Security Functional Requirement	M	O	S	Incl.	Rationale
FTP_TRP.1 Trusted Path	X			Y	Mandatory

Table 2, Security Functional Requirements (M – Mandatory, S – Selectable, O – Optional)

All operations performed on the IT security requirements are within the bounds set by the Protection Profile for Certification Authorities. Assignment and selection operations on security requirements are indicated in chapter 6.

3. Security Problem Definition

The security problem definition has been taken fromthe Protection Profile, ref. 8, and is reproduced here for the convenience of the reader , it includes the following parts:

- Threats;
- Organisational Security Policies, and
- Assumptions.

3.1. Threats

Threat	Description
T.PRIVILEGED_USER_ERROR	A privileged user or non-person entity (NPE) improperly exercises or adversely affects the TOE, resulting in unauthorized services, ineffective security mechanisms, or unintended circumvention of security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHENTICATED_ TRANSACTIONS	Relying parties within an information system depend on the TOE to accurately bind subjects to their credentials for use in authenticating and providing privacy for transactions. Without the proper binding provided by the TOE, relying parties cannot ensure adequate access controls on sensitive information, ensure transactional integrity, ensure proper accountability, and/or enforce nonrepudiation.
T.UNAUTHORIZED_ACCESS	A malicious user, process, or external IT entity intentionally circumvents TOE security mechanisms.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Remote users or external IT entities may take actions that adversely affect the security of the TOE.
T.USER_DATA_REUSE	A malicious user, process, or external IT entity may gain access to user data that is not cleared when resources are reallocated.
T.WEAK_CRYPTO	A weak hash or signature scheme may be compromised by an attacker and used to apply integrity checks to malicious content so that it appears legitimate

Table 3, Threats

3.2. Organisational Security Policies

Organisational Security Policy	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

Table 4, Organisational Security Policy

3.3. Assumptions

Assumption	Description
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are assumed to follow and apply all administrator guidance in a trusted manner.

Table 5, Assumption

4. Security Objectives

The security objectives has been taken from the Protection Profile, ref. 8, and is reproduced here for the convenience of the reader, it includes the following parts:

- Security objectives for the TOE;
- Security objectives for the operational environment; and
- Security objectives rationale.

4.1. Security Objectives for the TOE

Security Objective for the TOE	Description
O.AUDIT_LOSS_RESPONSE	The TOE will respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.
O.AUDIT_PROTECTION	The TOE will protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.
O.CERTIFICATES	The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.
O.CONFIGURATION_ MANAGEMENT	The TOE will conduct 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.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.INTEGRITY_PROTECTION	The TOE will provide appropriate integrity protection for TSF data and software and any user data stored by the TOE.
O.NON_REPUDIATION	The TOE will prevent a subscriber from avoiding accountability for sending a message by providing evidence that the subscriber sent the message; and control communications from unknown source.
O.PROTECTED_ COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. The TOE will protect data assets when they are being transmitted to and from the TOE, including through intervening untrusted components.
O.RECOVERY	The TOE will have the capability to store and recover to a previous state at the direction of the administrator (e.g., provide support for archival and recovery capabilities).
O.RESIDUAL_INFORMATION_ CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE will provide mechanisms that mitigate the risk of unattended sessions being hijacked.

Security Objective for the TOE	Description
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data. The TOE will record in audit records: date and time of action and the entity responsible for the action.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only privileged users are able to log in and configure the TOE, and provide protections for logged-in users. The TOE will ensure that administrative responsibilities are separated across different roles in order to mitigate the impact of improper administrative activities or unauthorized administrative access.
O.TSF_SELF_TEST	The TOE will provide integrity protection to detect modifications to firmware, software, and archived data.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and from a trusted source.

Table 6, Security Objective for the TOE

4.2. Security Objectives for the Operational Environment

Security Objective for the Operational Environment	Description
OE.CERT_REPOSITORY	The Operational Environment provides a certificate repository for storage of certificates (and optionally CRLs) issued by the TSF.
OE.CERT_REPOSITORY_ SEARCH	The Operational Environment provides the ability to search a certificate repository for specific certificate fields in certificates issued by the TSF and return the certificate and an identifier for the certificate that can be used to search the audit trail for events related to that certificate.
OE.AUDIT_RETENTION	The Operational Environment provides mechanisms for retention of audit records for both normal and extended retention periods.
OE.AUDIT_REVIEW	The Operational Environment provides a mechanism for the review of specified audit data.
OE.AUDIT_STORAGE	The Operational Environment provides a mechanism for the storage of specified audit data.
OE.CRYPTOGRAPHY	The Operational Environment provides cryptographic services that can be invoked by the TSF in order to perform security functionality.
OE.KEY_ARCHIVAL	The Operational Environment provides the ability to use split knowledge procedures to enforce two party control to export keys necessary to resume CA functionality if the TSF should fail.

Security Objective for the Operational Environment	Description
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.PUBLIC_KEY_PROTECTION	The Operational Environment provides protection for specified public keys associated with CA functions.
OE.SESSION_PROTECTION_ LOCAL	The Operational Environment provides the ability to lock or terminate local administrative sessions.
OE.SESSION_PROTECTION_ REMOTE	The Operational Environment provides the ability to lock or terminate remote administrative sessions.
OE.TOE_ADMINISTRATION	The Operational Environment provides specified management capabilities required for the overall operation of a Certificate Authority, and the ability to restrict access to a subset of the capabilities as specified in the ST.
OE.TRUSTED_ADMIN	The administrator of the TOE is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
OE.TRUSTED_PLATFORM	The operating system on which the TOE has been installed is securely configured, regularly patched, and not subject to unauthorized access.

Table 7, Security Objectives for the Operational Environment

4.3. Security Objectives Rationale

The security objectives rationale is copied from the Protection Profile for Certification Authorities.

SPD Element	Objective	Requirements
A.NO_GENERAL_PURPOSE It is assumed that there are no general purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	**OE.NO_GENERAL_PURPOSE** There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	N/A
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	**OE.PHYSICAL** Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	N/A
A.TRUSTED_ADMIN TOE Administrators are assumed to follow and apply all administrator guidance in a trusted manner.	**OE.TRUSTED_ADMIN** The administrator of the TOE is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.	N/A

SPD Element	Objective	Requirements
T.PRIVILEGED_USER_ERROR A privileged user or non-person entity (NPE) improperly exercises or adversely affects the TOE, resulting in unauthorized services, ineffective security mechanisms, or unintended circumvention of security mechanisms.	**O.AUDIT_LOSS_RESPONSE** The TOE will respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.	FAU_ADP_EXT.1, FAU_STG.4
	O.AUDIT_PROTECTION The TOE will protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.	FAU_ADP_EXT.1
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only privileged users are able to log in and configure the TOE, and provide protections for logged-in users. The TOE will ensure that administrative responsibilities are separated across different roles in order to mitigate the impact of improper administrative activities or unauthorized administrative access.	FIA_PMG_EXT.1, FIA_UAU.7, FIA_UAU_EXT.1, FIA_UIA_EXT.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MTD.1, FMT_SMF.1, FMT_SMR.2, FPT_APW_EXT.1, FTA_SSL.4
	OE.AUDIT_GENERATION The Operational Environment provides a mechanism for the generation of portions of the audit data.	
	OE.AUDIT_STORAGE The Operational Environment provides a mechanism for the storage of specified audit data.	
	OE.AUDIT_REVIEW The Operational Environment provides a mechanism for the review of specified audit data.	
	OE.AUDIT_RETENTION The Operational Environment provides mechanisms for retention of audit records for both normal and extended retention periods.	
	OE.SESSION_PROTECTION_LOCAL The Operational Environment provides the ability to lock or terminate local administrative sessions.	
	OE.SESSION_PROTECTION_REMOTE The Operational Environment provides the ability to lock or terminate remote administrative sessions.	
	OE.TOE_ADMINISTRATION The Operational Environment provides specified management capabilities required for the overall operation of a Certificate Authority, and the ability to restrict access to a subset of the capabilities as specified in the ST	
	OE.TRUSTED_PLATFORM The operating system on which the TOE has been installed is securely configured,	

SPD Element	Objective	Requirements
	regularly patched, and not subject to unauthorized access.	
T.UNAUTHENTICATED_TRANSACTIONS Relying parties within an information system depend on the TOE to accurately bind subjects to their credentials for use in authenticating and providing privacy for transactions. Without the proper binding provided by the TOE, relying parties cannot ensure adequate access controls on sensitive information, ensure transactional integrity, ensure proper accountability, and/or enforce non-repudiation.	**O.CERTIFICATES** The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.	FDP_CER_EXT.1, FDP_CER_EXT.2, FDP_CER_EXT.3, FDP_CRL_EXT.1, FDP_CSI_EXT.1, FDP_OCSPG_EXT.1, FIA_ESTS_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FPT_NPE_EXT.1
	O.CONFIGURATION_MANAGEMENT The TOE will conduct 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.	FDP_CER_EXT.1, FDP_CRL_EXT.1, FDP_OCSPG_EXT.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MTD.1, FPT_NPE_EXT.1
	O.INTEGRITY_PROTECTION The TOE will provide appropriate integrity protection for TSF data and software and any user data stored by the TOE.	FCS_CDP_EXT.1, FDP_ITT.1, FPT_ITT.1,
	O.NON_REPUDIATION The TOE will prevent a subscriber from avoiding accountability for sending a message by providing evidence that the subscriber sent the message; and control communications from unknown source.	FCO_NRO_EXT.2, FCO_NRR_EXT.2
	OE.PUBLIC_KEY_PROTECTION The Operational Environment provides protection for specified public keys associated with CA functions	
	OE.TOE_ADMINISTRATION The Operational Environment provides specified management capabilities required for the overall operation of a Certificate Authority, and the ability to restrict access to a subset of the capabilities as specified in the ST	
T.UNAUTHORIZED_ACCESS A malicious user, process, or external IT entity intentionally circumvents TOE security mechanisms.	**O.PROTECTED_COMMUNICATIONS** The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. The TOE will protect data assets when they are being transmitted to and from the TOE, including through intervening untrusted components.	FCS_CDP_EXT.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_STG_EXT.1, FCS_TLSC_EXT.2, FDP_ITT.1, FPT_ITT.1 FPT_KST_EXT.1, FPT_KST_EXT.2, FPT_SKP_EXT.1,

SPD Element	Objective	Requirements
		FTP_ITC.1, FTP_TRP.1
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only privileged users are able to log in and configure the TOE, and provide protections for logged-in users. The TOE will ensure that administrative responsibilities are separated across different roles in order to mitigate the impact of improper administrative activities or unauthorized administrative access.	FIA_PMG_EXT.1, FIA_UAU.7, FIA_UAU_EXT.1, FIA_UIA_EXT.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), FMT_MOF.1(4), FMT_MOF.1(5), FMT_MTD.1, FMT_SMF.1, FMT_SMR.2, FPT_APW_EXT.1, FTA_SSL.4
	OE.CRYPTOGRAPHY The Operational Environment provides cryptographic services that can be invoked by the TSF in order to perform security functionality.	
	OE.KEY_ARCHIVAL The Operational Environment provides the ability to use split knowledge procedures to enforce two-party control to export keys necessary to resume CA functionality if the TSF should fail.	
	OE.SESSION_PROTECTION_LOCAL The Operational Environment provides the ability to lock or terminate local administrative sessions.	
	OE.SESSION_PROTECTION_REMOTE The Operational Environment provides the ability to lock or terminate remote administrative sessions.	
	OE.TOE_ADMINISTRATION The Operational Environment provides specified management capabilities required for the overall operation of a Certificate Authority, and the ability to restrict access to a subset of the capabilities as specified in the ST	
T.UNAUTHORIZED_UPDATE A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.	**O.VERIFIABLE_UPDATES** The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and from a trusted source.	FCS_CDP_EXT.1, FCS_COP.1(2), FIA_X509_EXT.2, FPT_TUD_EXT.1
T.UNDETECTED_ACTIONS Remote users or external IT entities may take actions that adversely affect the security of the TOE.	**O.AUDIT_LOSS_RESPONSE** The TOE will respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.	FAU_ADP_EXT.1, FAU_STG.4
	O.AUDIT_PROTECTION The TOE will protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.	FAU_ADP_EXT.1
	O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and send those data to an external IT entity. The TOE will record in	FAU_ADP_EXT.1, FAU_GEN.1, FAU_GEN.2 FAU_SAR.1

SPD Element	Objective	Requirements
	audit records: date and time of action and the entity responsible for the action.	FAU_SAR.3 FAU_GCR_EXT.1, FAU_SEL.1 FAU_STG_EXT.1, FIA_UIA_EXT.1, FPT_STM.1
	OE.AUDIT_GENERATION The Operational Environment provides a mechanism for the generation of portions of the audit data.	
	OE.AUDIT_STORAGE The Operational Environment provides a mechanism for the storage of specified audit data.	
	OE.AUDIT_REVIEW The Operational Environment provides a mechanism for the review of specified audit data.	
	OE.AUDIT_RETENTION The Operational Environment provides mechanisms for retention of audit records for both normal and extended retention periods.	
	OE.CERT_REPOSITORY The Operational Environment provides a certificate repository for storage of certificates (and optionally CRLs) issued by the TSF.	
	OE.CERT_REPOSITORY_SEARCH The Operational Environment provides the ability to search a certificate repository for specific certificate fields in certificates issued by the TSF and return the certificate and an identifier for the certificate that can be used to search the audit trail for events related to that certificate.	
T.USER_DATA_REUSE A malicious user, process, or external IT entity may gain access to user data that is not cleared when resources are reallocated.	**O.RESIDUAL_INFORMATION_CLEARING** The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.	FDP_RIP.1
T.WEAK_CRYPTO A weak hash or signature scheme may be compromised by an attacker and used to apply integrity checks to malicious content so that it appears legitimate.	**O.PROTECTED_COMMUNICATIONS** The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. The TOE will protect data assets when they are being transmitted to and from the TOE, including through intervening untrusted components.	FCS_CDP_EXT.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_STG_EXT.1, FCS_TLSC_EXT.2, FDP_ITT.1, FPT_ITT.1 FPT_KST_EXT.1, FPT_KST_EXT.2, FPT_SKP_EXT.1,

SPD Element	Objective	Requirements
		FTP_ITC.1, FTP_TRP.1
	O.VERIFIABLE_UPDATES The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and from a trusted source.	FCS_CDP_EXT.1, FCS_COP.1(2), FIA_X509_EXT.2, FPT_TUD_EXT.1
	OE.CRYPTOGRAPHY The Operational Environment provides cryptographic services that can be invoked by the TSF in order to perform security functionality.	
	OE.KEY_ARCHIVAL The Operational Environment provides the ability to use split knowledge procedures to enforce two-party control to export keys necessary to resume CA functionality if the TSF should fail.	
P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.	**O.DISPLAY_BANNER** The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1

Table 8, Security Objectives Rationale

5. Extended Components Definition

Extended components have been defined in the Protection Profile for Certification Authorities.

Extended security requirements are explicitly identified in Table 9 and thoroughly described in the PP.

Extended Components
FAU_ADP_EXT.1 Audit Dependencies
FAU_GCR_EXT.1 Generation of Certificate Repository
FAU_STG_EXT.1 External Audit Trail Storage
FCO_NRO_EXT.2 Certificate-Based Proof of Origin
FCO_NRR_EXT.2 Certificate-Based Proof of Receipt
FCS_CDP_EXT.1 Cryptographic Dependencies
FCS_CKM_EXT.4 Cryptographic Key Destruction
FCS_HTTPS_EXT.1 HTTPS Protocol
FCS_RBG_EXT.1 Cryptographic Random Bit Generation
FCS_STG_EXT.1 Cryptographic Key Storage
FCS_TLSC_EXT.2 TLS Client Protocol with Mutual Authentication
FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication
FDP_CER_EXT.1 Certificate Profiles
FDP_CER_EXT.2 Certificate Request Matching
FDP_CER_EXT.3 Certificate Issuance Approval
FDP_CRL_EXT.1 Certificate Revocation List Validation
FDP_CSI_EXT.1 Certificate Status Information
FDP_OCSPG_EXT.1 OCSP Basic Response Generation
FIA_ESTS_EXT.1 Enrollment over Secure Transport (EST) Server
FIA_PMG_EXT.1 Password Management
FIA_X509_EXT.1 Certificate Validation
FIA_X509_EXT.2 Certificate-Based Authentication
FIA_X509_EXT.3 X509 Certificate Request
FIA_UAU_EXT.1 Authentication Mechanism
FIA_UIA_EXT.1 User Identification and Authentication
FPT_APW_EXT.1 Protection of Privileged User Passwords
FPT_KST_EXT.1 No Plaintext Key Export
FPT_KST_EXT.2 TSF Key Protection
FPT_NPE_EXT.1 NPE Constraints
FPT_SKP_EXT.1 Protection of Keys
FPT_TUD_EXT.1 Trusted Update

Table 9, Extended components

6. Security Requirements

The security requirements are based on the Protection Profile, ref. 8, and include the following parts:

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

6.1. Security Functional Requirements

The following conventions have been applied in this document. Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.

- Iteration: Allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parenthesis placed at the end of the component. For example FCS_COP.1 (1) and FCS_COP.1(2) indicate that the ST includes two iterations of the FCS_COP.1 requirement, “1” and “2”.
- Assignment: Allows the specification of an identified parameter. Assignments performed in the Protection Profile, ref. 8, are copied into this ST in plain text surrounded by brackets (e.g., [assignment]). Assignments performed in this ST are indicated using ***bold italics*** and are surrounded by brackets (e.g., [***assignment***]).
- Selection: Allows the specification of one or more elements from a list. Selections performed in the Protection Profile, ref. 8, are copied into this ST in plain text surrounded by brackets (e.g., [assignment]). Selections performed in this ST are indicated using **bold** and are surrounded by brackets (e.g., [**selection**]).
- Refinements performed in the Protection Profile, ref. 8, are copied into this ST in plain text and are identified with "Refinement:" right after the short name. Additions to the CC text are specified in plain underlined text. Refinements performed in this ST are identified with "**Refinement**:" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.

6.1.1. Security Audit (FAU)

Table 10 describes the TOE SFRs related to security audit

FAU_ADP_EXT.1	**Audit Dependencies**
FAU_ADP_EXT.1.1	The TSF shall implement audit functionality and [**no additional audit functionality**] in order to perform audit operations on the following audit data: [***Auditable events in Table 11 through Table 13 that require persistent storage***].
FAU_GCR_EXT.1	**Generation of Certificate Repository**
FAU_GCR_EXT.1.1	The TSF shall [**invoke the Operational Environment to store**] certificates and [**CRLs**] issued by the TSF.

FAU_GEN.1	**Audit data generation**
FAU_GEN.1.1	**Refinement**: The TSF shall generate ***and [no other actions]*** an audit record of the following auditable events: a) Start-up of the **TSF** audit functions; b) All auditable events for the [not specified*]* level of audit; and c) All administrative actions invoked through the TSF interface; d) [***Specifically defined auditable events listed in Table 11 through Table 13***].
FAU_GEN.1.2	**Refinement:** The TSF shall **[include]** within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***information specified in column three of Table 11 through Table 13***]].
FAU_GEN.2	**User identity association**
FAU_GEN.2.1	**Refinement:** For audit events resulting from 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_SAR.1	**Audit Review**
FAU_SAR.1.1	The TSF shall provide [Auditors] with the capability to read all information from the audit records.
FAU_SAR.1.2	**Refinement**: The TSF shall provide the audit records in a manner suitable for the ***Auditor*** to interpret the information.
FAU_SAR.3	**Selectable Audit Review**
FAU_SAR.3.1	The TSF shall provide the ability to apply [searches] of audit data based on [***serial number***] associated with the event.
FAU_SEL.1	**Selective Audit**

FAU_SEL.1.1	**Refinement:** The TSF shall be able to select the set of events to be audited ***by specific mechanisms*** from the set of all auditable events based on the following attributes: a) [**object identity, user identity, subject identity, host identity, event type**] b) [***time, outcome, module, certificate authority***].
FAU_STG.4	**Prevention of audit data loss**
FAU_STG.4.1	**Refinement:** The TSF shall [prevent audited events, except those taken by the **Auditor**] and [**generate an error message according to FPT_FLS.1]** if the audit trail ***cannot be written to***.
FAU_STG_EXT.1	**External Audit Trail Storage**
FAU_STG_EXT.1.1	The TSF shall maintain availability and integrity of audit data by storing it [**locally on the TOE, locally on the TOE platform]**.

Table 10, FAU Security Audit

Table 11 describes the auditable events and respective data.

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/ Extended	Responsible TSF or OE Component
FAU_ADP_EXT.1	None.	None.	N/A	
FAU_GCR_EXT.1	None.	None.	N/A	
FAU_GEN.1	None.	None.	N/A	
FAU_GEN.2	None.	None.	N/A	
FAU_STG.4	None.	None.	N/A	
FCO_NRO_EXT.2	None.	None.	N/A	
FCS_CDP_EXT.1	None.	None.	N/A	
FCS_STG_EXT.1	None.	None.	N/A	
FDP_CER_EXT.1	Certificate generation.	Success: [*Certificate object identifier*]. **Note**: The certificate object identifier is a hyperlink to the certificate value.	Extended	TSF

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/ Extended	Responsible TSF or OE Component
FDP_CER_EXT.2	Linking of certificate to certificate request	Success: [*Certificate object identifier*], [*Certificate request*]. Failure: Reason for failure, [*Certificate request*].	Extended	TSF
FDP_CER_EXT.3	Failed certificate approvals.	Reason for failure. [*Certificate request*].	Normal	TSF
FDP_CSI_EXT.1	None.	None.	N/A	
FDP_RIP.1	None.	None.	N/A	
FIA_X509_EXT.1	Failed certificate validations.	None.	Normal	OE
FIA_X509_EXT.2	Failed authentications.	None.	Normal	OE
FIA_UAU_EXT.1a	All uses of the authentication mechanism used for access to TOE related functions.	Origin of the attempt (e.g., IP address).	Normal	TSF
FIA_UAU_EXT.1b	All uses of the authentication mechanism used for access to TOE related functions.	Origin of the attempt (e.g., IP address).	Normal	TSF
FIA_UIA_EXT.1	All use of the identification and authentication mechanism used for TOE related roles.	Provided user identity. Origin of the attempt (e.g., IP address).	Normal	TSF
FMT_MOF.1(1)	None.	None.	N/A	
FMT_MOF.1(2)	None.	None.	N/A	
FMT_MOF.1(3)	None.	None.	N/A	
FMT_MOF.1(4)	None.	None.	N/A	
FMT_MOF.1(5)	None.	None.	N/A	
FMT_MTD.1	None.	None.	N/A	
FMT_SMF.1	None.	None.	N/A	
FMT_SMR.2	Modifications to the group of users that are part of a role.	Modifications to the group of users that are part of a role.	Extended	TSF

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/ Extended	Responsible TSF or OE Component
FPT_FLS.1	Invocation of failures under this requirement.	Indication that the TSF has failed with the type of failure that occurred.	Normal	TSF
FPT_KST_EXT.1	None.	None.	N/A	
FPT_KST_EXT.2	All unauthorized attempts to use TOE secret and private keys.	Identifier of user or process that attempted access.	Normal	OE
FPT_RCV.1	The fact that a failure or service discontinuity occurred; resumption of the regular operation.	The type of failure or service discontinuity.	Extended	TSF
FPT_SKP_EXT.1	None.	None.	N/A	
FPT_STM.1	Changes to the time.	The old and new values for the time.	Normal	OE
FPT_TUD_EXT.1	Initiation of update.	Version number.	Extended	OE
FTA_SSL.4	The termination of an interactive session.	None.	Normal	TSF
FTA_TAB.1	None.	None.	N/A	
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.	Normal	OE

Table 11, Auditable Events and Audit Data

Table 12 describes the auditable events and respective data for optional requirements.

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
FCS_COP.1(5)	None.	None.	N/A	
FPT_SKY_EXT.1	None.	None.	N/A	
FPT_TST_EXT.1	Execution of this set of TSF integrity tests.	For integrity violations, the identity of the object that	Normal	N/A

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
	Detected integrity violations.	caused the integrity violation.		
FPT_TST_EXT.2	Execution of this set of TSF integrity tests. Detected integrity violations.	For integrity violations, the identity of the object that caused the integrity violation.	Normal	N/A
FDP_CER_EXT.4	Certificate generation.	Name/identifier of certificate, value of certificate generated.	Extended	N/A
FDP_SDP_EXT.1	None.	None.	N/A	N/A
FDP_STG_EXT.1	Changes to the trusted public keys and certificates relevant to TOE functions, including additions and deletions.	The public key and all context information associated with the key.	Normal	N/A
FPT_NPE_EXT.1	All changes to NPE rule sets and NPE associations.	The changes made to the NPE rule sets and associations.	Extended	TSF
FTA_SSL.3	The termination of a remote session by the session termination mechanism.	None.	Normal	N/A
FTA_SSL_EXT.1	Any attempts at unlocking or termination of an interactive session.	None.	Normal	N/A

Table 12, Auditable Events for Optional Requirements

Table 13 describes the auditable events and respective data for selectable requirements.

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
FAU_SCR_EXT.1	None.	None.	N/A	
FAU_SAR.1	None.	None.	N/A	
FAU_SAR.3	None.	None.	N/A	
FAU_SEL.1	All	None.	Normal	TSF

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
	modifications to the audit configuration that occur while the audit collection functions are operating.			
FAU_STG.1(1)	None	None.	N/A	
FAU_STG.1(2)	None	None	N/A	
FAU_STG_EXT.1	None.	None.	N/A	
FAU_STG_EXT.2	None,	None.	N/A	
FCO_NRR_EXT.2	None.	None.	N/A	
FCS_CKM.1	All occurrences of non- ephemeral and [selection: ephemeral, no other] key generation for TOE related functions.	Success: public key generated	Normal	OE
FCS_CKM.2	All occurrences of nonephemeral and [*selection: ephemeral, no other*] key establishment for TOE related functions.	Success: key established	Normal	OE
FCS_CKM_EXT.1(1)	None.	None.	N/A	
FCS_CKM_EXT.1(2)	None.	None.	N/A	
FCS_CKM_EXT.1(3)	None	None.	N/A	
FCS_CKM_EXT.1(4)	None.	None.	N/A	
FCS_CKM_EXT.4	Failure of the key destruction process for TOE related keys.	Identity of object or entity being cleared.	Normal	OE
FCS_CKM_EXT.5	Detection of integrity violation for stored TSF data.	None.	Normal	N/A
FCS_CKM_EXT.6	All key archival actions.	None.	Extended	N/A

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
FCS_CKM_EXT.7	None.	None.	N/A	
FCS_CKM_EXT.8	None.	None.	N/A	
FCS_COP.1(1)	None.	None.	N/A	
FCS_COP.1(2)	All occurrences of signature generation using a CA signing key. Failure in signature generation	Name/identifier of object being signed Identifier of key used for signing. None.	Extended Normal	OE
FCS_COP.1(3)	None.	None.	N/A	
FCS_COP.1(4)	None.	None.	N/A	
FCS_HTTPS_EXT.1	Failure to establish a HTTPS session. Establishment/ Termination of a HTTPS	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and	Normal	OE
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment/ Termination of an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	Normal	N/A
FCS_RBG_EXT.1	None.	None.	N/A	
FCS_TLSC_EXT.2	Failure to establish a TLS session. Establishment/ Termination of a TLS session.	Reason for failure. None.	Normal	
FCS_TLSS_EXT.1	Failure to establish a TLS session. Establishment/ Termination of a TLS session.	Reason for failure. None.	Normal	N/A
FCS_TLSS_EXT.2	Failure to establish a TLS session.	Reason for failure.	Normal	

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
	Establishment/Termination of a TLS session.	None.		
FDP_CRL_EXT.1	Failure to generate CRL.	None.	Normal	
FDP_ITT.1	None.	None.	N/A	
FDP_OCSPG_EXT.1	Failure to generate certificate status information.	None.	Extended	TSF
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts. The action taken. The reenablement of disabled nonadministrative accounts.	None.	Normal	N/A
FIA_CMCS_EXT.1	CMC requests (generated or received) containing certificate requests or revocation requests. CMC responses issued.	Identifiers for all entities authenticating the request, including the entity providing client authentication for the CMC transport (if any). The submitted request. Any signed response	Extended	N/A
FIA_CMCC_EXT.1	CMC requests (generated or received) containing certificate requests or revocation requests. CMC responses issued.	Identifiers for all entities authenticating the request, including the entity providing client authentication for the CMC transport (if any). The submitted request. Any signed response.	Extended	N/A

Requirement	Auditable Events	Additional Audit Record Contents	Retention Normal/Extended	Responsible TSF or OE Component
FIA_ESTC_EXT.1	EST requests (generated or received) containing certificate requests or revocation requests. EST responses issued.	Identifiers for all entities authenticating the request, including the entity providing client authentication for the EST transport (if any). The submitted request. Any signed response.	Extended	N/A
FIA_ESTS_EXT.1	EST requests (generated or received) containing certificate requests or revocation requests. EST responses issued.	Identifiers for all entities authenticating the request, including the entity providing client authentication for the EST transport (if any). The submitted request. Any signed response.	Extended	TSF
FIA_PMG_EXT.1	None.	None.	N/A	
FIA_PSK_EXT.1	None.	None.	N/A	
FIA_UAU.7	None.	None.	N/A	
FPT_APW_EXT.1	None.	None.	N/A	
FPT_ITT.1	None.	None.	N/A	
FPT_SKY_EXT.2	Access control violations for users involved in key share establishment or control.	None.	Extended	N/A
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	Normal	OE

Table 13, Auditable Events for Selection-Based Requirements

6.1.2. Communication (FCO)

FCO_NRO_EXT.2	Certificate-Based Proof of Origin
FCO_NRO_EXT.2.1	The TSF shall provide proof of origin for certificates it issues in accordance with the digital signature requirements using a mechanism in accordance with RFC 5280 and FCS_COP.1(2).
FCO_NRO_EXT.2.2	The TSF shall provide proof of origin for certificate status information it issues in accordance with the digital signature requirements in [**CRLs (RFC 5280), OCSP (RFC 6960),** ***[OCSP (RFC 2560)]]*** and FCS_COP.1(2).
FCO_NRO_EXT.2.3	The TSF shall require and verify proof of origin for certificate requests it receives [**EST using mechanisms in accordance with FIA_ESTS_EXT.1**].
FCO_NRO_EXT.2.4	The TSF shall require and verify proof of origin for public keys contained in certificate requests it receives via [**proof-of-possession mechanisms in EST in accordance with FIA_ESTS_EXT.1**].
FCO_NRO_EXT.2.5	The TSF shall [require and verify proof of origin for revocation requests it receives via [**EST using optional "full CMC" functionality in accordance with FIA_ESTS_EXT.1***]*, *[**support manual processes for revocation requests and responses***]].
FCO_NRR_EXT.2	**Certificate-Based Proof of Receipt**
FCO_NRR_EXT.2.1	The TSF shall provide proof of receipt for [**EST**] by providing signed responses using mechanisms in accordance with [**FIA_ESTS_EXT.1**].

Table 14, FCO - Communication

6.1.3. Cryptographic Support (FCS)

FCS_CDP_EXT.1	Cryptographic Dependencies
FCS_CDP_EXT.1.1	The TSF shall [**invoke interfaces provided by the Operational Environment**] in order to perform [**all**] cryptographic operations.
FCS_CKM.1	**Cryptographic Key Generation**
FCS_CKM.1.1	**Refinement:** The TSF shall **[invoke interfaces provided by the Operational Environment to generate] *asymmetric*** cryptographic keys in accordance with the specified key generation algorithm: **[** • **RSA schemes using cryptographic key sizes of 2048- and 3072-bit that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;** • **ECC schemes using "NIST curves" [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;** • **FFC schemes using cryptographic key sizes of 2048- and 3072-bit that meet the following: FIPS PUB 186-4, "Digital Signature**

	Standard (DSS)", Appendix B.1] and specified cryptographic key sizes [*assignment*: *equivalent to or greater than a symmetric key strength of 112 bits*] ~~*that meet the following: [assignment: list of standards]*~~.**
FCS_CKM.2	**Cryptographic Key Establishment**
FCS_CKM.2.1	**Refinement:** The TSF shall **[invoke interfaces provided by the Operational Environment to perform] key establishment** in accordance with a specified cryptographic key **establishment** algorithm **[** • RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2; • Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"; • Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"; • Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3] ~~*that meet the following: [assignment: list of standards*~~].
FCS_CKM_EXT.4	**Cryptographic Key Destruction**
FCS_CKM_EXT.4.1	The TSF shall [**invoke interfaces provided by the Operational Environment to destroy**] all cryptographic keys and critical security parameters which are not permanently protected from export by hardware when no longer required, in accordance with the specified cryptographic key destruction method [• **for volatile memory, the destruction shall be executed by a [** removal of the power to the memory]**,** • **for non-volatile memory that consists of the invocation of an interface provided by the underlying platform that [** instructs the underlying platform to destroy the abstraction that represent the key]]
FCS_CKM_EXT.4.2	The TSF shall [**invoke interfaces provided by the Operational Environment to destroy**] all plaintext keying material cryptographic security parameters when no longer needed.
FCS_COP.1(1)	**Cryptographic Operation (AES Encryption/Decryption)**
FCS_COP.1.1(1)	**Refinement:** The TSF shall **[invoke interfaces in the operational environment to perform]** [*encryption and decryption*] in accordance with a specified cryptographic algorithm: **[** • **AES-CBC (as defined in NIST SP 800-38A) mode,** • **AES-CCM (as defined in NIST SP 800-38C) mode,**

	• **AES-GCM (as defined in NIST SP 800-38D) mode,** • **AES Key Wrap (KW) (as defined in NIST SP 800-38F) mode** • **AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F) mode]** and cryptographic key size ***[*128-bit, 256-bit**] ~~***that meet the following: [assignment: list of standards***~~ **]**.
FCS_COP.1(2)	**Cryptographic Operation (Cryptographic Signature)**
FCS_COP.1.1(2)	**Refinement**: The TSF shall [**invoke interfaces in the operational environment to perform**] [*cryptographic signature services*] in accordance with the following specified cryptographic algorithms [• **RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of [2048 and 3072 bits] that meets FIPS-PUB 186-4, "Digital Signature Standard",** • **Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256, 384, or 512 bits that meets FIPS PUB 186-4, "Digital Signature Standard" with "NIST curves" P-256, P-384 and [P-521] (as defined in FIPS PUB 186-4, "Digital Signature Standard"),** • **Digital Signature Algorithm (DSA) with a key size (modulus) of 2048 and 3072 bits, that meets FIPS-PUB 186-4, "Digital Signature Standard"*] ~~and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.**
FCS_COP.1(3)	**Cryptographic Operation (Cryptographic Hashing)**
FCS_COP.1.1(3)	**Refinement:** The TSF shall **[invoke interfaces in the operational environment to perform]** [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm **[***SHA-256, SHA-384, SHA-512***] *and message digest sizes [256, 384, 512] bits*** that meet the following: [*FIPS Pub 180-4, "Secure Hash Standard"*].
FCS_COP.1(4)	**Cryptographic Operation (Keyed-Hash Message Authentication)**
FCS_COP.1.1(4)	**Refinement:** The TSF shall **[invoke interfaces in the operational environment to perform]** [keyed hash message authentication] in accordance with a specified cryptographic algorithm ***HMAC-[SHA-256, SHA-384, SHA-512], key size [256, 384, 512] and message digest sizes [256, 384, 512] bi*****ts** that meet the following: [FIPS Pub 198-1,"The Keyed Hash Message Authentication Code"; FIPS Pub 180-4, "Secure Hash Standard"].
FCS_HTTPS_EXT.1	**HTTPS Protocol**
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS.
FCS_RBG_EXT.1	**Cryptographic Random Bit Generation**
FCS_RBG_EXT.1.1	The TSF shall [**invoke interfaces in the operational environment to perform***] all deterministic random bit generation (RBG) services in accordance with NIST Special Publication 800-90A using [**CTR_DRBG(AES)**].
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [**an Operational Environment-based noise source**] with a minimum of [**128 bits**] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and authorization factors that it will generate.

FCS_STG_EXT.1	**Cryptographic Key Storage**
FCS_STG_EXT.1.1	Persistent private and secret keys shall be stored within the [**Operational Environment***] [***in a hardware cryptographic module**].
FCS_TLSC_EXT.2	**TLS Client Protocol with Mutual Authentication**
FCS_TLSC_EXT.2.1	The TSF shall implement [**TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)**] supporting the following ciphersuites: [• **TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268** • **TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268** • **TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268** • **TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268** • **TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246** • **TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246** • **TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288** • **TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288** • **TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288** • **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288** *].*
FCS_TLSC_EXT.2.2	The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.
FCS_TLSC_EXT.2.3	The TSF shall establish a trusted channel only if the peer certificate is valid.
FCS_TLSC_EXT.2.4	The TSF shall [**present the Supported Elliptic Curves Extension with the following NIST curves: [None] *and no other curves***] in the Client Hello.
FCS_TLSC_EXT.2.5	The TSF shall support mutual authentication using X.509v3 certificates.
FCS_TLSS_EXT.2	**TLS Server Protocol with Mutual Authentication**
FCS_TLSS_EXT.2.1	The TSF shall implement [**TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)***] supporting the following ciphersuites: [• **TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268** • **TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268** • **TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268** • **TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268** • **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492** • **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492** • **TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246** • **TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246** • **TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288** • **TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288** • **TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288** • **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289** • **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289**

	• **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289** • **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289** • **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289** • **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289** • **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]** and no other ciphersuite.
FCS_TLSS_EXT.2.2	The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [**no other TLS versions**].
FCS_TLSS_EXT.2.3	The TSF shall [**perform RSA key establishment with key size [selection: 2048 bits, 3072 bits,]; generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size 2048 bits and [3072 bits**]].
FCS_TLSS_EXT.2.4	The TSF shall support mutual authentication of TLS clients using X.509 certificates.
FCS_TLSS_EXT.2.5	For communications configured to require TLS with mutual authentication, the shall not establish a trusted channel if the client certificate is invalid.
FCS_TLSS_EXT.2.6	The TSF shall respond with a fatal TLS error if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate presented for client authentication does not match the expected identifier for the client.

Table 15, FCS - Cryptographic Support

6.1.4. User Data Protection (FDP)

FDP_CER_EXT.1	**Certificate Profiles**
FDP_CER_EXT.1.1	The TSF shall implement a certificate profile function and shall ensure that issued certificates are consistent with configured profiles.
FDP_CER_EXT.1.2	The TSF shall generate certificates using profiles that comply with requirements for certificates as specified in IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, while ensuring that the following conditions are met: a) The version field shall contain the integer 2. b) The issuerUniqueID or subjectUniqueID fields are not populated. c) The serialNumber shall be unique with respect to the issuing Certification Authority. d) 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. e) The issuer field is not empty. f) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a signature algorithm specified in FCS_COP.1(2). g) The following extensions are supported: a. subjectKeyIdentifier b. authorityKeyIdentifier c. basicConstraints d. keyUsage e. extendedKeyUsage

	f. certificatePolicy h) A subject field containing a null Name (e.g., a sequence of zero relative distinguished names) is accompanied by a populated critical subjectAltName extension. i) The subjectKeyIdentifier extension is populated with a value unique for each public key contained in a certificate issued by the TSF. j) The authorityKeyIdentifier extension in any certificate issued by the TOE must be populated and must be the same as the subjectKeyIdentifier extension contained in the issuer's signing certificate. k) Populated keyUsage and extendedKeyUsage fields in the same certificate contain consistent values.
FDP_CER_EXT.1.3	The TSF shall be able to generate at least 20 bits of random for use in issued certificates to be included in [**serialNumber**] fields, where the random values are generated in accordance with FCS_RBG_EXT.1.
FDP_CER_EXT.2	**Certificate Request Matching**
FDP_CER_EXT.2.1	The TSF shall establish a linkage from certificate requests to issued certificates.
FDP_CER_EXT.3	**Certificate Issuance Approval**
FDP_CER_EXT.3.1	The TSF shall support the approval of certificates by [**RA/VA**] issued according to a configured certificate profile.
FDP_CRL_EXT.1	**Certificate Revocation List Validation**
FDP_CRL_EXT.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: a) If the version field is present, then it shall contain a 1. b) If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1. c) 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. d) The signature and signatureAlgorithm fields shall contain the OID for a digital signature algorithm in accordance with FCS_COP.1(2). e) The thisUpdate field shall indicate the issue date of the CRL. f) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.
FDP_CSI_EXT.1	**Certificate Status Information**
FDP_CSI_EXT.1.1	The TSF shall provide certificate status information whose format complies with [**ITU-T Recommendation X.509v2 CRL, the OCSP standard as defined by [RFC 6960, RFC 2560**]].
FDP_CSI_EXT.1.2	The TSF shall support the approval of changes to the status of a certificate by [**RA**].

FDP_ITT.1	Basic Internal Transfer Protection
FDP_ITT.1.1	**Refinement**: The TSF shall ~~***enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to***~~ prevent the [*disclosure, modification*] of user data when it is transmitted between physically separated parts of the TOE ***through the use of [TLS, TLS/HTTPS].***
FDP_OCSPG_EXT.1	**OCSP Basic Response Generation**
FDP_OCSPG_EXT.1.1	The TSF shall ensure that all mandatory fields in the OCSP response contain values in accordance with the standards specified in FDP_CSI_EXT.1. At a minimum, the following items shall be enforced: a) The version field shall indicate a current version. b) The signatureAlgorithm field shall contain the object identifier (OID) for a digital signature algorithm in accordance with FCS_COP.1(2). c) The thisUpdate field shall indicate the time at which the status being indicated is known to be correct. d) The producedAt field shall indicate the time at which the OCSP responder signed the response. e) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.
FDP_RIP.1	**Subset Residual Information Protection**
FDP_RIP.1.1	**Refinement**: The TSF ***and [Operational Environment]*** shall ensure that any previous information content of a resource is made unavailable upon the [**deallocation of the resource from**] the following objects: [***secret and ephemeral keys, passwords***].

Table 16, FDP - User Data Protection

6.1.5. Identification and Authentication (FIA)

FIA_ESTS_EXT.1	Enrollment over Secure Transport (EST) Server
FIA_ESTS_EXT.1.1	The TSF shall use the Enrollment over Secure Transport (EST) protocol as specified in RFC 7030 to receive, process, and respond to certificate simple enrollment requests from authorized clients.
FIA_ESTS_EXT.1.2	The TSF shall authenticate EST clients for re-enrollment via TLS certificate-based mutual authentication in accordance with RFC 7030 Section 3.3.2 and FCS_TLSS_EXT.2.
FIA_ESTS_EXT.1.3	The TSF shall authenticate EST clients for initial enrollment and for supplemental authentication via [**HTTP basic authentication in accordance with RFC7030 section 3.2.3; TLS certificate-based mutual authentication in accordance with RFC 7030 section 3.3.2 and FCS_TLSS_EXT.2**]
FIA_ESTS_EXT.1.4	The TSF shall authorize EST clients based on [[***policy used by the TOE to determine client authorization in accordance with RFC 7030 section 3.7***]].

FIA_PMG_EXT.1	**Password Management**
FIA_PMG_EXT.1.1	The TSF shall provide the following password management capabilities for privileged passwords: • Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters:[**“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”**]; • Minimum password length shall be settable by the Administrator, and support passwords of 14 characters or greater.
FIA_X509_EXT.1	**Certificate Validation**
FIA_X509_EXT.1.1	The TSF shall [**interface with the Operational Environment to validate**] certificates in accordance with the following rules: ○ IETF RFC 5280 certificate validation and certificate path validation. ○ The certificate path must terminate with a certificate in the Trust Anchor Database. ○ The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.. ○ The TSF shall validate the revocation status of the certificate using [**OCSP as specified in RFC 6960, CRL as specified in RFC 5759**]. ○ The TSF shall validate the extendedKeyUsage (EKU) field according to the following rules: ○ Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. ○ Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field. ○ Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field. ○ OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-dp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field. ○ Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.
FIA_X509_EXT.1.2	The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.
FIA_X509_EXT.2	**Certificate-Based Authentication**
FIA_X509_EXT.2.1	The TSF shall [**interface with the Operational Environment to use**] X.509v3 certificates as defined by RFC 5280 to support authentication for code signing for TOE updates, [**TLS, HTTPS**], and [***integrity verification for TSF protected data, integrity verification for TSF software and firmware, [privileges user’s access, access for EST]***].

FIA_X509_EXT.2.2	When the TSF cannot determine the current revocation status of a certificate, the TSF shall [**allow the administrator to choose whether to accept the Certificate**]
FIA_X509_EXT.2.3	The TSF shall not establish a trusted communication channel if the peer certificate is deemed invalid.
FIA_X509_EXT.3	**X509 Certificate Request**
FIA_X509_EXT.3.1	The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key, CA's distinguished name, [***no other information describing the CA implemented by the TOE***].
FIA_X509_EXT.3.2	The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.
FIA_UAU.7	**Protected Authentication Feedback**
FIA_UAU_EXT.7.1	**Refinement**: The TSF shall provide only [**obscured feedback for each character entered and [no other feedback]**] to the privileged user while the authentication is in progress.
FIA_UAU_EXT.1(1)	**Authentication Mechanism (CLI)**
FIA_UAU_EXT.1.1(1)	The TSF shall [**provide**] a [**password-based authentication mechanism**] to perform privileged user authentication.
FIA_UAU_EXT.1(2)	**Authentication Mechanism (UI)**
FIA_UAU_EXT.1.1(2)	The TSF shall [**interface with the OE to provide**] a [***[certificate-based authentication mechanism]***] to perform privileged user authentication.
FIA_UIA_EXT.1	**User Identification and Authentication**
FIA_UIA_EXT.1.1	The TSF shall allow the following actions prior to requiring a non-TOE entity to initiate the identification and authentication process: – Display the warning banner in accordance with FTA_TAB.1; – Obtain certificate status information; – [[***Enrolment and public information retrieval requests***]].
FIA_UIA_EXT.1.2	The TSF shall require each user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user, including subscriber certificate renewal, subscriber revocation requests, privileged user access, [**no other actions**].
FIA_UIA_EXT.1.3	For subscriber actions, the TSF shall verify that the DN of the certificate presented by the subscriber for authentication matches that of the certificate being affected by the subscriber's actions.

Table 17, FIA - Identification and Authentication

6.1.6. Security Management (FMT)

FMT_MOF.1(1)	Management of Security Functions Behavior (Administrator Functions)
FMT_MOF.1.1(1)	**Refinement**: The **[TSF, Operational Environment]** shall restrict the ability to ***1. manage the TOE locally and remotely (TSF);*** ***2. configure the audit mechanism (TSF);*** ***3. configure and manage certificate profiles (TSF);*** ***4. modify revocation configuration (TSF);*** ***5. perform updates to the TOE (OE);*** ***6. perform on-demand integrity tests (OE);*** ***7. import and remove X.509v3 certificates into/from the Trust Anchor Database (TSF);*** ***[*** ***8. import [CIMC secret keys into cryptographic modules secret and private keys other than the CA's signing keys] (TSF);*** ***9. configure certificate revocation list function (TSF);*** ***10. configure OCSP function (TSF);*** ***11. disable deprecated algorithms (TSF);*** ***12. accept certificates whose validity cannot be determined (TSF);*** ***[*** ***13. The capability to change the frequency of the audit log signing event (TSF);*** ***14. The capability to configure the backup parameters (TSF);*** ***15. 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.) (TSF);*** ***16. The capability to request the generation of Component keys (used to protect data in more than a single session or message) (TSF);*** ***17. The capability to request the loading of Component private keys into cryptographic modules (TSF);*** ***18. The capability to change (add, revise, delete) the trusted public keys (TSF);*** ***19. The capability to zeroize CIMC plaintext private and secret keys (TSF);*** ***20. The capability to export a component private key (TSF).*** ***]]*** to [Administrators].

FMT_MOF.1(2)	**Management of Security Functions Behavior (CA/RA Functions)**
FMT_MOF.1.1(2)	**Refinement**: The [**TSF**] shall restrict the ability to ***1. approve and execute the issuance of certificates;*** ***2. configure subscriber self-service request constraints;*** ***[*** ***3. configure automated certificate approval management;*** ***4. approve rulesets that govern the authorizations of AORs to manage particular certificates on behalf of an organization;*** ***5. accept, process and export CMC messages;*** ***] to [none].***
FMT_MOF.1(3)	**Management of Security Functions Behavior (CA Operations Functions)**
FMT_MOF.1.1(3)	**Refinement**: The [***TSF***] shall restrict the ability to ***1. approve certificate revocation;*** ***[*** ***2. perform archival and recovery;*** ***3. import a key share to support recovery of a CA signing key;*** ***4. approve rulesets that govern the authorizations of RAs to manage particular certificates on behalf of an organization;*** ***5. export PKCS#10 certificate request;*** ***6. import CA certificate;*** ***]*** to ***[CA Operations Staff].***
FMT_MOF.1(4)	**Management of Security Functions Behavior (Admin/Officer Functions)**
FMT_MOF.1.1(4)	**Refinement**: The [***Operational Environment***] shall restrict the ability to ***1. perform destruction of sensitive data when no longer needed;*** ***[*** ***2. participate as a second party for archival and recovery;*** ***3. import a key share to support recovery of a CA signing key;*** ***4. perform encrypted export of private or secret key or critical data*** ***5. no other function*** ***]*** to [**Administrators**].
FMT_MOF.1(5)	**Management of Security Functions Behavior (Auditor Functions)**

FMT_MOF.1.1(5)	**Refinement**: The [***TSF***] shall restrict the ability to 1. ***Delete entries from the audit trail*** ***[*** 2. ***Search the audit trail*** 3. ***Set or change the retention period parameter for audit records requiring extended retention*** ***]*** to [*auditors*].
FMT_MTD.1	**Management of TSF Data**
FMT_MTD.1.1	The TSF shall restrict the ability to manage the TSF data to [privileged users].
FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	Refinement: The [**TSF, Operational Environment**] shall be capable of performing the following management functions: [1. ***Ability to manage the TOE locally and remotely (TSF);*** 2. ***Ability to perform updates to the TOE (OE);*** 3. ***Ability to perform archival and recovery (TSF);*** 4. ***Ability to manage the audit mechanism (TSF);*** 5. ***Ability to configure and manage certificate profiles (TSF);*** 6. ***Ability to approve and execute the issuance of certificates (TSF);*** 7. ***Ability to approve certificate revocation (TSF);*** 8. ***Ability to modify revocation configuration (TSF);*** 9. ***Ability to configure subscriber self-service request constraints (TSF);*** 10. ***Ability to perform on-demand integrity tests (OE);*** 11. ***Ability to destroy sensitive user data when no longer needed (TSF, OE);*** 12. ***Ability to import and remove X.509v3 certificates into/from the Trust Anchor Database (TSF);*** ***[*** 13. ***Ability to configure the NPE ruleset (TSF);*** 14. ***Ability to configure automated process used to approve the revocation of a certificate or information about the revocation of a certificate (TSF);*** 15. ***Ability to approve rulesets that govern the authorizations of RAs or AORs to manage particular certificates on behalf of an organization (TSF);*** ***[*** 16. ***Ability to modify the CRL configuration (TSF);*** ***Ability to modify the OCSP configuration (TSF);*** ***]*** 17. ***Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1 (TSF);*** 18. ***Ability to configure the cryptographic functionality (TSF);*** 19. ***Ability to import private keys (TSF);***

	20. ***Ability to export TOE private keys (not for archival) (TSF);*** 21. ***Ability to disable deprecated algorithms (TSF);*** 22. ***Ability to accept certificates whose revocation status cannot be determined (TSF).***]].
FMT_SMR.2	**Restrictions on Security Roles**
FMT_SMR.2.1	**Refinement**: The TSF ***and [no other component***] shall maintain the roles: [• Administrator, • Auditor, • CA Operations Staff, • **[RA Staff,** • **Authorized Organizational Representative]]** **Application note:** The corresponding TOE role names are: Administrator – Super Administrator Auditor – Auditor CA Operations Staff – CA Administrators RA Staff - RA Administrators Authorized Organizational Representative - Supervisor
FMT_SMR.2.2	**Refinement**: The TSF ***and [no other component]*** shall be able to associate users with roles.
FMT_SMR.2.3	**Refinement**: The TSF ***and [no other component]*** shall ensure that the conditions [– No identity is authorized to assume both an Auditor role and any of the other roles in FMT_SMR.2.1; and – No identity is authorized to assume both a CA Operations Staff role and any of the other roles in FMT_SMR.2.1] are satisfied.

Table 18, FMT - Security Management

6.1.7. Protection of the TSF (FPT)

FPT_APW_EXT.1	**Protection of Privileged User Passwords**
FPT_APW_EXT.1.1	The TSF shall store passwords in non-plaintext form.
FPT_APW_EXT.1.2	The TSF shall prevent the reading of plaintext passwords.
FPT_FLS.1	**Failure with Preservation of Secure State**
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [***[a secure component failure**], [**No other potential Operational Environment failures***]]. **Application note:** A secure component failure will result in an error message giving the Administrator possibility to perform a secure restart.
FPT_ITT1	**Basic Internal TSF Data Transfer Protection**

FPT_ITT.1.1	**Refinement**: The TSF shall protect TSF data from [disclosure, modification*]* when it is transmitted between separate parts of the TOE through the use of [**TLS, TLS/HTTPS**].
FPT_KST_EXT.1	**No Plaintext Key Export**
FPT_KST_EXT.1.1	The TSF and [**Operational Environment**] shall prevent the plaintext export of [***all TOE secret and private keys and user secret and private keys***].
FPT_KST_EXT.2	**TSF Key Protection**
FPT_KST_EXT.2.1	The TSF and [**Operational Environment**] shall prevent unauthorized use of all TSF private and secret keys.
FPT_NPE_EXT.1	**NPE Constraints**
FPT_NPE_EXT.1.1	The TSF shall enforce an Administrator-configurable ruleset that specifies authorizations to submit NPE certificate requests.
FPT_NPE_EXT.1.2	The TSF shall require the CA Operations Staff to register any RA, and shall require a CA Operations Staff or authorized RA to register any AORs, and associate each AOR with an organization or set of devices prior to that AOR making requests on behalf of an assigned organization or devices.
FPT_RCV.1	**Manual Trusted Recovery**
FPT_RCV.1.1	After [***a system crash***] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided. **Application note**: A system crash will result in a secure restart that is logged.
FPT_SKP_EXT.1	**Protection of Keys**
FPT_SKP_EXT.1.1	The TSF shall [**interface with the Operational Environment to implement**] the ability to prevent reading of all pre-shared keys, private, and secret keys (e.g., KEKs, DEKs, session keys).
FPT_STM.1	**Reliable Time Stamps**
FPT_STM.1.1	**Refinement**: The TSF shall ***[interface with the Operational Environment to provide]*** reliable time stamps.
FPT_TUD_EXT.1	**Trusted Update***
FPT_TUD_EXT.1.1	The TSF shall *[***interface with the Operational Environment to implement**] the ability to check for updates and patches to the TOE.
FPT_TUD_EXT.1.2	The TSF shall [***interface with the Operational Environment to implement]*** the ability to provide Administrators the ability to initiate updates to TOE firmware/software.
FPT_TUD_EXT.1.3	The TSF shall [***interface with the Operational Environment to implement]*** the ability to verify firmware/software updates to the TOE using a digital signature prior to installing those updates.
FPT_TUD_EXT.1.4	The TSF shall **[interface with the Operational Environment to implement**] the ability to verify the digital signature whenever the software or firmware is externally loaded into the TOE and if verification fails, the TSF shall [***inform the Administrator***].

Table 19, FPT - Protection of the TSF

* Application Note. The TOE is not delivered signed. A checksum can be used for the verification of the integrity of the TOE.

6.1.8. TOE Access (FTA)

FTA_SSL.4	**User-Initiated Termination**
FTA_SSL.4.1	**Refinement**: The TSF shall ***[implement] the ability to*** allow ***privileged*** user-initiated termination of the ***privileged*** user's own interactive session
FTA_TAB.1	**Default TOE Access Banners**
FTA_TAB.1.1	**Refinement**: Before establishing ***a privileged*** user session the TSF shall display ***an Administrator-configured*** advisory ***notice and consent*** warning message regarding unauthorized use of the TOE.

Table 20, FTA - TOE Access

6.1.9. Trusted Path/Channels (FTP)

FTP_ITC.1	**Inter-TSF Trusted Channel**
FTP_ITC.1.1	**Refinement:** The TSF shall use **[HTTPS, TLS] to** provide a ***trusted*** communication channel between itself and ***authorized external network based IT entities supporting the following capabilities*****: [*external cryptographic module, directory services, RA,[database]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [the TSF, the authorized IT entities] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [***cryptographic services provided by an external network HSM, directory services, VA].***
FTP_TRP.1	**Trusted Path**
FTP_TRP.1.1	**Refinement**: The TSF shall ***use [HTTPS, TLS]*** to provide ***a trusted*** communication path between itself and ***remote subscribers and privileged users*** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].
FTP_TRP.1.2	**Refinement**: The TSF shall permit ***remote subscribers*** and privileged users to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [initial subscriber and privileged user authentication and all remote administration actions].

Table 21, FTP Trusted Path/Channels

6.2. Security Assurance Requirements

6.2.1. Development (ADV)

ADV_FSP.1	Basic Functional Specification
	Developer action elements:
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D Developer Note:	The developer shall provide a tracing from the functional specification to the SFRs. *As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.*
	Content and presentation elements:
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-noninterfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
	Evaluator action elements:
ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.1E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Table 22, ADV – Development assurance requirements

6.2.2. Guidance Documentation (AGD)

AGD_OPE.1	Operational User Guidance
	Developer action elements:
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Developer Note:	*Rather than repeat information here, the developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluator will be checking for. This will provide the necessary information for the preparation of acceptable guidance.*

	Content and presentation elements:
AGD_OPE.1.1C	The operational user guidance shall describe, for each privileged user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each privileged user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each privileged user role, the available functions and interfaces, in particular all security parameters under the control of the privileged user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each privileged user role, clearly present each type of security-relevant event relative to the privileged user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each privileged user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
	Evaluator action elements:
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1	**Preparative Procedures**
	Developer action elements:
AGD_PRE.1.1D	The developer shall provide the TOE, including its preparative procedures.
Developer Note:	*As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.*
	Content and presentation elements:
AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
	Evaluator action elements:

AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Table 23, AGD – Guidance documentation assurance requirements

6.2.3. Life-Cycle Support (ALC)

ALC_CMC.1	**Labeling of the TOE**
	Developer action elements:
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
	Content and presentation elements:
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
	Evaluator action elements:
ALC_CMC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_CMS.1	**TOE CM Coverage**
	Developer action elements:
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
	Content and presentation elements:
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
	Evaluator action elements:
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 24, ALC – Life-cycle support assurance requirements

6.2.4. Tests (ATE)

ATE_IND.1	**Independent Testing – Conformance**
	Developer action elements:
ATE_IND.1.1D	The developer shall provide the TOE for testing.
	Content and presentation elements:
ATE_IND.1.1C	The TOE shall be suitable for testing.
	Evaluator action elements:

ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Table 25, ATE – Tests assurance requirements

6.2.5. Vulnerability Analysis (AVA)

AVA_VAN.1	**Vulnerability Survey**
AVA_VAN.1.1D	**Developer action elements:**
	The developer shall provide the TOE for testing.
	Content and presentation elements:
AVA_VAN.1.1C	The TOE shall be suitable for testing.
	Evaluator action elements:
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Table 26, AVA – Vulnerability analysis assurance requirements

6.3. Security Requirements Rationale

The SFRs and SARs which are claimed in chapter 6 are consistent with the SFRs that are defined in the claimed Protection Profile

7. TOE Summary Specifications

7.1. Security Audit (FAU)

FAU_ADP_EXT.1	**Audit Dependencies**
FAU_ADP_EXT.1.1	Auditable events are listed in Table 11 to Table 13. The event formatting is described in the guidance documentation.
FAU_GCR_EXT.1	**Generation of Certificate Repository**
FAU_GCR_EXT.1.1	The certificate repository is provided by the TOE database in the operational environment. PKCS#11 is used as interface.
FAU_GEN.1	**Audit data generation**
FAU_GEN.1.1	All auditable events are listed in Table 11 through Table 13.
FAU_GEN.1.2	Additional information is specified in column three of Table 11 through Table 13. Generation of ephemeral keys is not audited.
FAU_GEN.2	**User identity association**
FAU_GEN.2.1	NA
FAU_SAR.1	**Audit Review**
FAU_SAR.1.1	N/A
FAU_SAR.1.2	
FAU_SAR.3	**Selectable Audit Review**
FAU_SAR.3.1	N/A
FAU_SEL.1	**Selective Audit**
FAU_SEL.1.1	N/A
FAU_STG_EXT.1	**External Audit Trail Storage**
FAU_STG_EXT.1.1	All audit events are stored in the database. All audit events are individually signed.
FAU_STG.4	**Prevention of audit data loss**
FAU_STG.4.1	The TOE will stop working if the TOE database is not receiving audit data (e.g., it is full). The TOE will display an error message according to FPT_FLS.1 if the TOE database is not receiving audit data.

Table 27, FAU - Security audit, TSS description

7.2. Communication (FCO)

<table>
<tr><th>FCO_NRO_EXT.2</th><th>Certificate-Based Proof of Origin</th></tr>
<tr><td>FCO_NRO_EXT.2.1
FCO_NRO_EXT.2.2
FCO_NRO_EXT.2.3
FCO_NRO_EXT.2.4
FCO_NRO_EXT.2.5</td><td>The TOE uses the HSM to digitally sign certificates, CRLs, and OCSP responses it creates using one of the algorithms in the table below as determined by the issuing certificate’s key type. The TOE also uses the HSM to digitally sign the database table. The choice of key type and size is made when the issuer credential or TSF credential is created and remains so until a new credential is created. The table differentiates between key sizes that can be generated vs those that it can support (i.e., the PKCS#11 Cryptographic Module can be used to generate a public/private key pair using its own tools that may support different key sizes than the TOE itself can generate on the PKCS#11 Cryptographic Module).

<table>
<tr><td>Key</td><td>Supported Key Sizes</td><td>Generated Key Sizes</td></tr>
<tr><td>RSA</td><td>2048, 3072, (4096, 8192) bits</td><td>2048, 3072, (4096, 8192)</td></tr>
<tr><td>ECDSA</td><td>All NIST defined B, K, and P curves with key length 256, 384, 512 bits</td><td>NIST curves: P-256, P-384, P-521</td></tr>
<tr><td>DSA</td><td>2048, 3072, (4096, 8192) bits</td><td>2048, 3072, (4096, 8192)</td></tr>
</table>

Manual processes for revocation requests and responses are described in ref. [6].</td></tr>
<tr><th>FCO_NRR_EXT.2</th><th>Certificate-Based Proof of Receipt</th></tr>
<tr><td>FCO_NRR_EXT.2.1</td><td>The TSF shall provide proof of receipt for EST by providing signed responses using mechanisms in accordance with FIA_ESTS_EXT.1.</td></tr>
</table>

Table 28, FCO - Communication, TSS description

7.3. Cryptographic Support (FCS)

<table>
<tr><th>FCS_CDP_EXT.1</th><th>Cryptographic Dependencies</th></tr>
<tr><td>FCS_CDP_EXT.1.1</td><td>The TSF uses a PKCS#11 interface for invoking all cryptographic services from the HSM</td></tr>
<tr><th>FCS_CKM.1</th><th>Cryptographic Key Generation</th></tr>
<tr><td>FCS_CKM.1.1</td><td>The following asymmetric key sizes are supported:

<table>
<tr><th>Scheme</th><th>Size</th></tr>
<tr><td>RSA</td><td>2048, 3072</td></tr>
<tr><td>ECC NIST curves</td><td>P-256, P-384, P-521</td></tr>
<tr><td>FFC</td><td>2048, 3072</td></tr>
</table>

RSA and FFC keys with 4096 and 8192 bit lengths are also supported but not tested in the evaluated configuration.

RSA and ECC keys are used for cipher suites used for TLS/HTTPS communication and for digital signature generation and verification. FCC keys are used for digital signature generation and verification.</td></tr>
</table>

FCS_CKM.2	**Cryptographic Key Establishment**
FCS_CKM.2.1	RSA-based key establishment schemes and Elliptic curve-based key establishment schemes are used for cipher suites used for TLS/HTTPS communication both as sender and recipient. RSA-based key establishment schemes, elliptic curve-based key establishment schemes and finite field-based key establishment schemes are used for digital signature generation and verification. Key establishment scheme using Diffie-Hellman group 14 meets RFC 3526, Section 3 fully.
FCS_CKM_EXT.4	**Cryptographic Key Destruction**
FCS_CKM_EXT.4.1 FCS_CKM_EXT.4.2	All secret and private keys and critical security parameters which are not permanently protected from export by hardware are destroyed when the power is removed, if stored in volatile memory, and by instructing the HSM to overwrite if stored in non-volatile memory.
FCS_COP.1(1)	**Cryptographic Operation (AES Encryption/Decryption)**
FCS_COP.1.1(1)	The following AES algorithms are supported: • AES-CBC (as defined in NIST SP 800-38A) mode, • AES-CCM (as defined in NIST SP 800-38C) mode, • AES-GCM (as defined in NIST SP 800-38D) mode, • AES Key Wrap (KW) (as defined in NIST SP 800-38F) mode • AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F) mode]. Key sizes of 128 and 256 bits are supported.
FCS_COP.1(2)	**Cryptographic Operation (Cryptographic Signature)**
FCS_COP.1.1(2)	The following digital signature algorithms and key sizes are supported: • RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 and 3072 bits that meets FIPS-PUB 186-4, “Digital Signature Standard”, • Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256, 384, 512 bits that meets FIPS PUB 186-4, “Digital Signature Standard” with “NIST curves” P-256, P-384 and P-521 (as defined in FIPS PUB 186-4, “Digital Signature Standard”), • Digital Signature Algorithm (DSA) with a key size (modulus) of 2048, 3072 bits, that meets FIPS-PUB 186-4, “Digital Signature Standard”.
FCS_COP.1(3)	**Cryptographic Operation (Cryptographic Hashing)**
FCS_COP.1.1(3)	The hashing algorithms SHA-256, SHA-384, SHA-512 and message digest sizes 256, 384, and 512 bits that meet the following: FIPS Pub 180-4, “Secure Hash Standard” are supported.
FCS_COP.1(4)	Cryptographic Operation (Keyed-Hash Message Authentication)

<table>
<tr><td>FCS_COP.1.1(4)</td><td>The HMAC algorithms HMAC-SHA-256, SHA-384, and SHA-512, and key sizes 256, 384, and 512 and message digest sizes 256, 384, and 512 bits that meet the following: FIPS Pub 198-1,“The Keyed Hash Message Authentication Code”; FIPS Pub 180-4, “Secure Hash Standard” are supported.</td></tr>
<tr><td>FCS_HTTPS_EXT.1</td><td>HTTPS Protocol</td></tr>
<tr><td>FCS_HTTPS_EXT.1.1</td><td rowspan="2">TLS is used to implement HTTPS, complying with RFC 2818.</td></tr>
<tr><td>FCS_HTTPS_EXT.1.2</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>Cryptographic Random Bit Generation</td></tr>
<tr><td>FCS_RBG_EXT.1.1</td><td rowspan="2">SafeNet Luna SA (not tested in the evaluated configuration):
Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode)

Utimaco CryptoServer:
Hash-based deterministic random number generator (DRG.4 acc. AIS 31) with true random number generator (PTG.2 acc. AIS 31)</td></tr>
<tr><td>FCS_RBG_EXT.1.2</td></tr>
<tr><td>FCS_STG_EXT.1</td><td>Cryptographic Key Storage</td></tr>
<tr><td>FCS_STG_EXT.1.1</td><td>
<table>
<tr><th>Key</th><th>Purpose</th><th>Storage</th><th>Protection</th></tr>
<tr><td>CA Issuers (asymmetric)</td><td>Signing certificates, CRLs, and OCSP responses</td><td>HSM</td><td>Protected by HSM</td></tr>
<tr><td>TLS/HTTPS Server Key (asymmetric)</td><td>Server Authentication</td><td>HSM</td><td>Protected by HSM</td></tr>
<tr><td>TSF Credential (asymmetric)</td><td>Encryption of CA secrets (HSM PINs, database password, etc.)</td><td>HSM</td><td>Protected by HSM</td></tr>
<tr><td>TLS/HTTPS Client Key (asymmetric)</td><td>Authentication</td><td>HSM</td><td>Protected by HSM</td></tr>
</table>
</td></tr>
<tr><td>FCS_TLSC_EXT.2</td><td>TLS Client Protocol with Mutual Authentication</td></tr>
<tr><td>FCS_TLSC_EXT.2.1</td><td rowspan="4">The following cipher suites are supported:
• TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
• TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
• TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
• TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
• TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
• TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
• TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
• TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
• TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
• TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
• TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
• TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
].</td></tr>
<tr><td>FCS_TLSC_EXT.2.2

FCS_TLSC_EXT.2.3</td></tr>
<tr><td>FCS_TLSC_EXT.2.4</td></tr>
<tr><td>FCS_TLSC_EXT.2.5</td></tr>
<tr><td>FCS_TLSS_EXT.2</td><td>TLS Server Protocol with Mutual Authentication</td></tr>
</table>

FCS_TLSS_EXT.2.1	The following cipher suites are supported: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
FCS_TLSS_EXT.2.2 FCS_TLSS_EXT.2.3	
FCS_TLSS_EXT.2.4	
FCS_TLSS_EXT.2.5 FCS_TLSS_EXT.2.6	

Table 29, FCS – Cryptographic support, TSS description

7.4. User Data Protection (FDP)

FDP_CER_EXT.1	**Certificate Profiles**
FDP_CER_EXT.1.1	The TOE implements a certificate profile function and issues certificates consistent with the profile's configuration. A CA account can have one or more profiles which are configured by an administrator using the TOE's web interface. Using that interface the administrator can assign a name (Certificate Profile ID), extensions, and default properties to the profile. Proof-of-possession of the private key corresponding to the request is addressed in 0. Certificate serial numbers consist of random output from the HSM that meets the requirements of FCS_RGB_EXT.1, where output that does not meet certificate serial number constraints in RFC5280 and X.690 are discarded (and a new random value generated). The number of bytes is configurable up to 20.
FDP_CER_EXT.1.2	
FDP_CER_EXT.1.3	
FDP_CER_EXT.2	**Certificate Request Matching**
FDP_CER_EXT.2.1	Each certificate request is identified by a unique request ID which is linked to the issued certificate. Each certificate is identified by a unique issuer DN and serial number.
FDP_CER_EXT.3	**Certificate Issuance Approval**

FDP_CER_EXT.3.1	The TOE supports the approval of certificates issued according to a configured certificate profile through the web interface, the RA management interface or EST. Only user roles given 'Approve End Entity Actions' permission can approve certificates via the web interface (which is the only interface through which manual issuance occurs).
FDP_CRL_EXT.1	**Certificate Revocation List Validation**
FDP_CRL_EXT.1.1	The TOE supports CRL generation on demand or on schedule depending on its configuration. Issued CRLs contain values in accordance with ITU-T Recommendation X.509 as follows: a) If the version field is present, then it shall contain a 1. b) If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1. c) 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. d) The signature and signatureAlgorithm fields shall contain the OID for a digital signature algorithm in accordance with FCS_COP.1(2). e) The thisUpdate field shall indicate the issue date of the CRL. f) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.
FDP_CSI_EXT.1	**Certificate Status Information**
FDP_CSI_EXT.1.1	The TSF shall provide certificate status information whose format complies with ITU-T Recommendation X.509v2 CRL, the OCSP standard as defined by RFC 6960, RFC 2560. Users with 'Revoke End Entities' permission, or subscribers, can approve changes to the status of a certificate. This can be done via the TOE's web interface and the RA management interface. The process varies based on the interface.
FDP_CSI_EXT.1.2	
FDP_ITT.1	**Basic Internal Transfer Protection**
FDP_ITT.1.1	The TSF prevents the disclosure and modification of user data when it is transmitted between physically separated parts of the TOE through the use of TLS and TLS/HTTPS.
FDP_OCSPG_EXT.1	**OCSP Basic Response Generation**
FDP_OCSPG_EXT.1.1	The TSF ensures that all mandatory fields in the OCSP response contain values in accordance with the standards specified in FDP_CSI_EXT.1. At a minimum, the following items are enforced: a) The version field shall indicate a current version. b) The signatureAlgorithm field shall contain the object identifier (OID) for a digital signature algorithm in accordance with FCS_COP.1(2). c) The thisUpdate field shall indicate the time at which the status being indicated is known to be correct. d) The producedAt field shall indicate the time at which the OCSP responder signed the response.

	e) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.
FDP_RIP.1	**Subset Residual Information Protection**
FDP_RIP.1.1	The TOE does not store any personally identifiable information, that does not also appear in a certificate. The TOE does handle EST passwords and the TLS session object. The TSF and the HSM ensures that any previous information content of a resource is made unavailable when no longer used. The following objects are : secret and ephemeral keys, passwords.

Table 30, FDP – User data protection, TSS description

7.5. Identification and Authentication (FIA)

FIA_ESTS_EXT.1	**Enrollment over Secure Transport (EST) Server**
FIA_ESTS_EXT.1.1 FIA_ESTS_EXT.1.2	The TOE supports Enrollment over Secure Transport (EST) protocol as described in RFC 7030 to receive and act upon certificate enrollment requests using the simple enrollment method described in RFC 7030 Section 4.2. Certificate enrollment requests are authenticated using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2, authenticated using a username and password as specified by RFC 7030 Section 3.2.3, or authenticated using a special RA certificate issued by the CA and asserting the id-kp-cmcRA OID in its extended key usage extension as specified by RFC 7030 Section 3.7.
FIA_ESTS_EXT.1.3	
FIA_ESTS_EXT.1.4	
FIA_PMG_EXT.1	**Password Management**
FIA_PMG_EXT.1.1	A minimum password length is settable by the Administrator, and passwords of 14 characters or greater are supported. Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.
FIA_X509_EXT.1	**Certificate Validation**
FIA_X509_EXT.1.1 FIA_X509_EXT.1.2	The TSF uses the HSM to validate certificates in accordance with the following rules: – IETF RFC 5280 certificate validation and certificate path validation. – The certificate path must terminate with a certificate in the Trust Anchor Database. – The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates. – The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5759. – The TSF shall validate the extendedKeyUsage field according to the following rules: o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.

	○ Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field. ○ Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field. ○ OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-dp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field. ○ Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.
FIA_X509_EXT.2	**Certificate-Based Authentication**
FIA_X509_EXT.2.1	The TOE uses X.509v3 certificates, as defined by RFC 5280, to authenticate privileged users, subscribers, RAs, and DBAccess clients over HTTPS, and to verify the integrity of software updates. Certificates can also be used for EST access authentication. When the TSF cannot determine the current revocation status of a certificate the administrator is allowed to choose whether to accept the certificate or not.
FIA_X509_EXT.2.2	
FIA_X509_EXT.2.3	
FIA_X509_EXT.3	**X509 Certificate Request**
FIA_X509_EXT.3.1 FIA_X509_EXT.3.2	NA
FIA_UAU.7	**Protected Authentication Feedback**
FIA_UAU_EXT.7.1	For password based authentication, the entered password is obfuscated. For certificate-based authentication no obfuscation is necessary.
FIA_UAU_EXT.1(1)	**Authentication Mechanism (CLI)**
FIA_UAU_EXT.1.1(1)	NA
FIA_UAU_EXT.1(2)	**Authentication Mechanism (UI)**
FIA_UAU_EXT.1.1 (2)	NA
FIA_UIA_EXT.1	**User Identification and Authentication**
FIA_UIA_EXT.1.1	The TSF allows the following actions prior to requiring a non-TOE entity to initiate the identification and authentication process: – Display the warning banner in accordance with FTA_TAB.1; – Obtain certificate status information; Enrolment and public information retrieval requests.
FIA_UIA_EXT.1.2	
FIA_UIA_EXT.1.3	

Table 31, FIA – Identification and authentication, TSS description

7.6. Security Management (FMT)

FMT_MOF.1(1)	**Management of Security Functions Behavior (Administrator Functions)**

FMT_MOF.1.1(1)	NA
FMT_MOF.1(2)	**Management of Security Functions Behavior (CA/RA Functions)**
FMT_MOF.1.1(2)	NA
FMT_MOF.1(3)	**Management of Security Functions Behavior (CA Operations Functions)**
FMT_MOF.1.1(3)	NA
FMT_MOF.1(4)	**Management of Security Functions Behavior (Admin/Officer Functions)**
FMT_MOF.1.1(4)	The Operational Environment restricts the following functions to administrator roles: 1. perform destruction of sensitive data when no longer needed; 2. participate as a second party for archival and recovery; 3. import a key share to support recovery of a CA signing key; 4. perform encrypted export of private or secret key or critical data This is done through the HSM authentication mechanisms.
FMT_MOF.1(5)	**Management of Security Functions Behavior (Auditor Functions)**
FMT_MOF.1.1(5)	NA
FMT_MTD.1	**Management of TSF Data**
FMT_MTD.1.1	TSF data can only be manipulated through the administrative Web interface or command line commands. Both requires authentication of privileged users.
FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	NA
FMT_SMR.2	**Restrictions on Security Roles**
FMT_SMR.2.1	It is possible to grant the following privileges to any role created through the TOE: – Authorized CAs – End Entity Rules – End Entity Profiles – Validators – Internal Keybinding Rules – Other Rules The following predefined roles corresponds to the roles listed in FMT_SMR.2.1: Administrator – Super Administrator Auditor – Auditor CA Operations Staff – CA Administrators RA Staff - RA Administrators Authorized Organizational Representative – Supervisors
FMT_SMR.2.2	
FMT_SMR.2.3	

Table 32, FMT – Security management, TSS description

7.7. Protection of the TSF (FPT)

FPT_APW_EXT.1	**Protection of Privileged User Passwords**
FPT_APW_EXT.1.1 FPT_APW_EXT.1.2	Passwords are stored in the database in a non-readable form. The database authentication prohibits unauthorized access.
FPT_FLS.1	**Failure with Preservation of Secure State**
FPT_FLS.1.1	A secure component failure, such as the TOE itself, the HSM, the database, or the underlying application server, will result in an error message.
FPT_ITT1	**Basic Internal TSF Data Transfer Protection**
FPT_ITT.1.1	The TOE protects TSF data in transit between separate parts by TLS and HTTPS/TLS.
FPT_KST_EXT.1	**No Plaintext Key Export**
FPT_KST_EXT.1.1	There is no way to export private keys used by the TSF or users from the TOE.
FPT_KST_EXT.2	**TSF Key Protection**
FPT_KST_EXT.2.1	TSF private and secret keys are stored in the HSM and protected from unauthorized access by the HSM authentication measures.
FPT_NPE_EXT.1	**NPE Constraints**
FPT_NPE_EXT.1.1	The TSF enforces an Administrator-configurable ruleset that specifies authorizations to submit NPE certificate requests.
FPT_NPE_EXT.1.2	The TSF requires the CA Operations Staff to register any RA, and requires a CA Operations Staff or authorized RA to register any AORs, and associate each AOR with an organization or set of devices prior to that AOR making requests on behalf of an assigned organization or devices.
FPT_RCV.1	**Manual Trusted Recovery**
FPT_RCV.1.1	After a failure of integrity is detected, the TOE shuts itself down in an orderly manner and can be started the ordinary way.
FPT_SKP_EXT.1	**Protection of Keys**
FPT_SKP_EXT.1.1	The TSF provides no mechanisms allowing the reading of any private, or secret keys. The HSM maintains its own protections of keys it holds and in the evaluated configuration does not provide any mechanism for reading those keys.
FPT_STM.1	**Reliable Time Stamps**
FPT_STM.1.1	The TOE obtains the current time from its operational environment. The current system time is used when: Generating audit records, issuing certificates, CRLs, and signing OCSP responses. The SFRs that use time are: FAU_GEN.1.2, FCO_NRO_EXT.2.2, FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1, FDP_CER_EXT.3,

	FDP_CSI_EXT.1, FDP_CRL_EXT.1, FDP_OCSP_EXT.1.1, FIA_X509_EXT.1, and FIA_X509_EXT.2.
FPT_TUD_EXT.1	**Trusted Update**
FPT_TUD_EXT.1.1	The TOE release or EAR-archive is digitally signed and verified before installed. The verification is done using the public key of the signing certificate. If the verification fails the Administrator is informed by an error message.
FPT_TUD_EXT.1.2	
FPT_TUD_EXT.1.3	
FPT_TUD_EXT.1.4	

Table 33, FPT – Protection of the TSF, TSS description

7.8. TOE Access (FTA)

FTA_SSL.4	**User-Initiated Termination**
FTA_SSL.4.1	NA
FTA_TAB.1	**Default TOE Access Banners**
FTA_TAB.1.1	Before establishing a privileged user session over the administrative HTTPS/TLS interface the TSF displays an Administrator-configured advisory notice and consent warning message regarding unauthorized use of the TOE.

Table 34, FTA – TOE Access, TSS description

7.9. Trusted Path/Channels (FTP)

FTP_ITC.1	**Inter-TSF Trusted Channel**
FTP_ITC.1.1	The TSF uses TLS for the trusted communication channel to the HSM, directory services, RA and database. The TSF uses the BouncyCastle crypto library for the cryptographic operations.
FTP_ITC.1.2	
FTP_ITC.1.3	
FTP_TRP.1	**Trusted Path**
FTP_TRP.1.1 FTP_TRP.1.2	The TSF uses HTTPS/TLS for the trusted communication path to the remote subscribers and privileged users.
FTP_TRP.1.3	

Table 35, FTP – Trusted path/channel, TSS description

8. 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*.
7. EJBCA Common Criteria Guidance Supplement, version 0.4, 2020-09-15
8. Protection Profile for Certification Authorities, version 2.1, 2017-12-01, National Information Assurance Partnership

9. Glossary

ACME	Automatic Certificate Management Environment
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
CMP	Certificate Management Protocol
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
EST	Enrollment over Secure Transport
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
RA	Registration Authority

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
VA	Validation Authority
VAN	Vulnerability Analysis CC components
VM	Virtual Machine