Entrust®

Entrust Certificate Authority 10.1 and Entrust Certificate Authority Administration 10.1

Security Target

Document issue: 1.1

January 25, 2023

Prepared By: Saffire Systems

P.O. Box 40295

Indianapolis, IN 46240

Table of Contents

Table of Tables

Table of Figures

1 Introduction

1.1 ST Reference

ST Title:	Entrust Certificate Authority 10.1 and Entrust Certificate Authority Administration 10.1 Security Target
ST Version:	1.1
ST Author:	Entrust Corporation Saffire Systems
ST Date:	January 25, 2023

1.2 TOE Reference

TOE Developer:	Entrust Corporation
Evaluation Sponsor:	Entrust Corporation
TOE Identification:	Entrust Certificate Authority and Entrust Certificate Authority Administration with the following license codes: • Enterprise (X.509) • CVCA for Foreign DVs (EAC[1] / ePassport) • CVCA for Domestic DVs (EAC / ePassport) • DV for Inspection Systems (EAC / ePassport)
TOE Version:	10.1
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

1.3 TOE Overview

1.3.1 TOE Product Type

The Target of Evaluation (TOE) is Entrust Certificate Authority 10.1 and Entrust Certificate Authority Administration 10.1, an enterprise Public Key Infrastructure (PKI) solution providing both a Certification Authority (CA) and a Registration Authority (RA). Entrust Certificate Authority is an enterprise CA application designed to generate, protect, and manage a CA, and to provide certificate issuance and management services. Entrust Certificate Authority Administration is a graphical front-end administration interface (RA) designed to integrate with Entrust Certificate Authority and facilitate CA policy management and certificate management tasks.

1.3.2 TOE Security Functionality

- Security Audit
  - Audit record generation for security-relevant events
  - Selective audit

[1] EAC – Extended Access Control

    - Audit trail protection
- Security Management
    - Role based access control
    - Security Management functions
    - TOE Access Control Policy
- Identification and Authentication
    - Password and certificate-based authentication
- Remote Data Entry and Export (Communication)
    - Proof and verification of origin
    - Trusted Channel
- Certificate Management
    - Certificate generation
    - Certificate revocation status reporting
- Certificate Revocation
    - Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP)
- Key Management
    - Key generation
    - Private/public key protection
    - Key zeroization
    - Cryptographic Operations

1.3.3 TOE Hardware Requirements

The TOE is a software-only TOE that is designed to run on any computing platform that can support the underlying operating system (OS). Consequently, the OS determines the minimal hardware requirements. In general, a computing system that meets the following minimum requirements will be compatible with the TOE.

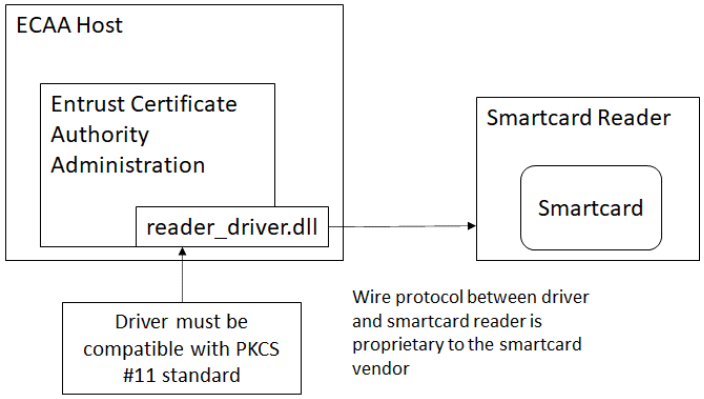
Table 1: Minimum Hardware Requirements

Component	Memory	CPU	HD	Network
Entrust Certificate Authority	4GB RAM	Dual-core 64-bit 3.0GHz	100GB	100BASE-T
Entrust Certificate Authority Administration	2GB RAM	Single-core 64-bit 1.4GHz	50GB	100BASE-T

1.3.3.1 Smartcard/Token

Entrust Certificate Authority Administration (ECAA) is capable of integrating with a smartcard or a token connected via compatible reader. A digital ID (i.e. identity certificate and a private key) can be saved to a smartcard or token and used to authenticate to ECAA. That card or a token must remain in the reader for Entrust Certificate Authority Administration to operate.

Figure 1: Smartcard integration



In the evaluated configuration, use the Thales SafeNet eToken 5110 CC or Thales Safenet eToken 5110 FIPS with Thales SafeNet Authentication Client v10.8 (R6) or later.

The smartcard or token is considered part of the Operational Environment (OE) and outside the TOE boundary; as such smartcard/token functionality and security is not evaluated. However, the TOE functionality that uses the smartcard or token is considered part of the TSF. ECAA communicates with a smartcard/token using a driver that implements the standard PKCS #11 API.

Administrators must store their digital ID (Entrust profile) on a smartcard or token in the evaluated configuration.

1.3.3.2 Optional Hardware Requirements

This section identifies the optional hardware that can be deployed with the TOE to provide additional security mechanisms. The hardware defined in this section are required as part of the operational environment in the evaluated configuration.

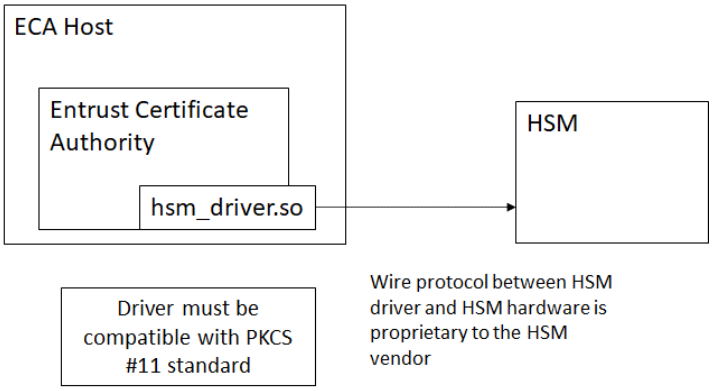
1.3.3.2.1 Hardware Security Module

Entrust Certificate Authority (ECA) is capable of integrating with a compatible hardware security module (HSM). This configuration is otherwise known as a “hardware mode”, where the HSM performs the following operations:

- securely generating, storing, and protecting the CA signing private key
- signing certificates, CRLs, and OCSP responder certificates using the CA signing private key
- protecting the data in the ECA database by generating a symmetric encryption key on the HSM that is used to provide protection of data stored in the ECA database

When deployed with ECA in the evaluated configuration, the HSM is considered part of the Operational Environment (OE) and outside the TOE boundary; as such, HSM functionality and security is not evaluated. However, the TOE functionality that uses the HSM is considered part of the TSF. ECA communicates with an HSM using a driver that implements the standard PKCS #11 API. The communication between the HSM driver and the HSM hardware is proprietary and completely opaque to the TOE.

Figure 2: HSM integration



Any FIPS 140-2 level 3-certified HSM that implements PKCS #11 is considered compatible with ECA. However, the following HSMs are known to correctly integrate with ECA:

- Entrust nShield Connect XC with Security World Client 12.80.4 or later
- Thales Luna Network HSM S700-series with Thales Luna Client 7.1.0-380 or later

1.3.4 TOE Software Requirements

1.3.4.1 Supported Platforms

The evaluated configuration includes the following supported platforms for ECA and ECAA.

Entrust Certificate Authority 10.1 is supported on the following platforms:

- Microsoft Windows Server 2019, 2022
- Red Hat Enterprise Linux (RHEL) 7.9 or later
- Red Hat Enterprise Linux (RHEL) 8.4, or later

Entrust Certificate Authority Administration 10.1 is supported on the following platforms:

- Microsoft Windows Server 2019, 2022 (with GUI)
- Microsoft Windows 10 64-bit
- Microsoft Windows 11 64-bit

1.3.4.2 Operational Environment Software

The TOE is designed to integrate with the following software components which are required to test all claimed security functionality:

Database The following external databases are supported by the TOE:

- PostgreSQL 13 or later (Community Version)
- EDB Postgres Advanced Server 13 or later
- Oracle 19c or later patch sets
- Microsoft SQL Server 2019 or later

Directory The following directory systems are supported by the TOE:

- Synchronoss Directory Server 8.1.0 or later
- Active Directory Domain Services – Windows Server 2019 or later

- Active Directory Lightweight Directory Services – Windows Server 2019 or later

OCSP Responder

The following VA/OCSP responder systems are supported by the TOE when a PostgreSQL or EDB Postgres Advanced Server external database is used:

- Entrust KeyOne VA[2] 4.0 or later

1.3.4.3 Optional Operational Environment Software

Entrust Certificate Agent is a software application which offers automatic lifecycle management of digital identities and certificates created by ECA. Entrust Certificate Agent can manage both software-based and smartcard-based certificates, and can be integrated with compatible FIPS 140-2 Level 2 smartcards to create and manage digital identities.

X.509 PKI end-users require client software components to communicate with the RA and CA to perform their lifecycle certificate management functions. Entrust Certificate Agent provides certificate lifecycle management functions.

All PKI end-user applications, including Entrust Certificate Agent, are outside the scope of evaluation as they have no CA or RA functionality.

The TOE is tested using testing tools written with the customer-provided toolkits listed below. These testing tools and toolkits themselves are not in the scope of the evaluated configuration. Entrust provides additional products that utilize these toolkits that customers can use with the TOE.

- Entrust Authority Security Toolkit for the Java Platform
- Entrust Authority Security Administration Toolkit for the Java Platform

In addition to Entrust Certificate Agent, the following modules/tools provided by Entrust use the above toolkits and can be used to exercise ECA X.509 functionality[3]:

- Entrust Administration Services CMP[4] v2 Service
- Entrust Administration Services User Management Service
- Entrust Administration Services User Registration Service
- Entrust Administration Services Certificate Expiry Service
- Entrust Administration Services Auto-enrollment Service
- Entrust Administration Services CSR Enrollment Services
- Entrust Administration Services CSR-SCEP Service
- Entrust Administration Services EST Service
- Entrust Administration Services MDM Web Service
- Entrust Administration Services MDM-SCEP Service
- Entrust Administration Services Windows Native Enrollment Service
- Entrust CA Gateway

[2] Validation Authority (VA)
[3] Note: The functionality of these tools is not in the scope of the evaluation and was not tested during the evaluation.
[4] Certificate Management Protocol

The TOE also supports issuance of ISO 7816 Card Verifiable (CV) certificates in support of Extended Access Control (EAC). EAC uses CV certificates to unlock biometric data stored in Machine Readable Travel Documents. These applications provided by Entrust use the above toolkits. Instead of using the local command shell, the following EAC software components could be used to remotely administer the EAC functionality:

- Entrust Administration Services CVCA Administration
- Entrust Administration Services DV Administration
- Entrust Administration Services DV Web Service
- Entrust Administration Services SPOC Administration
- Entrust Administration Services SPOC Web Service
- Entrust Administration Services SPOC Domestic Web Service
- Entrust Administration Services DV Certificate Key Management Service
- Entrust Authority IS[5] Concentrator
- Entrust Authority IS Client

1.4 TOE Description

The TOE is Entrust Certificate Authority (ECA) and Entrust Certificate Authority Administration (ECAA) 10.1, an enterprise public key infrastructure (PKI) solution. The TOE implements Certification Authority (CA) and Registration Authority (RA) functionality in the PKI deployment. ECA is an enterprise CA application designed to manage keys and issue certificates. ECAA is an enterprise RA application that offers an administrative interface designed to integrate with ECA to issue and manage certificates. ECAA is also designed to facilitate CA policy management.

The core services that are the basis for the PKI management functionality include:

- CA key management (managing CA signing key pair, master keys, database encryption keys, and enforcing infrastructure security policies)
- user management (providing the capability for authorized operators to manage other users including passwords, keys, roles and permissions, and so on)
- end-entity digital identities management (managing end-entity digital identities including creation, initialization, deletion, recovery, revocation, key update etc.)
- cross-certificate management (generating and maintaining X.509 cross-certificates) – not tested with Active Directory Domain Services
- CRL issuance at specified regular intervals
- signing OCSP responder certificates
- publishing revocation information to an OCSP responder
- Country Verifying Certificate Authority (CVCA) management (managing CVCA keys, modelling DVs, and managing DV keys)
- Document Verifier (DV) management (managing DV keys, managing relationships with CVCAs, modelling Inspection Systems, and managing Inspection System keys)

The support services provided by ECA with respect to the CA infrastructure include:

[5] IS = Inspection System

- self-management (initializing ECA, configuring master users and the First Officer, creating the default security policies, and starting and stopping ECAA services)
- audit trail management (maintaining and analyzing a secure audit record of critical and non-critical events within the infrastructure)
- directory management (maintaining the schema and directory entries related to the CA environment)

1.4.1 Deployment

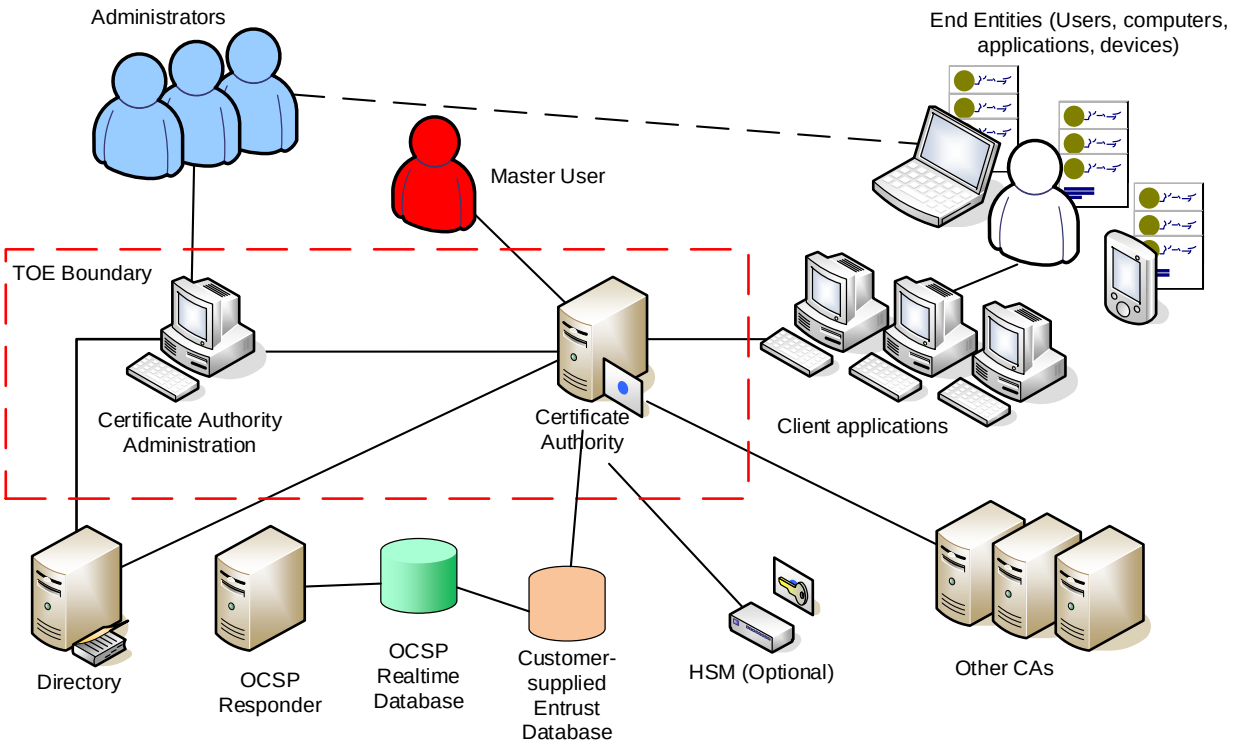
ECA PKI systems are deployed in the following primary types of environments:

- traditional hierarchical X.509 CA environments with one or more PKI applications
- ePassport Country Verifying CA environments which issue ISO 7816 Card Verifiable (CV) certificates in support of Extended Access Control (EAC)

In all these environments, the TOE requires a database to store relevant information: master keys, security policies, certificate policies, digital identities, and information about the entities that were issued certificates.

The CA publishes CA certificates, end entity certificates, policies, and CRLs to a directory.

Figure 3: TOE Deployment



1.4.1.1 Traditional X.509 deployment

Traditional hierarchical deployments support one or more PKI applications using X.509 certificates with revocation checking. Typical deployments include ECA and ECAA running on dedicated hardware. These deployments include a database and a connection to a directory service for publishing certificates and

CRLs. ECA uses various certificate profiles to issue certificates that are tailored to specific application requirements (such as TLS Certificates for e-commerce or publicly-secure Web sites).

This type of deployment supports the [X.509] and [RFC 5280] standards. This type of deployment also supports additional standards to meet application-specific requirements.

1.4.1.2 ePassport EAC deployment

ePassport EAC is implemented using ECA with different license codes: CVCA for Domestic DVs, CVCA for Foreign DVs, and DV for Inspection Systems. An ePassport EAC deployment of ECA creates an X.509 CA for administration and an EAC CA for issuance and management of Card Verifiable (CV) certificates.

An Extended Access Control (EAC) infrastructure has two distinct types of CAs:

- A Country Verifying Certification Authority (CVCA) is a trusted CA within a country. Countries can have multiple CVCAs. The CVCA is used for the country's EAC implementation. A CVCA issues certificates to Document Verifier (DV) CAs within its own country as well as to DVs in other countries.
- A Document Verifier (DV) is a distinct type of a CA that issues certificates to Inspection Systems (IS) within its own direct area of responsibility. There may be several DVs in a given country. An IS uses its certificates to authenticate to the ePassport chip to unlock the biometric data stored on the chip, and validates the signatures on this biometric data.

Each Entrust Certificate Authority EAC deployment must be either a CVCA (Country Verifying Certification Authority) or a DV (Document Verifier), but cannot be both due to the nature of the entities and the trust model. Certificates issued to CVCAs, DVs, and ISs are not published in the directory, are short-lived, and by definition have no revocation scheme.

A digital signature on an ePassport is derived from the Country Signing Certification Authority (CSCA) certificate and the Document Signer Certificate (DSC). Together, the signature and certificates form a trust chain to the Certification Authority of the issuing country, and they are securely stored on the chip of the ePassport as the Document Security Object.

This type of deployment supports the [ICAO] and [RFC 5280] standards.

1.4.1.3 Operational Environment Client Systems

1.4.1.3.1 X.509

The TOE can interact with administrative client systems and end user client systems. In the evaluated configuration, the TOE communicates with administrative client systems using Administration Service Handler (ASH), XML Administration Protocol (XAP) or CMP. End user client systems use CMP exclusively. The only client system in the TOE is the ECAA.

The TOE issues X.509v3 certificates that can secure user and device identities. For example, a Web browser connecting to a Web server could consume a certificate generated by the TOE.

ECA can generate different types of digital certificates. Each certificate type is managed according to the ECA Security Policy. Security Policies are created and managed using Registration Authorities (RAs), in this case Entrust Certificate Authority Administration (ECAA). Certificates are issued to end users using the RA. This process typically involves verification of the end user identity.

Certificate lifecycle management can be done using Entrust Certificate Agent. Entrust Certificate Agent is an application that is capable of automatically integrating with ECA. Entrust Certificate Agent is installed on the client systems for transparent management of the digital identities.

1.4.1.3.2 EAC

The TOE also supports the issuance of ISO 7816 Card Verifiable (CV) certificates in support of Extended Access Control (EAC). EAC uses CV certificates to unlock biometric data stored in Machine Readable Travel Documents (MRTDs). Optional EAC software components can be used to remotely administer the EAC functionality.

1.4.2 Entrust Certificate Authority

Entrust Certificate Authority 10.1 is the Certification Authority (CA) and the core component of the TOE. The main functions of ECA are:

- creation of key pairs for CA
- creation of key pairs for users
- creation of certificates for all public keys
- management of a secure database that allows the recovery of users' key pairs
- maintaining certificate revocation lists
- enforcement of an organization's security policy

ECA includes other capabilities to enhance the security of an organization, including:

- ability to interoperate with other CAs or with other PKI-enabled products
- ability to support and maintain a strict CA hierarchy and provide fine-grained control to limit relationships between CAs
- ability to specify and modify the actions that administrators and users can perform using a flexible configuration of roles, groups, user registration dialogs, and user settings
- use of ISO 7816 certificates to support EAC for ePassports
- ability to specify the CA signing algorithm and CA signing key size
- ability to specify the CVCA signing algorithm and key size
- ability to specify the DV signing algorithms and key sizes
- ability to renew the CA signing key pair, CVCA signing key pair, or DV signing key pairs before they expire, and to recover from possible CA key compromise

1.4.3 Entrust Certificate Authority Administration

Entrust Certificate Authority Administration 10.1 is the Registration Authority (RA) application that provides the graphical administrative interface for the TOE. ECAA is restricted to the TOE Administrators, where they authenticate themselves using digital certificates. ECAA is primarily used for:

- Management of X.509 users
- X.509 certificate issuance
- renewal of X.509 certificates
- revocation of issued X.509 certificates
- initiation of client X.509 key recovery operations
- configuration of security policies
- configuration of certificate templates
- review of audit logs

All messages between ECAA and ECA are secured for confidentiality, integrity, and authentication. ECA and ECAA communicate using the ASH and CMP protocols. Messages over the ASH protocol are secured via a TLS v1.2 tunnel provided by the operational environment. The TOE protects the confidentiality and integrity of all private keys[6] and secret keys[7] transferred between entities using the CMP protocol. The CMP protocol also protects the integrity of certificates and public keys.

1.4.4 TOE Physical Boundary

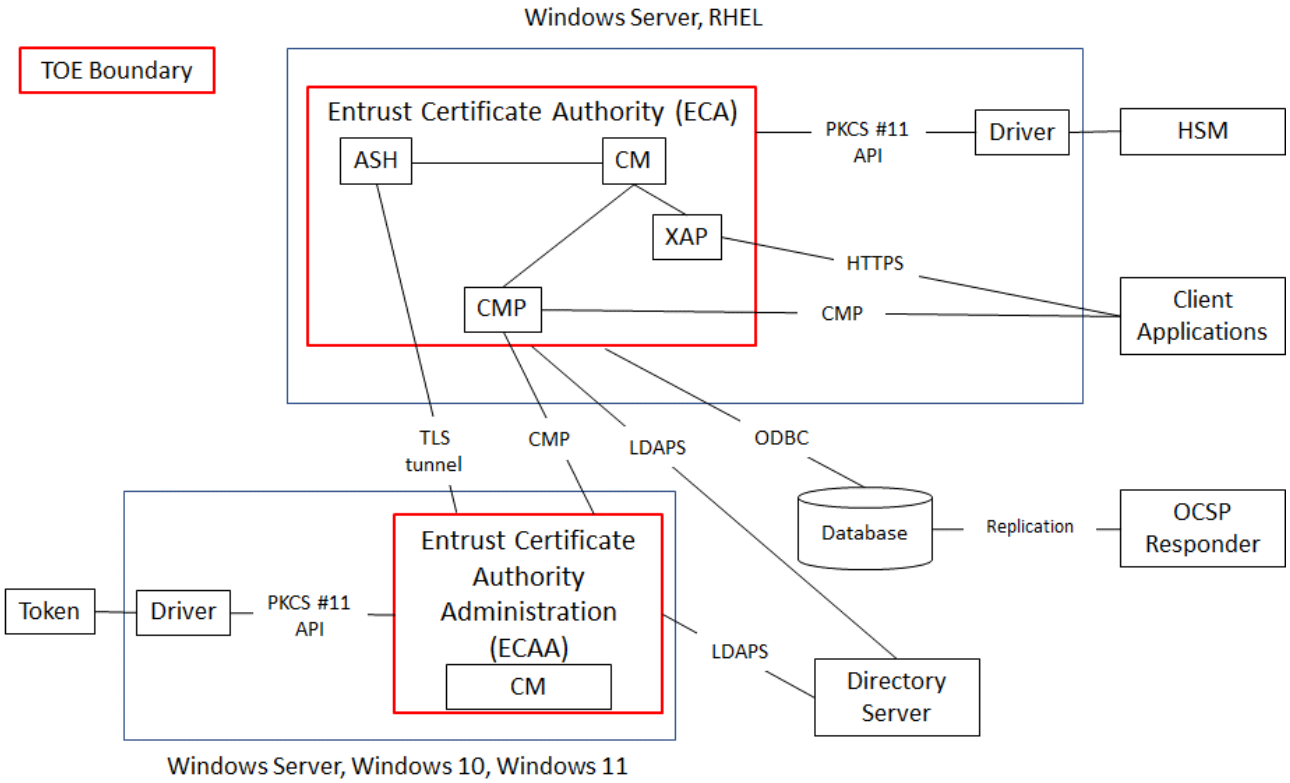
The TOE is a software-only application that is installed on an operating system running on dedicated hardware. The TOE includes two components: ECA and ECAA. The TOE does not include the hardware or the operating system on which it is installed. All hardware used to deploy the TOE is in the operational environment. (Refer to Sections 1.3.3 and 1.3.4 for a list of the hardware and software in the operational environment.)

Figure 4 depicts the physical boundary for the TOE. The Client Applications box in the figure represents both end user clients and administrative clients. End User clients only use the CMP protocol. Administrative clients use both the CMP and XAP over HTTPS protocols.

[6] Private keys may be stored for long periods. Private keys include ECA keys, administrative personnel keys, and, for key recovery purposes, private keys backed up in the ECA DB.

[7] The term secret keys refers to symmetric keys and authorization codes. Symmetric secret keys may be used to encrypt other secret or private keys when they are stored within or exported from the ECA. Authorization codes may be used to authenticate subscribers (users).

Figure 4: TOE Physical Boundary



ECA is delivered as a signed installer package compatible with either Windows Installer 5.0 (MSI installer) or RHEL yum installer (rpm package). The ECA deployment can also optionally install and configure PostgreSQL Database 12 as a local database for ECA, but this is not allowed in the evaluated configuration.

ECAA is delivered as a signed installer compatible with Windows Installer 5.0 (MSI installer).

Both installers are downloaded from the vendor's Web site (https://trustedcare.entrust.com), a secure portal which requires valid credentials to access the resources.

The TOE includes the guidance documentation which contains information on how to manage the TOE security functions. The guidance documentation is delivered to customers via a download from the vendor's Web site.

The TOE guidance includes the following documentation:

- Entrust Certificate Authority 10.1, Operations Guide, Document Issue 3.0, Date of Issue May, 2022
- Entrust Certificate Authority Administration 10.1, User Guide, Document Issue 2.0, Date of Issue May, 2022
- Entrust Certificate Authority 10.1, Installation Guide, Document Issue 2.0, Date of Issue May, 2022
- Entrust Certificate Authority 10.1 Deployment Guide, Document Issue 2.0, Date of Issue May 2022
- Entrust Certificate Authority 10.1 Database Configuration Guide, Document Issue 3.0, Date of Issue May 2022

- Entrust Certificate Authority 10.1 Directory Configuration Guide, Document Issue 2.0, Date of Issue May 2022
- Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide, Document Issue 1.0, Date of Issue November 2, 2022
- Entrust ePassport Solutions Guide 4.10, Document Issue 3.0, Date of issue May 2022

1.4.5 TOE Logical Boundary

The logical boundary of the TOE is defined by implemented security functionality as summarized in Section 1.3.2 of this document. Both ECA and ECAA include a Cryptographic Module (CM), Entrust Authority Security Kernel, which implements all cryptographic primitives used in utilized cryptographic protocols. The Entrust Authority Security Kernel is a multi-chip standalone FIPS 140-2 Level 2 validated (CMVP 3981) software-based module.

In the evaluated configuration, ECA and ECAA will communicate over a TLS v1.2 (RFC 5246) tunnel when using the Administration Service Handler (ASH) protocol. The TLS v1.2 tunnel is a required part of the operational environment. ASH is a proprietary protocol. Most X.509 certificate issuance is performed using the Certificate Management Protocol (CMP) (RFC 2510, RFC 2511 with partial support for RFC 4510 and RFC 4511).

The ECA XML Administration Protocol (XAP) subsystem supports X.509 administrative operations, EAC administrative operations, and EAC certificate management operations. XAP communications between ECA and administrative end clients are implemented by the TOE over an HTTPS connection.

The database and directory server used by ECA are required parts of the operational environment.

1.4.5.1 Security Audit

The ECA component of the TOE generates audit records for all security-relevant events. ECA can be configured to select which audit records are generated based on various attributes. For each event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The audit trail is protected from unauthorized modification and will detect changes to the audit records. The TOE also implements timestamps to ensure reliable audit information produced.

1.4.5.2 Identification and Authentication

Before any action, each user is identified with a login name or subject identity, and authenticated with either (a) a password or (b) a certificate and the associated private key. Each authorized user is associated with a subject identity, assigned role and specific permissions that determine access to TOE features.

1.4.5.3 Security Management

The ECAA component of the TOE provides GUI-based remote administration, separate from the command line interface.

The TOE implements roles that are used to control what operations users are allowed to perform on the TOE. All of the management functions are restricted according to the role assigned to the user or administrator.

The security management functions provided by the TOE include the ability to manage user accounts and roles, administer system configuration, view the audit records, configure the security audit functionality, certificate registration, certificate status change, PKI configuration, Certificate profile management, Revocation profile management, and Certificate Revocation List management.

ECA also enforces an access control policy on the ECA system data associated with the key and certificate functions performed by the ECA.

1.4.5.4 Remote Data Entry and Export

The TOE provides the ability to assure the identity of parties exchanging data using digitally signed certificates and revocation lists. This includes generating and verifying evidence of the identity of the originator of information.

The operational environment is configured to provide a TLS tunnel to protect communications between the TOE components (the ECA and ECAA) using the ASH protocol. Communications with the database are over TLS provided by the ODBC driver, where the ODBC driver is part of the operational environment.

The TOE implements CMP to protect the transfer of keys and certificates between its own components and between the TOE and the trusted external entities, such as administrative client applications and end entity client applications. To protect communications from modification and disclosure, the TOE also implements TLS v1.2 between:

- ECA and directory (LDAP over TLS)
- ECAA and directory (LDAP over TLS)
- ECA and XAP clients (XAP, a protocol which transfers information over HTTPS)

1.4.5.5 Certificate Management

The TOE generates certificates and establishes proof of possession before providing the certificate to the end user. The TOE is able to implement certificate definitions that comply with the specification provided by an Administrator.

1.4.5.6 Certificate Revocation

ECA generates and issues X.509 version 2 Certificate Revocation Lists. ECA can also publish certificate and certificate revocation information to an Online Certificate Status Protocol (OCSP) responder.

1.4.5.7 Key Management

The ECA component of the TOE makes use of the Cryptographic Module (CM) to perform the following cryptographic functionality:

- Key generation
- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification
- Entropy is collected and used to support seeding
- Critical Security Parameters (CSPs) are protected so that they are not directly viewable in plaintext and stored internally.
- CSPs are cleared when no longer in use

The CM also protects all private and secret key material using cryptographic mechanisms. The ECA protects public keys stored in the database against unauthorized modification.

The ECA component of the TOE uses that same CM to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs.

1.4.6 Excluded Functionality

The following TOE functionality is excluded and not enabled/utilized in the evaluated configuration:

- Proto-PKIX (SEP) - a proprietary protocol that handles certificate requests from legacy applications
- Autologin

- Database backup, which is only available with the embedded database that is not included in the evaluated configuration
- Cross-certification and subordinate CAs when using an Active Directory Domain Services

Administrative guidance will instruct administrators to not use the following features of the TOE. Use of the following TOE functionality is not permitted in the evaluated configuration and must not be used by administrators:

- CA migration functionality – provides the ability to migrate an existing CA from non-TOE software. This includes importing private keys and revocation lists.
- Move user functionality - allows for end-users to be moved from one TOE CA to a different TOE CA. This includes importing and exporting of private keys.
- Archive user functionality - allows archiving end-users that are not currently being used from the ECA database to an archive file.
- Smart Energy Profile 2 CAs
- Constructs used to store and protect the digital identities and certificates created by ECA (such as Entrust profiles)
- Online cross-certification is excluded from the evaluated configuration. (Note: Offline cross-certification is included in the evaluated configuration.)
- Online subordinate CA creation is excluded from the evaluated configuration. (Note: Offline subordinate CA creation is included in the evaluated configuration.)
- XAP user registration password functionality is excluded from the evaluated configuration. (This functionality allows a 'registration password' to be specified for a user. XAP provides an operation for matching a user-specified password against the known registration password that is stored in the database.)
- Use of an Entrust-supplied embedded PostgreSQL database is excluded from the evaluated configuration.
- Use of the ASH protocol by client systems other than ECAA
- Use of entropy in certificate validity dates
- Ability to view pre-10.0 audits
- Ability to archive audits from the DB
- Ability to repair revocation lists and user reference numbers
- Use of User attribute certificates
- Use of ECAA bulk commands
- Use of Entrust profiles for administrative users (.epf)
    - In the evaluated configuration, administrators must not use ECAA to create Entrust profiles for administrative users or for end users. Instead, administrators should use ECAA to create all such credentials on a PKCS #11 tokens.

The following TOE functionality is allowed, but does not interfere with the security functionality and was not tested during the CC certification:

- entDerEncoder utility
- High Availability (support for multiple CA nodes, also known as an Entrust CA cluster) and Listener Service
- Use of ECAA with multiple ECAs

2 Conformance claims

2.1 CC Conformance Claim

This ST is compliant with the following:

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April, 2017 [CC]
- CC Part 2 extended
- CC Part 3 conformant

2.2 PP and Package Claim

This ST does not claim conformance with any Protection Profiles.

This ST claims to be Security Assurance Level EAL 4 augmented with ALC_FLR.2.

3 Security Problem Definition

This section provides the following policies, threats and assumptions about the TOE.

3.1 Threats

Table 2: Authorized User Threats

Threat Name	Definition
T.Administrators commit errors or hostile actions	An administrative user commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.
T.User abuses authorization to collect and/or send data	User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.

Table 3: System Threats

Threat Name	Definition
T.Critical system component fails	Failure of one or more system components results in the loss of system critical functionality.
T.Message content modification	A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.

Table 4: Cryptographic Threats

Threat Name	Definition
T.Disclosure of private and secret keys	A private or secret key is improperly disclosed. The threat agent is an authorized user or erroneous protocol. An adverse action can be compromise of the security of the PKI and/or relying party systems that rely on PKI objects such as certificates or CRLs.
T.Modification of private/secret keys	A secret/private key is modified. The threat agent is an authorized user or erroneous protocol. An adverse action can be compromise of the security of the PKI and/or relying party systems that rely on PKI objects such as certificates or CRLs.

Table 5: External Attacks

Threat Name	Definition
T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

3.2 Organizational Security Policies (OSPs)

Table 6: Policy

Policy Name	Definition
P.Authorized use of information	Information shall be used only for its authorized purpose(s).
P.Cryptography	The TSF shall exclusively rely on verified cryptographic primitives to perform all cryptographic operations.

3.3 Assumptions

The usage assumptions are organized in three categories: personnel (assumptions about administrators and users of the system as well as any threat agents), physical (assumptions about the physical location of the TOE or any attached peripheral devices), and connectivity (assumptions about other IT systems that are necessary for the secure operation of the TOE).

Table 7: Personnel Assumptions

Assumption Name	Definition
A.Administrators Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Administrators.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)
A.Competent Administrators	Competent administrative users will be assigned to manage the TOE and the security of the information it contains.
A.CPS	All administrative users are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.

Table 8: Connectivity Assumptions

Assumption Name	Assumption Definition
A.Operating System	The operating system has been selected to provide the following functions required by this PKI to counter the perceived threats as identified in this ST: identification and authentication, process isolation and separation, reliable time stamps, file system access controls, enforcement of a TLS tunnel for ASH protocol communications.
A.Tunnel	The operational environment will protect the ASH protocol communications between ECA and ECAA from modification and disclosure. The operational environment will also protect the ODBC communications between ECA and the database from modification and disclosure.

Table 9: Physical Assumptions

Assumption Name	Assumption Definition
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical access.

4 Security Objectives

This section defines the Security Objectives (SOs) of the TOE and its supporting environment.

4.1.1 Security Objectives for the TOE

Table 10: TOE Security Objectives

Objective	Definition
O.Certificates	The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid and up to date.
O.Cryptographic functions	The TSF must implement all cryptographic functionality underpinned by the approved cryptographic standards for encryption/decryption, authentication, signature generation/verification algorithms, and key generation techniques. The TSF must use hardened cryptographic modules.
O.Non-repudiation	Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.
O.Data import/export	Protect keys and certificates when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
O.Individual accountability and audit records	Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.
O.Integrity protection of user data and software	Provide integrity protection using checksums for user data and software.
O.Limitation of administrative access	Design administrative functions so that administrative users do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Administrators who troubleshoot the system and perform system updates.
O.Maintain user attributes	Maintain a set of security attributes (which may include role membership, access permissions, etc.) associated with individual users. This is in addition to user identity.
O.Manage behavior of security functions	Provide management functions to configure, operate, and maintain the security mechanisms.
O.Protect stored audit records	Protect audit records against unauthorized access or modification to ensure accountability of user actions.
O.Protect user and TSF data during internal transfer	Ensure the integrity and confidentiality of user and TSF data transferred internally within the system using CMP.
O.Restrict actions before authentication	Restrict the actions a user may perform before the TOE authenticates the identity of the user.
O.Security-relevant configuration management	Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
O.Security roles	Maintain security-relevant roles and the association of users with those roles.
O.Time stamps	Provide time stamps to ensure that the sequencing of events can be verified.

4.1.2 Security Objectives for the Operational Environment (OE)

Table 11: Operational Environment Security Objectives

Objective	Definition
OE.Installation	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.
OE.Operating System	The operating system is hardened to provide adequate security, including identification and authentication, process isolation and separation, reliable time stamps, file system access controls, enforcement of a TLS tunnel for ASH protocol communications.
OE.Physical Protection	Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.
OE.Sufficient backup storage and effective restoration	Provide sufficient backup storage and effective recovery procedures to ensure that the system can be recreated.
OE.Control unknown source communication traffic	The operational environment must control (e.g. reroute or discard) communication traffic from unknown sources to prevent potential damage.
OE.Administrative guidance documentation	Deter administrative user errors by providing adequate documentation on securely configuring and operating the TOE.
OE.Administrators Review Audit Logs	Identify and monitor security-relevant events by requiring Administrators to review audit logs on a frequency sufficient to address level of risk.
OE.User authorization management	Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.
OE.Tunnel	ASH protocol communications between ECA and ECAA will be protected from modification and disclosure using a TLS v1.2 tunnel provided by the operational environment. ODBC protocol communications between ECA and the database will be protected from modification and disclosure using a TLS v1.2 tunnel provided by the ODBC driver in the operational environment.

5 Extended Components Definition

These extended components were created using the Certificate Issuing and Management Components Protection Profile, Version 1.5, August 11, 2011 as a guideline.

5.1 Extended FAU Components

5.1.1 Audit Trail Storage Integrity

FAU_STG_EXT.1 **Audit trail storage integrity**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.1.1 The TSF shall be able to [**selection, chose one of:** ***prevent, detect***] unauthorized modifications to the stored audit records in the audit trail.

Rationale: This component is based on the CC Part 2 FAU_STG.1 and is necessary because FAU_STG.1 in CC Part 2 also requires that the TSF be able to protect the stored audit records from unauthorized deletion. In this system, the database in the operational environment is responsible for protecting stored audit records from unauthorized deletion. The TSF does provide the functionality to detect unauthorized modifications to stored audit records.

5.2 Extended FCO Components

Enforced Proof of Origin and Verification of Origin

FCO_NRO_EXT.3 **Enforced proof of origin and verification of origin**

Hierarchical to:FCO_NRO.2

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO_EXT.3.1 The TSF shall enforce the generation of evidence of origin for certificate status information and all other security-relevant information at all times.

FCO_NRO_EXT.3.2 The TSF shall be able to relate the identity and [**assignment:** ***other attributes***] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

Application Note: The ST shall specify the list of other attributes that shall be linked to the information, for example, time of origin and location of origin.

FCO_NRO_EXT.3.3 The TSF shall verify the evidence of origin of information for all security-relevant information.

Rationale: This component is necessary as FCO_NRO.1.1 states that a request is to be made for the TSF to perform the action of generating evidence of origin, whereas it is expected that the TSF will perform this task automatically. The language in FCO_NRO.1.3 also attempts to narrow down limitations on the evidence, yet the TSF is expected to operate in a ubiquitous manner. Thus, although

FCO_NRO.1.2 could be used, an extended component is required due to the other requirements. This TSF supports the Security Objectives **O.Non-repudiation**

NOTE: Based on FCO_NRO_EXT.3, the TSF shall reject any information whose origin cannot be verified unless:

a) Acceptance of the information will not cause the TSF to perform any security relevant functions; and

b) Acceptance of the data will not cause the TSF to output or export any confidential information.

The TSF may, for example, accept information whose origin cannot be verified in the following case:

b) The received information will not be processed until an authorized user has accepted its contents (e.g., a certificate request). In this case, the received information may be processed as if it had originated from the authorized user who approved it.

5.2.1 Advanced Verification of Origin

FCO_NRO_EXT.4	**Advanced verification of origin**
	Hierarchical to: No other components.
	Dependencies: FCO_NRO_EXT.3
FCO_NRO_EXT.4.1	The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using a keyed hash based on an authentication code.
FCO_NRO_EXT.4.2	The TSF shall, for initial certificate registration messages sent on behalf of the certificate subject, only accept messages protected using a digital signature of an authorized administrator.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by existing CC requirements. It supports the security objective **O.Non-repudiation**.

5.3 Extended FCS Components

5.3.1 Cryptographic Parameter Transfer

FCS_CPT_EXT.1	**Cryptographic Parameter Transfer**
	Hierarchical to: No other components.
	Dependencies: No dependencies.
FCS_CPT_EXT.1.1	When using the CMP protocol, the TSF shall protect certificates, public keys, symmetric keys, and private keys from modification when transmitted between separate parts of the TOE.
FCS_CPT_EXT.1.2	When using the CMP protocol, the TSF shall protect certificates, public keys, symmetric keys, and private keys from modification when transmitted between the TOE and the PKI end-user application.

FCS_CPT_EXT.1.3 When using the CMP protocol, the TSF shall protect symmetric keys and private keys from disclosure when transmitted between separate parts of the TOE and between the TOE and the PKI end-user application.

Rationale: This component is necessary to clearly specify a unique requirement for PKI components requiring the protection of keys and certificates during transmission between parts of the TOE and between the TOE and the PKI end-user application.

5.3.2 Cryptographic Key Derivation

FCS_KDF_EXT.1 **Cryptographic Key Derivation**

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

FCS_KDF_EXT.1.1 The TSF shall utilize a password (or secret) and salt to derive an intermediate key, as defined in NIST SP 800-132 using keyed-hash functions, which is used to protect TSF data stored in the database.

Application Note: The keyed-hash functions used to derive the intermediate key must be specified in an iteration of FCS_COP.1.

5.4 Extended FDP Components

5.4.1 User Private Key Confidentiality Protection

FDP_ACF_EXT.2 **User private key confidentiality protection**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ACF_EXT.2.1 Administrator private keys shall be stored in a cryptographic module or stored in encrypted form. If Administrator private keys are stored in encrypted form, the encryption shall be performed by the cryptographic module.

FDP_ACF_EXT.2.2 If end entity private keys are stored in the TOE, they shall be encrypted. The encryption shall be performed by the cryptographic module.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.4.2 User Secret Key Confidentiality Protection

FDP_ACF_EXT.3 **User secret key confidentiality protection**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ACF_EXT.3.1 User secret keys[8] stored within the TOE, but not within a cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the cryptographic module.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.4.3 Certificate Generation

FDP_CER_EXT.1 **Certificate Generation**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_CER_EXT.1.1 The TSF shall only generate certificates whose format complies with [**selection:** ***the X.509 standard for public key certificates, ISO 7816 Card Verifiable (CV) certificates***].

FDP_CER_EXT.1.2 The TSF shall only generate certificates that are consistent with the currently defined certificate profile.

FDP_CER_EXT.1.3 Unless the certificate request is signed by an administrator, the TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FDP_CER_EXT.1.4 If the TSF generates X.509 public key certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that:

a) The **`version`** field shall contain the integer **0**, **1**, or **2**.

b) If the certificate contains an **`issuerUniqueID`** or **`subjectUniqueID`** then the `version` field shall contain the integer **1** or **2**.

c) If the certificate contains extensions then the **`version`** field shall contain the integer **2**.

d) The **`serialNumber`** shall be unique with respect to the issuing Certification Authority.

e) The **`validity`** field shall specify a **`notBefore`** value that is not preceded by the **`notAfter`** value.

f) The **`issuer`** field must contain a non-empty distinguished name (DN).

g) If the **`subject`** field contains a null **`Name`** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **`subjectAltName`** extension.

h) The **`signature`** field and the algorithm in the **`subjectPublicKeyInfo`** field shall contain the OID for an approved algorithm.

[8] The user secret keys are the authorization codes.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.4.4 Certificate Revocation List Validation

FDP_CRL_EXT.1 **Certificate revocation list validation**

Hierarchical to: No other components.

Dependencies: No dependencies

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 TSF shall ensure that:

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) The **`issuer`** field must contain a non-empty distinguished name (DN).
d) The **`signature`** and **`signatureAlgorithm`** fields shall contain the OID for a claimed digital signature algorithm.
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.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.4.5 Certificate Status Export

FDP_CSE_EXT.1 **Certificate status export**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_CSE_EXT.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3.

FDP_CSE_EXT.1.2 Certificate status information shall be exported from the TOE to an OCSP responder for the purpose of generating an OCSP response as specified in RFC 6960.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.4.6 Extended User Private and Secret Key Export

FDP_ETC_EXT.5 **Extended user private and secret key export**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ETC_EXT.5.1 User private and secret keys shall only be exported from the TOE in encrypted form.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.4.7 Stored Public Key Integrity Monitoring and Action

FDP_SDI_EXT.3 **Stored public key integrity monitoring and action**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_SDI_EXT.3.1 Public keys stored within the PKI, but not within a cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_EXT.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall [**assignment: *action taken to deny access to the key***].

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.5 Extended FMT Components

5.5.1 Extended Certificate Profile Management

FMT_MOF_EXT.3 **Extended certificate profile management**

Hierarchical to: No other components.

Dependencies: FMT_MOF.1 Management of security functions behavior
FMT_SMR.1 Security roles

FMT_MOF_EXT.3.1 The TSF shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_EXT.3.2 The TSF shall require [**assignment: *the authorized identified role***] to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;
- the length of time for which the certificate is valid;

FMT_MOF_EXT.3.3 If the certificates generated are X.509 public key certificates, the TSF shall require [Administrators] to specify the set of acceptable values for the following fields and extensions:

- **`keyUsage`**;
- **`basicConstraints`**;
- **`certificatePolicies`**

FMT_MOF_EXT.3.4 The TSF shall require [**assignment: *the authorized identified role***] to specify the acceptable set of certificate extensions.

Rationale: This component is necessary to specify a unique requirement of PKI components that is not addressed by the CC Part 2.

5.5.2 Extended Certificate Revocation List Profile Management

FMT_MOF_EXT.5 **Extended certificate revocation list profile management**

Hierarchical to: No other components.

Dependencies: FMT_MOF.1 Management of security functions behavior
FMT_SMR.1 Security roles

FMT_MOF_EXT.5.1 If the TSF issues CRLs, the TSF must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.

FMT_MOF_EXT.5.2 If the TSF issues CRLs, the TSF shall require the [**assignment: *the authorized identified role***] to specify the set of acceptable values for the following fields and extensions:

- **`nextUpdate`** (i.e., lifetime of a CRL).

FMT_MOF_EXT.5.3 If the TSF issues CRLs, the [**assignment: *the authorized identified role***] shall specify the acceptable set of CRL and CRL entry extensions.

Rationale: This component is necessary to specify a unique requirement of PKI components that is not addressed by the CC Part 2.

5.5.3 Private Key Confidentiality Protection

FMT_MTD_EXT.4 **TSF private key confidentiality protection**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_MTD_EXT.4.1 The CA private keys shall be stored in a cryptographic module or stored in encrypted form. If the CA private keys are stored in encrypted form, the encryption shall be performed by the cryptographic module.

FMT_MTD_EXT.4.2 The CA profile keys shall be stored in encrypted form in the CA database or stored in the local filesystem protected by the operational environment. If CA profile keys are stored in encrypted form, the encryption shall be performed by the cryptographic module.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.5.4 Secret Key Confidentiality Protection

FMT_MTD_EXT.5 **TSF secret key confidentiality protection**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_MTD_EXT.5.1 TSF secret keys[9] stored within the TOE, but not within a cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the cryptographic module.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

5.5.5 Extended TSF Private and Secret Key Export

FMT_MTD_EXT.7 **Extended TSF private and secret key export**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_MTD_EXT.7.1 TSF private and secret keys shall only be exported from the TOE in encrypted form.

Rationale: This component is necessary to specify a unique requirement for PKI components that is not addressed by the CC Part 2.

[9] TSF secret keys are keys used to generate symmetric keys that are used to encrypt other secret or private keys when they are stored within or exported from the ECA.

6 Security Requirements

6.1 Security Functional Requirements

This section specifies the security functional requirements that are applicable to the TOE.

Table 12: TOE Security Functional Requirements

Security Requirement		Component
Security Audit (FAU)	Audit data generation	FAU_GEN.1
	User identity association	FAU_GEN.2
	Audit review	FAU_SAR.1
	Selective audit	FAU_SEL.1
	Audit trail storage integrity	FAU_STG_EXT.1
Communication (FCO)	Enforced proof of origin and verification of origin	FCO_NRO_EXT.3
	Advanced verification of origin	FCO_NRO_EXT.4
Cryptographic Support (FCS)	Cryptographic key generation	FCS_CKM.1
	Cryptographic key destruction	FCS_CKM.4
	Cryptographic operation	FCS_COP.1
	Cryptographic parameter transfer	FCS_CPT_EXT.1
	Cryptographic key derivation	FCS_KDF_EXT.1
User Data Protection (FDP)	Subset access control	FDP_ACC.1
	Security attribute based access control	FDP_ACF.1
	User private key confidentiality protection	FDP_ACF_EXT.2
	User secret key confidentiality protection	FDP_ACF_EXT.3
	Certificate Generation	FDP_CER_EXT.1
	Certificate revocation list validation	FDP_CRL_EXT.1
	Certificate status export	FDP_CSE_EXT.1
	Extended user private and secret key export	FDP_ETC_EXT.5
	Stored public key integrity monitoring and action	FDP_SDI_EXT.3
Identification and Authentication (FIA)	User attribute definition	FIA_ATD.1
	Timing of authentication	FIA_UAU.1
	Timing of identification	FIA_UID.1
	User-subject binding	FIA_USB.1
Security Management (FMT)	Management of security functions behavior	FMT_MOF.1
	Extended certificate profile management	FMT_MOF_EXT.3
	Extended certificate revocation list profile management	FMT_MOF_EXT.5
	Management of security attributes	FMT_MSA.1
	Static attribute initialization	FMT_MSA.3
	Management of TSF data	FMT_MTD.1

Security Requirement		Component
	TSF private key confidentiality protection	FMT_MTD_EXT.4
	TSF secret key confidentiality protection	FMT_MTD_EXT.5
	Extended TSF private and secret key export	FMT_MTD_EXT.7
	Specification of management functions	FMT_SMF.1
	Restrictions on security roles	FMT_SMR.2
Protection of the TSF (FPT)	Reliable time stamps	FPT_STM.1
Trusted path/channels (FTP)	Inter-TSF trusted channel	FTP_ITC.1

Conventions

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 FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
  - **Assignment**: allows the specification of an identified parameter. Assignments 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 are indicated using bold and are surrounded by brackets (e.g., **[selection]**).
  - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***. Deletions are denoted with strikethrough text.

6.1.1 Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [**not specified]** level of audit; and
c) ***[The events listed in Table 13]***.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[the information specified in the Additional Details column in Table 13]***.

Additionally, the audit shall not include plaintext private or secret keys or other critical security parameters.

Table 13: Auditable Events and Audit Data

Section / Function	Component	Event	Additional Details
Public Key Access	FDP_SDI_EXT.3 Stored public key integrity monitoring and action	Verification of the checksum used to protect a public keys in the DB fails.	
Private Key Storage		All access to end entity private keys retained within the TOE for key recovery purposes	
Trusted Public Certificate Entry, Deletion	FMT_MOF.1	Import and deletions of trusted public certificates	Certificate serial number, subject, subject alternative name, certificate validity dates, authority key identifier and subject key identifier
Private Key Export	FDP_ETC_EXT.5 Extended user private and secret key export	The export of private keys	
	FMT_MTD_EXT.7 Extended TSF private and secret key export		
Certificate Registration	FDP_CER_EXT.1 Certificate Generation	All accepted X.509 certificate requests and accepted ISO 7816 certificate requests.	If certificate request is accepted, certificate type, the key type associated with the certificate, certificate serial number, subject, subject alternative name, certificate validity dates, signing CA.
Certificate Status Change Approval		All approved requests to change the status of a certificate.	
TSF Configuration		Successful security-relevant events for creating, modifying and deleting the configuration settings identified in Table 14.	
Certificate Profile Management	FMT_MOF_EXT.3 Extended certificate profile management	All changes to the certificate Profile	The key changes, additions, and deletions to the profile
Certificate Revocation List Profile Management	FMT_MOF_EXT.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile

FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 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

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide ***[administrative users with the Audit Log Permission: View user logs, Audit Log Permission: View own logs or Audit Log Permission: View all logs]*** with the capability to read ***[all of the relevant data]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SEL.1 Selection audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [**event type *(severity)***]
b) [***event number, range of event numbers***].

FAU_STG_EXT.1 Audit trail storage integrity

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.1.1 The TSF shall be able to [**detect**] unauthorized modifications to the stored audit records in the audit trail.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.2 Security Management

6.1.2.1 Roles

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [**modify the behavior of**] the functions [***listed in Table 14***] to [***the authorized roles as specified in Table 14***].

Table 14: Authorized Roles for Management of Security Functions Behavior

Section / Function	Component	Function / Authorized Role
Security Audit	FAU_GEN.1	The capability to configure the audit parameters shall be restricted to Master Users.
User Management	FIA_ATD.1	The capability to add and manage user accounts shall be restricted to users with the relevant User Permissions.
Security Roles	FMT_SMR.1	Subjects with the “Role Permissions: Modify” permission can change the requirements for performing operations in that role. Subjects with the relevant Role permissions can view, modify, create, and delete roles.
Certificate Status Change Approval	FDP_CSE_EXT.1	To revoke a certificate or place a certificate hold, the subject needs one of the following relevant permissions: To revoke a user certificate: User Permissions: Revoke certificates To revoke a subordinate CA certificate: Subordinate CA Permissions: Revoke. To revoke a cross-certified CA certificate, Cross-certified CA Permissions: Revoke To revoke a CA certificate, CA permissions: Revoke CA keys.
TSF Configuration	FMT_MTD1 FMT_SMF.1	Configuration settings which are only available via the command shell are restricted to Master Users. Remote operations that control TSF data require various permissions as defined in the Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide.
Certificate Profile Management	FMT_MOF_EXT.3	The capability to modify the certificate specifications remotely requires one of the following relevant Security Policy permissions: Import Certificate Specification, Modify User Policy, Create User Policy, Delete User Policy. The capability to modify the certificate specifications locally is restricted to Master Users.
Certificate Revocation List Profile Management	FMT_MOF_EXT.5	The capability to modify the certificate revocation list profile shall be restricted to Master Users and users with the View Security Policy and Modify Security Policy permissions.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [***TOE Access Control Policy specified in Section 8***] to restrict the ability to [**query, modify, delete**] the security attributes [***identity, role,***

groups, searchbase, certificate type] to [***administrative users with the relevant User Permissions***].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Management of security attributes

FMT_MSA.3.1 The TSF shall enforce the [***TOE Access Control Policy specified in Section 8***] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [***administrative users with the relevant User Permissions***] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [**query, modify, delete**] the [***TSF data identified in Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide***] to [***the permissions specified in Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide***].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [***functions listed in Table 14***].

FMT_SMR.2 Restrictions on security roles

Hierarchical to: FMT_SMR.1

Dependencies: No dependencies.

FMT_SMR.2.1 The TSF shall maintain the roles: [***Master User, administrator with sufficient permissions***].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [***no identity can assume more than one role at a time***
] are satisfied.

6.1.2.2 Access Control

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [***TOE Access Control Policy specified in Section 8***] on [

Subjects: all ECA users

Objects: user accounts

Operations: all operations among subjects and objects covered by the SFP

].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [***TOE Access Control Policy specified in Section 8***] to objects based on the following: [

Subject attributes: subject identity and the role that the subject is authorized to assume

Object attributes: role, groups, searchbase, certificate types

].

FDP_ACF.1.2 TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
The subject identity must be assigned a role that has the permission required to perform the operation and permission to administer each of the object's assigned attribute].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***Master User operations performed via the Control Command Shell command line utility***].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***].

6.1.3 Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of user security attributes belonging to individual users: [***user identifier, role, groups, searchbase, password for Master Users, certificate for all other users, certificate type***].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [***access to the login screen, help menu from the ECAA user interface, create or recover a profile using ECAA, Class 3 ECA Control Command Shell***[10]] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [***access to the login screen, help menu from the ECAA user interface, create or recover a profile using ECAA, Class 3 ECA Control Command Shell***[11]] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [***user identifier, role, group, searchbase, certificate type***].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***administrative users with the relevant User Permissions***].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users: [***administrative users with the relevant User Permissions***].

6.1.4 Remote Data Entry and Export

FCO_NRO_EXT.3 Enforced proof of origin and verification of origin

[10] See Entrust Certificate Authority 10.1, Operations Guide, Section F for a complete list of commands.
[11] See Entrust Certificate Authority 10.1, Operations Guide, Section F for a complete list of commands.

Hierarchical to: FCO_NRO.2

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO_EXT.3.1 The TSF shall enforce the generation of evidence of origin for certificate status information and all other security-relevant information at all times.

FCO_NRO_EXT.3.2 The TSF shall be able to relate the identity and [***no other attributes***] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

FCO_NRO_EXT.3.3 The TSF shall verify the evidence of origin of information for all security-relevant information.

FCS_CPT_EXT.1 Cryptographic Parameter Transfer

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_CPT_EXT.1.1 When using the CMP protocol, the TSF shall protect certificates, public keys, symmetric keys, and private keys from modification when transmitted between separate parts of the TOE.

FCS_CPT_EXT.1.2 When using the CMP protocol, the TSF shall protect certificates, public keys, symmetric keys, and private keys from modification when transmitted between the TOE and the PKI end-user application.

FCS_CPT_EXT.1.3 When using the CMP protocol, the TSF shall protect symmetric keys and private keys from disclosure when transmitted between separate parts of the TOE and between the TOE and the PKI end-user application.

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between ***ECA*** ~~itself~~ and another trusted IT product 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, another trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.2 The TSF shall initiate communication via the trusted channel for [***all write operations between ECA and the directory over LDAPS and all communications between ECA and end client over the XAP protocol***].

FCO_NRO_EXT.4 Advanced verification of origin

Hierarchical to: No other components.

Dependencies: FCO_NRO_EXT.3

FCO_NRO_EXT.4.1 The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using a keyed hash based on an authentication code.

FCO_NRO_EXT.4.2 The TSF shall, for initial certificate registration messages sent on behalf of the certificate subject, only accept messages protected using a digital signature of an authorized administrator.

6.1.4.1 Certificate Status Export

FDP_CSE_EXT.1 **Certificate status export**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_CSE_EXT.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3.

FDP_CSE_EXT.1.2 Certificate status information shall be exported from the TOE to an OCSP responder for the purpose of generating an OCSP response as specified in RFC 6960.

6.1.5 Key Management

6.1.5.1 Private Key Storage

FCS_CKM.1 **Cryptographic key generation**

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA, ECDSA, TDES and AES**] and specified cryptographic key sizes [

- **2048, 3072, 4096 and 6144 (RSA),**
- **P-256, P-384 (ECDSA),**
- **P-521 (ECDSA) (only available for X.509; not EAC / ePassport),**
- **192 bit (TDES), and**
- **128, 192, and 256 bit (AES)**

]

that meet the following: [**FIPS PUB 186-4 Appendix B (RSA and ECDSA), FIPS PUB 46-3 (TDES) and FIPS PUB 197 (AES)**].

FDP_ACF_EXT.2 **User private key confidentiality protection**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ACF_EXT.2.1 Administrator private keys shall be stored in a cryptographic module or stored in encrypted form. If Administrator private keys are stored in encrypted form, the encryption shall be performed by the cryptographic module.

FDP_ACF_EXT.2.2 If end entity private keys are stored in the TOE, they shall be encrypted. The encryption shall be performed by the cryptographic module.

FMT_MTD_EXT.4 TSF private key confidentiality protection

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_MTD_EXT.4.1 The CA private keys shall be stored in a cryptographic module or stored in encrypted form. If the CA private keys are stored in encrypted form, the encryption shall be performed by a cryptographic module.

FMT_MTD_EXT.4.2 The CA profile keys shall be stored in encrypted form in the CA database or stored in the local filesystem protected by the operational environment. If CA profile keys are stored in encrypted form, the encryption shall be performed by the cryptographic module.

6.1.5.2 Public Key Storage

FDP_SDI_EXT.3 Stored public key integrity monitoring and action

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_SDI_EXT.3.1 Public keys stored within the PKI, but not within a cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_EXT.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall [***return an error and audit the failure***].

6.1.5.3 Secret Key Storage

FCS_KDF_EXT.1 Cryptographic Key Derivation

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

FCS_KDF_EXT.1.1 The TSF shall utilize a password (or secret) and salt to derive an intermediate key, as defined in NIST SP 800-132 using keyed-hash functions, which is used to protect TSF data stored in the database.

FDP_ACF_EXT.3 User secret key confidentiality protection

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ACF_EXT.3.1 User secret keys stored within the TOE, but not within a cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the cryptographic module.

FMT_MTD_EXT.5 **TSF secret key confidentiality protection**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_MTD_EXT.5.1 TSF secret keys stored within the TOE, but not within a cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the cryptographic module.

6.1.5.4 Cryptographic Key Destruction

FCS_CKM.4 **Cryptographic key destruction**

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For plaintext keys in volatile storage, the destruction shall be executed by a single overwrite consisting of zeroes; or***
- ***For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that logically addresses the storage location of the key and performs a single, overwrite consisting of zeroes***]

that meets the following*:* [***No Standard***].

6.1.5.5 Private and Secret Key Export

FDP_ETC_EXT.5 **Extended user private and secret key export**

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_ETC_EXT.5.1 User private and secret keys shall only be exported from the TOE in encrypted form.

FMT_MTD_EXT.7 **Extended TSF private and secret key export**

Hierarchical to: No other components.

Dependencies: No dependencies

FMT_MTD_EXT.7.1 TSF private and secret keys shall only be exported from the TOE in encrypted form.

6.1.6 Certificate Profile Management

FMT_MOF_EXT.3 **Extended certificate profile management**

Hierarchical to: No other components.

Dependencies: FMT_MOF.1 Management of security functions behavior
FMT_SMR.1 Security roles

FMT_MOF_EXT.3.1 The TSF shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_EXT.3.2 The TSF shall require [**Master users or administrators with one of the following relevant Security Policy permissions: Import Certificate Specification, Modify User Policy, Create User Policy, Delete User Policy, Modify Role, Modify Security Policy**] to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;
- the length of time for which the certificate is valid;

FMT_MOF_EXT.3.3 If the certificates generated are X.509 public key certificates, the TSF shall require the [**Master users or administrators with one of the following relevant Security Policy permissions: Export Certificate Specification, Import Certificate Specification, Modify User Policy, Create User Policy, Delete User Policy, Modify Role, Modify Security Policy**] to specify the set of acceptable values for the following fields and extensions:

- `keyUsage`;
- `basicConstraints`;
- `certificatePolicies`

FMT_MOF_EXT.3.4 The Administrator shall specify the acceptable set of certificate extensions.

6.1.7 Certificate Revocation List Profile Management

FMT_MOF_EXT.5 **Extended certificate revocation list profile management**

Hierarchical to: No other components.

Dependencies: FMT_MOF.1 Management of security functions behavior
FMT_SMR.1 Security roles

FMT_MOF_EXT.5.1 If the TSF issues CRLs, the TSF must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.

FMT_MOF_EXT.5.2 If the TSF issues CRLs, the TSF shall require the [**Master Users or administrators with the View Security Policy and Modify Security Policy permissions**] to specify the set of acceptable values for the following fields and extensions:

- **`nextUpdate`** (i.e., lifetime of a CRL).

FMT_MOF_EXT.5.3 If the TSF issues CRLs, the [**Master Users**] shall specify the acceptable set of CRL and CRL entry extensions.

6.1.8 Certificate Generation

FDP_CER_EXT.1 **Certificate Generation**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_CER_EXT.1.1 The TSF shall only generate certificates whose format complies with [***the X.509 standard for public key certificates, ISO 7816 Card Verifiable (CV) certificates***].

FDP_CER_EXT.1.2 The TSF shall only generate certificates that are consistent with the currently defined certificate profile.

FDP_CER_EXT.1.3 Unless the certificate request is signed by an administrator, the TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FDP_CER_EXT.1.4 If the TSF generates X.509 public key certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that:

a) The **`version`** field shall contain the integer **0**, **1**, or **2**.

b) If the certificate contains an **`issuerUniqueID`** or **`subjectUniqueID`**, then the version field shall contain the integer **1** or **2**.

c) If the certificate contains extensions, then the `version` field shall contain the integer **2**.

d) The **`serialNumber`** shall be unique with respect to the issuing Certification Authority.

e) The `validity` field shall specify a **`notBefore`** value that is not preceded by the **`notAfter`** value.

f) The `issuer` field must contain a non-empty distinguished name (DN).

g) If the `subject` field contains a null **`Name`** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **`subjectAltName`** extension.

h) The `signature` field and the algorithm in the **`subjectPublicKeyInfo`** field shall contain the OID for an approved algorithm.

6.1.9 Certificate Revocation

FDP_CRL_EXT.1 **Certificate revocation list validation**

Hierarchical to: No other components.

Dependencies: No dependencies

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 TSF shall ensure that:

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) The **`issuer`** field must contain a non-empty distinguished name (DN).
d) The **`signature`** and **`signatureAlgorithm`** fields shall contain the OID for a claimed digital signature algorithm.
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.

6.1.10 Cryptographic Operations

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [***list of cryptographic operations – see Table 15***] in accordance with a specified cryptographic algorithm [***list of cryptographic algorithm – see Table 15****]* and cryptographic key sizes [***list of cryptographic key sizes – see Table 15***] that meet the following: [***list of standards – see Table 15***].

Table 15: Cryptographic Operations

Cryptographic Operation	Cryptographic Algorithm	Key Size	Cert #
Digital Signature Generation and Verification	RSA *FIPS PUB 186-4 Section 5*	Signature generation PKCS 1.5 mod 2048, 3072, 4096 Signature generation PKCSPSS mod 2048, 3072, 4096 Signature verification PKCS 1.5 mod2048, 3072 Signature verification PKCSPSS mod 2048, 3072	CAVP C605
		Signature verification PKCS 1.5 mod 4096 Signature verification PKCSPSS mod 4096	N/A
	ECDSA *FIPS PUB 186-4 Section 6*	Signature generation curves P-256, P-384, P-521 Signature verification curves P-256, P-384, P-521	CAVP C603
Key Generation	RSA Key Generation *FIPS PUB 186-4 Appendix B*	RSA 186-4 key generation mode B.3.6, mod 2048, 3072	CAVP C605
		RSA 186-4 key generation mode B.3.6, mod 4096	N/A
	ECDSA Key Generation *FIPS PUB 186-4 Appendix B*	ECDSA key generation curves P-256, P-384, P-521	CAVP C603
	TDES Key Generation	TDES key generation 192 bit	CAVP C606
	AES Key Generation	AES key generation 128, 192, 256 bit	CAVP C614

Cryptographic Operation	Cryptographic Algorithm	Key Size	Cert #
Block Ciphers	AES *FIPS PUB 197 (AES)* *NIST SP 800-38A* *NIST SP 800-38D* *NIST SP 800-38F*	AES-CBC encryption/decryption with key 128, 192, 256 bit AES-GCM encryption/decryption with key 128, 192, 256 bit	CAVP C614
	TDES *FIPS PUB 46-3 (DES)* *NISP SP 800-67 Rev2*	TDES-CBC	CAVP C606
Hash Functions	SHA *FIPS PUB 180-4*	SHA-1 message length 0-65536 bits (used in HMAC)[12] SHA-224 message length 0-65536 bits SHA-256 message length 0-65536 bits SHA-384 message length 0-65536 bits SHA-512 message length 0-65536 bits	CAVP C600
Keyed-hash Message Authentication Code (HMAC)	HMAC *FIPS PUB 180-4* *FIPS PUB 198-1*	HMAC-SHA-1 160 bits HMAC-SHA-224 224 bits HMAC-SHA-256 256 bits HMAC-SHA-384 384 bits HMAC-SHA-512 512 bits	CAVP C604
Random Bit Generation	DRBG *NIST SP 800-90A Rev1*	Hash DRBG SHA2-512 512 bits	CAVP C601
Key-based derivation functions (KDF)	PBKDF *RFC8018 PBKDF2 (SP800-132 PBKDF)*	HMAC-SHA-1 160 bits HMAC-SHA-224 224 bits HMAC-SHA-256 256 bits HMAC-SHA-384 384 bits HMAC-SHA-512 512 bits	CAVP A2106

[12] SHA-1 is used to support HMAC-SHA-1 which provides integrity services.

6.2 Security Assurance Requirements

This section specifies the assurance requirements for the TOE. Details of the assurance components specified in this section may be found in part 3 of the Common Criteria.

The following table provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.2: Flaw reporting procedures.

Table 16: Access Controls

Assurance Class	Component ID	Component Title
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3	Focused vulnerability analysis

7 TOE Summary Specification

This section describes the security functions provided by Entrust Certificate Authority and Entrust Certificate Authority Administration to meet the SFRs specified for the TOE in Section 6.1. Each security function described in this section contributes to meeting one or several SFRs.

7.1 Security Audit

7.1.1 Specification of auditable events and recorded information

The TOE does not provide the capability to start and stop the audit functions independently of the TOE operation. The audit function starts and stops whenever the ECA service starts and shuts down and these are auditable events so it is possible to determine from the audit trail whether audit was active in the particular timeframe. ECA also audits all of the events specified in Section B of [ECA Operations Guide], including security relevant events specified in the Table 13: Auditable Events and Audit Data.

Each audit event includes the following information: audit log number, date and time of event, node, event text (which includes the type of event and outcome), severity, administrator name, target name, audit state, extra text, and an integrity checksum.

This security function addresses the following SFR: FAU_GEN.1

7.1.2 Accountability of users

Each audit event is uniquely associated with the identity of the user who caused the event, as appropriate.

This security function addresses the following SFR: FAU_GEN.2

7.1.3 Audit review

The ECAA provides an interface to allow administrators to read the audit records stored in the ECA database. These audit records are presented in a human-readable format that allows the information to be interpreted.

This security function addresses the following SFR: FAU_SAR.1

7.1.4 Audit data selection

ECA always generates an audit entry for any auditable events but these audit entries are not by default externally published. Entrust Certificate Authority is capable of publishing audit entries based on a configuration setting; this configuration setting specifies the audit events to be published and those specific events that are not to be published. The values for the Publish and Exclude entries include: all, alarms, events, logs, audit_number and audit_range.

This security function addresses the following SFR: FAU_SEL.1

7.1.5 Audit Data Protection

ECA stores all audit entries in the database. A checksum is created for each of the audit events. The checksum detects any audit records that have been modified or added.

All audit events have a unique audit number.

Database access controls in the operating environment prevent audit records from being deleted, modified, or added by unauthorized users.

This security function addresses the following SFRs: FAU_STG_EXT.1,

7.1.6 Reliable Time Source

The TOE relies on the system clock of the host for a reliable time stamp. A date/time stamp is included and associated with each audit entry.

This security function addresses the following SFR: FPT_STM.1

7.2 Security Management

7.2.1 Roles

7.2.1.1 Role Definition

Every user in the ECA is assigned a role that controls what operations the user can perform and which user accounts that administrative user can operate on. A role is a set of permissions that defines what administrative tasks the role is able to perform. The TOE includes several pre-defined roles that can be used to administer the system or used to create custom roles. Administrative users are allowed to create custom roles to meet the needs of the organization.

Most permissions allow users assigned that role to perform a specific administrative operation, such as adding users to ECA. Other permissions specify the scope of an operation, such as the list of groups that users assigned that role can operate upon. Permissions are provided for each of the following categories (refer to the *Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide* for a list of all permissions):

- Audit Log
- Bulk Operations & Reports
- Certificates
- Certification Authority (CA)
- Directory
- Extended Access Control (CVCA)
- Extended Access Control (DV)
- Groups
- License Information
- Policy OIDs
- Queued Requests
- Roles
- Searchbase
- Security Policy
- User Templates
- Users

The TOE maintains Master Users and administrators with assigned roles/permissions. Master Users are highly trusted individuals responsible for installing and configuring ECA and for maintaining the certificates, database, and directory. Master Users use the Control Command Shell command line utility to manage ECA.

When a new user is created (with the exception of Master Users), the new user must be associated with a role. The End User role has no administrative permissions, and so cannot access the PKI via ECAA. No user may have more than one role.

Some conditions must hold in order for the role to be assigned to the user. A user can be associated with a given role only as explicitly assigned by an administrator with sufficient permissions over that role.

The three default Master Users can never be deleted. Custom Master User accounts can be created and deleted. A user cannot be disassociated from the Master User role.

The TSF has the ability to require multiple authorizations to perform sensitive operations, such as recovering a user account, and adding a user account. By default, the system does not require multiple authorizations to perform sensitive operations.

This security function, in conjunction with the Management of security functions behavior described in Section 7.2.2, addresses the following SFRs: FMT_MOF.1 and FMT_SMR.2

7.2.2 Management of security functions behavior

Each role provides access to a specific set of operations, including the ability to modify the behavior of the PKI system. Certain operations are only available to users with roles that have sufficient permissions to the user account being operated upon. Some role restrictions are described in Table 14: Authorized Roles for Management of Security Functions Behavior.

The TOE maintains a user identifier, one user role, one or more user groups, one searchbase, and a certificate type for each user. The security attributes associated with user accounts can only be viewed, modified or deleted by administrative users with the relevant User Permissions as provided by their user role. The administrative user creating a new user account must assign an identity. If the administrative user does not specify a role, groups, searchbase, and certificate type, default values for each of these security attributes are assigned to the user. The default role is the end user role. The default searchbase is the CA domain searchbase, and the default certificate type is the ent_default. The default groups assigned to the new user are based on the group memberships and permissions of the administrator creating the user.

In addition, the TOE restricts the ability to view, modify, and delete TSF data to users with roles assigned permissions as defined in the *Entrust Certificate Authority 10.1 Common Criteria Supplemental Guide*.

This security function, in conjunction with the security function Role Definition described in Section 7.2.1.1, addresses the following SFRs: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_MSA.1, and FMT_MSA.3.

7.2.3 Access Control

The TOE controls access to all ECA user accounts based on the permissions assigned to the role of the administrative user accessing the user account. . The permissions assigned to a role define the operations the administrative user with that role can perform and which user account security attributes that the administrative user can operate on. To perform an operation on a user account, the administrative user must be assigned a role that has the permission required to perform the operation as well as the permission to administer each of the security attributes (role, groups, searchbase, and certificate type) assigned to the user account.

Using the Control Command Shell command line utility, Master users have the authority to perform all operations on ECA user accounts that are available through that utility. Master users are not assigned permissions.

This security function addresses the following SFRs: FDP_ACC.1 and FDP_ACF.1

7.3 Identification and Authentication

The TOE maintains a user identifier, one user role, one or more user groups, one searchbase, password for Master Users, certificate(s) and certificate type for all other users.

This security function addresses the following SFRs: FIA_ATD.1

7.3.1 Authentication of users

The TOE does not allow the selection of any TOE-mediated function before the user is successfully authenticated. Master Users authenticate to the ECA with a password. All other administrative users authenticate using a certificate and the associated private keys. (The private keys and associated certificates comprise an Entrust profile which is stored on the user's token. The authentication required to access the user's keys/certificate is implemented by the token which is in the operational environment.) All functions require the user to be authenticated before allowing any TSF-mediated action.

For non-Master users to create/recover their profile, they must obtain a reference number and authorization code from a Master User or an Entrust administrator. The authorization code is used to authenticate the user prior to creating the Entrust profile.

This security function addresses the following SFR: FIA_UAU.1

7.3.2 Identification of users

The TOE does not allow selection of any TOE-mediated function before the user is successfully identified. All functions require the user to be identified before allowing any TSF-mediated action.

For non-Master users to create/recover their profile, they must obtain a reference number and authorization code from a Master User or an Entrust administrator. The reference number is used to identify the user prior to creating the Entrust profile.

This security function addresses the following SFR: FIA_UID.1

7.3.3 User-Subject Binding

The TOE associates the user identity with subjects acting on behalf of human users. The user identity is authenticated at login and remains associated with subjects acting on behalf of the human user as long as the login session is valid. The TOE also associates a role, one or more user groups, a searchbase, and a certificate type to each subject. Changes made to a user's role, user groups and searchbase take effect on the next requested operation.

This security function addresses the following SFR: FIA_USB.1

7.4 Remote Data Entry and Export

The TOE provides protected communication channels between itself and remote entities and between its own physically separate components. Protected transmissions are required for any key management and certificate management transactions (including certificate requests, key recovery and automatic key update of end user encryption key and signing key pairs) between the TOE and Client Applications.

Key management and certificate management transactions between the TOE and end user client applications are carried over CMP. Administrative transactions between the TOE and administrative client applications are carried over XAP.

Communications between the ECA and ECAA are transmitted using ASH or CMP. The operational environment provides a TLS v1.2 tunnel to protect communications using the ASH protocol between the ECA and ECAA.

ECA and ECAA communicate with the directory using LDAPS (LDAP over TLS). ECA communicates with the database using ODBC. Communications between the TOE and database are transmitted using ODBC secured with TLS which is provided by an ODBC driver in the operational environment.

7.4.1 Enforced Proof of Origin and Verification of Origin

The TOE generates and provides digital signatures on all certificates and CRLs. X.509 certificate requests and key updates are conducted through PKIX-CMP which enforces authentication as well as confidentiality and integrity protection.

The TOE verifies the digital signature on all certificates, CRLs and ARLs; PKIX-CMP enforces authentication and integrity verification for all certificate request and key update transactions.

This security function addresses the following SFR: FCO_NRO_EXT.3

7.4.2 TLS Implementations

Communications over XAP between ECA and administrative client systems are protected from disclosure and modification as all data is sent over TLS v1.2 implemented by the TOE. These communications are initiated by the client.

For services available to ECAA users that are implemented with the ASH protocol, all ASH communication is tunneled over TLS v1.2 which is provided by the operational environment. These services include administrative functions, user initialization, automatic key updates, key recovery services, and cross-certification establishment.

Certificate issuance functionality is conducted over the CMP protocol. See Section 7.4.4 for more information on protection of CMP.

Communications between ECA/ECAA and the directory are initiated by ECA/ECAA. All write operations are performed by the TOE using LDAPS (LDAP over TLS). Some read operations occur over LDAP because the data being retrieved is signed and considered public information.

Communications between ECA and the database are initiated by ECA and use ODBC over TLS, where TLS is implemented by the ODBC driver in the operational environment.

This security function addresses the following SFRs: FTP_ITC.1

7.4.3 Verification of Origin

Initial certificate registration messages sent by a certificate subject are only accepted by the TOE if the messages are protected using a keyed hash based on an authorization code (a shared secret). Initial certificate registration messages sent on behalf of the certificate subject are only accepted by the TOE if the messages are protected using a digital signature of an authorized administrator.

This security function addresses the following SFRs: FCO_NRO_EXT.4

7.4.4 Cryptographic Parameter Transfer

The TOE implements multiple protocols to transmit cryptographic parameters between ECA and ECAA and between the TOE and a remote trusted entity. Key management and certificate management transactions are carried over CMP. Communications between the ECA and ECAA are transmitted using ASH or CMP. Communications between the ECA and end client are transmitted over CMP.

The CMP protocol encrypts all private and secret keys transmitted between entities in order to protect the keys from unauthorized disclosure. The CMP protocol protects all keys and certificates from unauthorized modification when transmitted between entities using either digital signatures or keyed hash algorithms.

For new users and users performing a key recovery, users are identified with a reference number, and an authorization code serves as a shared secret to integrity-protect the messages. For other key management operations, the CMP messages are signed. CMP messages from a user client must be signed with their signing key. By default, CMP responses from the ECA to the client are signed with the

ECA CA's protocol signing keys. Administrators can configure ECA to sign the CMP responses from the ECA with the ECA CA's signing key, instead of the ECA CA's protocol signing keys.

This security function addresses the following SFRs: FCS_CPT_EXT.1

7.5 Certificate Management

7.5.1 Certificate Generation

The TOE generates certificates whose format complies with X.509 version 3 certificates. In EAC environments, the TOE also issues Card Verifiable (CV) certificates whose format complies with ISO 7816. All generated certificates must be consistent with the defined certificate specification.

For X.509 certificates, the TOE ensures that:

- **`SerialNumber`** is unique;
- **`notBefore`** is not preceded by the **`notAfter`** value;
- **`Issuer`** must contain a non-empty DN;
- If the `subject` field contains a null **`Name`** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **`subjectAltName`** extension

In addition, **`subjectPublicKeyInfo`** can be set to contain the OID for approved algorithms.

Proof of possession is established before a certificate can be made available to an end user, unless the certificate request is signed by an administrator. Proof of possession is established either when the end user includes the private key in the certificate request, or when ECA encrypts the certificate using the public key that was included in the certificate request.

This security function addresses the following SFR: FDP_CER_EXT.1

7.5.2 Certificate Status Export

ECA issues Certificate Revocation Lists (CRLs) in a format that complies with X.509 version 2 CRLs as specified in RFC 5280 Section 6.3. The TOE can also integrate with an OCSP (Online Certificate Status Protocol as specified in RFC 6960) responder for the purpose of generating an OCSP response. This integration involves replicating certificate revocation information from the ECA database to a database used by the OCSP responder.

This security function addresses the following SFR: FDP_CSE_EXT.1

7.5.3 Certificate Profile Management

The TOE implements flexible certificate definitions for X.509 certificates and ensures that issued certificates are consistent with that specification. It requires Master users or administrators with one of the following relevant Security Policy permissions: Import Certificate Specification, Modify User Policy, Create User Policy, Delete User Policy, Modify Role, Modify Security Policy to specify the set of acceptable values for:

- the key owner's identifier;
- the algorithm identifier for the subject's public/private key pair;
- the length of time for which the certificate is valid; and
- the **`keyUsage`**, **`basicConstraints`** and **`certificatePolicies`** attributes.

This security function addresses the following SFR: FMT_MOF_EXT.3

7.6 Certificate Revocation

7.6.1 CRL Profile Management

The TOE generates CRLs according to the ISO/ITU X.509 and IETF RFC 5280 specifications. The TOE specifies its own DN for the issuer and, by default, does not specify **`issuerAltName`**. Some values, such as **`nextUpdate`**, can be modified by a Master User. The TOE only allows Master Users or users with roles that are assigned the View Security Policy and Modify Security Policy permissions to specify the set of acceptable values for the i**`nextUpdate`** field. The TOE only allows Master Users to specify the set of acceptable values for CRL extensions and CRL entry extensions.

This security function addresses the following SFR: FMT_MOF_EXT.5

7.6.2 CRL Validation

The TOE only generates X.509 version 2 CRLs. The **`Issuer`** attribute is set to the CA's DN and never contains a null name.

- The **`Signature`** and **`signatureAlgorithm`** attributes can be set to contain the OID for algorithms claimed in FCS_COP.1.
- **`thisUpdate`** is set to the CRL issue time (UCT time)
- **`nextUpdate`** is set to the next CRL issue time (UCT time) and never precedes the time specified for the **`thisUpdate`** attribute

This security function addresses the following SFR: FDP_CRL_EXT.1

7.7 Key Management

7.7.1 Key Derivation

The TOE implements password-based key derivations functions (KDF) to derive cryptographic keys from passwords/secrets. The TSF uses a password/secret and salt to derive an intermediate key, as defined in NIST SP 800-132 using the HMAC-SHA-256 functions specified in FCS_COP.1.

The KDF is used to derive Master User Keys and to derive the keys used to protect the database.

This security function addresses the following SFR: FCS_KDF_EXT.1

7.7.2 Key Generation

All key material used within ECA is generated and used within the software-based cryptographic module (CM) specified in Section 1.4.5. The CM generates RSA, ECDSA, TDES, and AES keys according to standards and parameters listed in the Table 15: Cryptographic Operations. When integrated with an HSM, CA key generation is performed by the HSM. In this mode of operation, CA keys do not leave the HSM; from the TOE's point of view, key generation is performed in the operational environment. When an HSM is used, server-generated end entity keys are generated by the software-based CM.

This security function addresses the following SFR: FCS_CKM.1

7.7.3 Private Key Protection

All key material used within the TOE is generated by the CM within the TOE or by the HSM. Keys are exported only when suitably protected, such as when encrypted using approved techniques. The CA private keys are the CA signing keys used to sign certificates and certificate status information. The CA private keys are stored in the DB or in the HSM. The CA profile (public/private) keys are used for key agreement and trusted channel authentication.

When integrated with an HSM, CA private keys can be generated and stored on an HSM and the CA key protection is a function of the HSM. In this mode of operation, CA keys do not leave HSM; from the TOE's point of view, key protection is accomplished in the operational environment when an HSM is deployed.

The TSF secret keys are keys used to generate the symmetric keys that are then used to protect the TSF data in the DB, such as encrypting other secret or private keys. For enhanced protection, ECA can generate a key on an HSM and use that key to add an additional layer of encryption on the TSF secret keys stored in the DB.

User private keys are stored in the database in an encrypted form and only exported to end users over PKIX-CMP. Authorization codes are stored in the database in an encrypted form and exported over ASH or XAP.

Subject private keys that are used to generate digital signatures are not generated by ECA but by the subjects themselves. Subjects can also optionally generate their own private encryption keys using client software.

This security function addresses the following SFRs: FDP_ACF_EXT.2, FDP_ACF_EXT.3, FMT_MTD_EXT.4, FMT_MTD_EXT.5, FMT_MTD_EXT.7 and FDP_ETC_EXT.5

7.7.4 Public Key Protection

End-user public keys stored in the database by ECA are protected against unauthorized modification using a checksum. ECA checks the checksum on each element stored in the database each time that item is read. An error is returned to the calling function and an error is logged when verification is not successful.

ECA exports end-user public keys embedded in X.509v3 certificates. All certificates are digitally signed, which protects the exported public keys against unauthorized modifications.

This security function addresses the following SFR: FDP_SDI_EXT.3

7.7.5 Key Zeroization

The Cryptographic Module (CM) provides the capability to zeroize plaintext secret and private keys. The hardware security module (HSM) supported by ECA also provides a capability to zeroize plaintext secret and private keys.

The destruction of plaintext keys in volatile storage is executed by a single overwrite consisting of zeroes. The destruction of plaintext keys in non-volatile storage is executed by the invocation of an interface provided by a part of the TSF that logically addresses the storage location of the key and performs a single overwrite consisting of zeroes.

This security function addresses the following SFR: FCS_CKM.4

7.7.6 Cryptographic Operations

All cryptographic operations, except PBKDF2, are performed within the Cryptographic Module, Entrust Authority Security Kernel, a multi-chip standalone FIPS 140-2 Level 2 validated (CMVP 3981) software-based module. The PBKDF2 implementation has been issued an algorithm certificate. The supported

cryptographic operations include encryption and decryption, digital signature generation and verification, hashing, random number generation, and keyed-hash message authentication code (HMAC) generation and verification. These operations are performed in accordance with the following standards:

Table 17: Cryptographic Operations and Usage

Cryptographic Operation	Standard	Usage
Encryption/decryption	FIPS PUB 197(AES)	Encrypt keys, secrets, and other sensitive information stored in the DB Encrypt packages transmitted over HTTPS/LDAPS protocol. The PKIX-CMP protocol encrypts all private and secret keys transmitted between entities.
	FIPS PUB 46-3 (TDES)	Encrypt keys, secrets, and other sensitive information stored in the DB. The PKIX-CMP protocol encrypts all private and secret keys transmitted between entities.
Signature generation/verification	FIPS PUB 186-4 (ECDSA and RSA);	Sign/verify certificate contents to create/verify X.509 certificates Sign/verify certificate contents to create/verify ISO 7816 (ePassport EAC) certificates Sign/verify CRLs and ARLs Sign/verify certificate registration messages Certificate-based authentication Protect PKIX-CMP, TLS/HTTPS protocol communications. Verify XAP requests
Key Generation	RSA Key Generation ECDSA Key Generation FIPS PUB 186-4 Appendix B	Generate a CA signing key pair when an HSM is not used Generate TSF key pairs Generate end-entity key pairs
	TDES Key Generation AES Key Generation	Generate TLS session keys Generate CMP session keys

Cryptographic Operation	Standard	Usage
Hashing	FIPS PUB 180-4 (SHA)	Certificate-based authentication Digital signature generation/verification Certificate fingerprints
Keyed-hash Message Authentication Code (HMAC)	FIPS PUB 180-4, FIPS PUB 198-1	Prevent unauthorized modification of data in PKIX-CMP Protocol Authenticate incoming PKIX-CMP enrollment/recovery requests Software integrity checksum
Random Bit Generation	NIST SP 800-90A Rev 1	Key generation
Key-based derivation functions (KDF)	PBKDF RFC8018 PBKDF2 (SP800-132 PBKDF)	Derive a key from the Master User password

ECA also optionally supports the use of a hardware security module (HSM) for X.509 CA key generation and storage, CVCA key generation and storage, DV key generation and storage, signing of certificates, and signing of CRLs. ECA also supports the use of an HSM for the database encryption, although HSM database encryption is not used by default. For the purpose of this evaluation, the HSM is part of the operational environment.

This security function addresses the following SFR: FCS_COP.1 and FCS_CKM.1.

8 TOE Access Control Policy

This TOE Access Control Policy is referenced from a number of SFRs including FDP_ACF.1.1 and FMT_MSA.3 and is required to complete the specification of those SFRs.

The TOE shall support the administration and enforcement of a PKI TOE access control policy that provides the capabilities described below.

Subjects (human users) will be granted access to objects (data/files) based upon the:

1. Identity of the subject requesting access,
2. Role (or roles) the subject is authorized to assume,
3. Type of access requested,
4. Content of the access request, and,
5. Possession of a secret or private key, if required.

Subject identification includes:

- Unique identifier
- Authentication data
- A role assigned to a user

All permissions essentially refer to the following access types, with explicit allow or deny:

- Read
- Write
- Execute

The assignment and management of permissions will be the responsibility of the role(s) with the Role Permissions required to make changes.

9 Rationale

9.1 Conformance Claims Rationale

This ST does not contain a Conformance claim rationale.

9.2 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, policies, or assumptions.

9.2.1 Tracing Between Security Objectives and Security Problem Definition

The following tables provide a mapping of security objectives to the environment defined by the assumptions, threats and policies, illustrating that each security objective covers at least one assumption, threat or policy and that each assumption, threat and policy is covered by at least one security objective.

Table 18: Mapping Security Objectives to Assumptions

Assumptions / **Security Objectives**	A.Competent Administrators	A.Operating System	A.Physical Protection	A.Administrators Review Audit Logs	A.CPS	A.Authentication Data Management	A.Tunnel
OE.Installation	X						
OE.Operating System		X					
OE.Physical protection			X				
OE.Sufficient backup storage and effective restoration	X						
OE.Control unknown source communication traffic						X	
OE.Administrative user guidance documentation	X				X		
OE.Administrators review audit logs				X			
OE.User authorization management						X	
OE.Tunnel							X

Table 19: Mapping Security Objectives to OSP

OSP / Security Objectives	P.Authorized use of information	P.Cryptography
OE.User authorization management	X	
O.Cryptographic functions		X
O.Maintain user attributes	X	
O.Security-relevant configuration management	X	
O.Security roles	X	

Table 20: Mapping Security Objectives to Threats

Threats / Security Objectives	T.Administrators commit errors or hostile actions	T.User abuses authorization to collect and/or send data	T.Critical system component fails	T.Message content modification	T.Disclosure of private and secret keys	T.Modification of private keys	T.Hacker gains access	T.Social engineering
OE.Installation			X					
OE.Operating System			X					
OE.Physical protection					X	X		
OE.Sufficient backup storage and effective restoration	X		X					
OE.Control unknown source communication traffic							X	
OE.Administrative guidance documentation								X
OE.Administrators review audit logs	X	X	X			X	X	

Threats / Security Objectives	T.Administrators commit errors or hostile actions	T.User abuses authorization to collect and/or send data	T.Critical system component fails	T.Message content modification	T.Disclosure of private and secret keys	T.Modification of private keys	T.Hacker gains access	T.Social engineering
OE.User authorization management		X			X	X	X	
O.Certificates	X			X				X
O.Cryptographic functions				X	X	X		
O.Non-repudiation	X	X						
O.Data import/export				X			X	
O.Individual accountability and audit records	X	X			X		X	
O.Integrity protection of user data and software						X		
O.Limitation of administrative access	X	X			X			X
O.Maintain user attributes	X							
O.Manage behavior of security functions	X							
O.Protect stored audit records	X					X		
O.Protect user and TSF data during internal transfer				X	X	X	X	
O.Restrict actions before authentication	X							
O.Security-relevant configuration management	X							
O.Security roles		X						
O.Time stamps	X							
OE.Tunnel				X				

9.2.2 Security Objectives Sufficiency

The following discussions provide information regarding:

- Why the identified security objectives provide for effective countermeasures to the threats;
- Why the identified security objectives provide complete coverage of each organizational security policy;
- Why the identified security objectives uphold each assumption.

9.2.2.1 Threats and Objectives Sufficiency

Table 21: Threats by Authorized Users

Threat	Countered by
T.Administrators commit errors or hostile actions • An administrative user commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.	OE.Sufficient backup storage and effective restoration Ensures that there is sufficient backup storage and effective restoration to recreate the data. This ensures that data is available from backup, even if the current copy is lost through failure of a system component (e.g., a disk drive failure) or user error (e.g. rm -rf).
	OE.Administrators Review Audit Logs Ensures that security-relevant events recorded in audit logs are reviewed by Administrators to detect security violations.
	O.Certificates Ensures that certificates, certificate revocation lists, and certificate status information are valid. The validation of information provided by Officers that is to be included in certificates helps to prevent improperly entered information from appearing in certificates.
	O.Non-repudiation Prevents a user from avoiding accountability for their actions.
	O.Individual accountability and audit records Provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. These audit records will expose administrators that perform inappropriate operations so they can be held accountable.
	O.Limitation of administrative access The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific. Limiting the set of operations that a user may perform limits the damage that a user may cause.
	O.Maintain user attributes Maintains a set of security attributes (which may include group membership, access rights, etc.) associated with individual users in addition to user identity. This prevents users from performing operations that they are not authorized to perform.
	O.Manage behavior of security functions Provides management controls/functions for security mechanisms. This ensures that security mechanisms which protect against hostile users are properly configured.

Threat	Countered by
	O.Protect stored audit records Ensures that audit records are protected against unauthorized access or modification to provide and maintain for traceability of user actions.
	O.Restrict actions before authentication Ensures that only a limited set of actions may be performed before a user is authenticated.
	O.Security-relevant configuration management Manages and updates system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
	O.Time stamps Ensures that time stamps are provided to verify a sequence of events. This allows the reconstruction of a timeline of events when performing an audit review.
T.User abuses authorization to collect and/or send data User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.	OE.Administrators Review Audit Logs Ensures that security-relevant events recorded in audit logs are reviewed by Administrators.
	OE.User authorization management Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.
	O.Non-repudiation Prevents a user from avoiding accountability for their actions.
	O.Individual accountability and audit records Provides individual accountability for management actions. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This audit records will expose users who failed to act or abuse their privileges to collect and/or send data.
	O.Limitation of administrative access Design administrative functions so that all roles do not automatically have access to all security management functions.
	O.Security Roles Security-relevant roles are maintained and associated with users to limit the capabilities of each user, reducing the risk of a user improperly accessing sensitive or security-critical data.

Table 22: System-level Threats

Threat	Countered by
T.Critical system component fails Failure of one or more system components results in the loss of system critical functionality.	OE.Installation Ensures that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security. This ensures that critical system components do not fail as a result of improper installation.

Threat	Countered by
	OE.Operating System The operating system used is hardened to provide adequate security, including identification and authentication, process isolation and separation, reliable time stamps, file system access controls, enforcement of a TLS tunnel for ASH protocol communications.
	OE.Sufficient backup storage and effective restoration Ensures that there is sufficient backup storage and effective restoration to recreate the data. This ensures that data is available from backup, even if the current copy is lost through failure of a system component (e.g., a disk drive failure) or user error (e.g. rm -rf).
	OE.Administrators Review Audit Logs Ensures that security-relevant events recorded in audit logs are reviewed by Administrators.
T.Message content modification A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.	O.Certificates Certificates are used for authentication and messages are signed to prevent undetected modification.
	O.Cryptographic functions Strong cryptography protects data when being transmitted to or from the TOE. Protection of data in transit permits the TOE or the external user to detect modified messages, message replay, or unauthorized messages.
	O.Data import/export Protect keys and certificates when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
	O.Protect user and TSF data during internal transfer Protects data being transmitted between separated parts of the TOE using CMP. Protection of data in transit permits the TOE to detect modified messages, message replay, or fraudulent messages.
	OE.Tunnel ASH protocol communications between ECA and ECAA will be protected from modification and disclosure using a TLS v1.2 tunnel provided by the operational environment. ODBC protocol communications between ECA and the database will be protected from modification and disclosure using a TLS v1.2 tunnel provided by the ODBC driver in the operational environment.

Table 23: Cryptographic Threats

Threat	Countered by
T.Disclosure of private and secret keys A private or secret key is improperly disclosed. The threat agent is an authorized user or erroneous protocol. An adverse action can be compromise of the security of the PKI and/or relying party systems that rely on PKI objects such as certificates or CRLs.	OE.Physical Protection Physical protection ensures that the TOE;s components, including private and secret keys are not available via physical access.
	OE.User authorization management Ensures that user authorization and privilege data are consistent with organizational security and personnel policies.
	O.Cryptographic functions Ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, signature generation/verification; and key generation techniques. The TSF uses hardened cryptographic modules. Use of hardened cryptographic modules ensures that cryptographic keys are adequately protected when they are stored within cryptographic modules.

Threat	Countered by
	O.Individual accountability and audit records Provides individual accountability for audited events. Audit records provide information on access to private and secret keys. These audit records will expose potential disclosure of private and secret keys.
	O.Limitation of administrative access The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific. Limiting the number of users who have access to cryptographic keys reduces the likelihood of unauthorized disclosure.
	O.Protect user and TSF data during internal transfer Protects private and secret keys from unauthorized disclosure during transmission between separated parts of the TOE using CMP.
T.Modification of private/secret keys A secret/private key is modified. The threat agent is an authorized user or erroneous protocol. An adverse action can be compromise of the security of the PKI and/or relying party systems that rely on PKI objects such as certificates or CRLs.	OE.Physical Protection Physical protection ensures that the TOE's components, including private and secret keys are not available via physical access.
	OE.User authorization management Ensures that user authorization and privilege data are consistent with organizational security and personnel policies. This includes ensuring that unauthorized users do not have access to secret or private keys.
	OE.Administrators Review Audit Logs Modification of private and secret keys is logged, ensuring that such actions will be detected when logs are reviewed.
	O.Cryptographic functions Ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, signature generation/verification, and key generation techniques. The TSF uses hardened cryptographic modules. Use of hardened cryptographic modules ensures that cryptographic keys are adequately protected when they are stored within cryptographic modules.
	O.Integrity protection of user data and software Provide appropriate integrity protection using checksums for user data and software.
	O.Protect stored audit records Ensures that audit records are protected against unauthorized modification to provide for traceability of user actions. This objective ensures that modifications to private and secret keys can be detected through the audit trail.
	O.Protect user and TSF data during internal transfer Protects private and secret keys from unauthorized modification during transmission between separated parts of the TOE using CMP.
	OE.Tunnel ASH protocol communications between the ECA and ECAA will be protected from modification and disclosure using a TLS v1.2 tunnel provided by the operational environment. ODBC protocol communications between ECA and the database will be protected from modification and disclosure using a TLS v1.2 tunnel provided by the ODBC driver in the operational environment.

Table 24: Threat of External Attack

Threat	Countered by
T.Hacker gains access A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.	OE.Control unknown source communication traffic Ensures that attempts to communicate with the TOE are made by known sources. Various kinds of hacker attacks can be detected or prevented by rerouting or discarding suspected illegitimate traffic.
	OE.Administrators Review Audit Logs All attempts to access to the TOE is logged, ensuring that such actions will be detected when logs are reviewed.
	OE.User authorization management Ensures that user authorization and privilege data are consistent with organizational security and personnel policies.
	O.Data import/export Protect keys and certificates when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
	O.Individual accountability and audit records Provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This allows for the detection of unauthorized activity. Once detected, the further damage resulting from such activity can be eliminated or mitigated.
	O.Protect user and TSF data during internal transfer Ensure the integrity of user and TSF data transferred internally within the system over CMP, minimizing opportunities for passive eavesdropping.
	OE.Administrative guidance documentation Providing adequate guidance deters and limits errors by administrators.
	O.Certificates Certificates are used for definitive authentication to prevent impersonation.
	O.Limitation of administrative access The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. By limiting the number of users who have access to specific management functionality reduces the likelihood of successful social engineering attack.

9.2.2.2 Policies and Objectives Sufficiency

Table 25: Policies Supported by Objectives

Policy	Supported by
P.Authorized use of information Information shall be used only for its authorized purpose(s).	OE.User authorization management Ensures user authorization and privilege data is managed and updated to ensure they are consistent with organizational policies.
	O.Maintain user attributes Maintains a set of security attributes (role and access control permissions) associated with users that prevent users from performing operations that they are not authorized to perform.

Policy	Supported by
	O.Security roles Ensures that security-relevant roles are specified and that users are assigned to one (or more) of the defined roles. This prevents users from performing operations that they are not authorized to perform.
	O.Security-relevant configuration management Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
P.Cryptography The TSF shall exclusively rely on verified cryptographic primitives to perform all cryptographic operations.	O.Cryptographic functions Ensures that approved cryptographic standards for encryption/decryption, authentication, authentication, signature generation/verification algorithms, and key generation techniques are followed and only strong cryptography is used.

9.2.2.3 Assumptions and Objectives Sufficiency

Table 26: Personnel Assumptions Supported by Objectives

Assumption	Supported by
A.Administrators Review Audit Logs Audit logs are required for security-relevant events and must be reviewed by the Administrators.	OE.Administrators Review Audit Logs Ensures that security-relevant events recorded in audit logs are reviewed by Administrators.
A.Authentication Data Management An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)	OE.Control unknown source communication traffic The operational environment must control (e.g. reroute or discard) communication traffic from an unknown sources to protect authentication functionality.
	OE.User authorization management Ensures that user authorization and privilege data are consistent with organizational security and personnel policies.
A.Competent Administrators Competent administrative users will be assigned to manage the TOE and the security of the information it contains.	OE.Installation Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.
	OE.Sufficient backup storage and effective restoration Provides sufficient backup storage and effective recovery procedures to ensure that the system can be recreated.
	OE.Administrative guidance documentation Deters administrative user errors by providing adequate documentation on securely configuring and operating the TOE.
A.CPS All administrative users are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.	OE.Administrative guidance documentation Provides administrative users with adequate documentation on securely configuring and operating the TOE, which includes the CP and CPS.

Table 27: Connectivity Assumptions Supported by Objectives

Assumption	Supported by
A.Operating System The operating system has been selected to provide the following functions required by this PKI to counter the perceived threats as identified in this ST: identification and authentication, process isolation and separation, reliable time stamps, file system access controls, enforcement of a TLS tunnel for ASH protocol communications.	OE.Operating System Ensures that the operating system used is hardened to provide adequate security, including identification and authentication, process isolation and separation, reliable time stamps, file system access controls, enforcement of a TLS tunnel for ASH protocol communications.
A.Tunnel The operational environment will protect the ASH protocol communications between ECA and ECAA from modification and disclosure. The operational environment will also protect the ODBC communications between ECA and the database from modification and disclosure.	OE.Tunnel Ensures that the operating environment protects ASH protocol communications between ECA and ECAA from modification and disclosure using a TLS v1.2 tunnel. Ensures that the operating environment protects ODBC protocol communications between ECA and the database from modification and disclosure using a TLS v1.2 tunnel provided by the ODBC driver.

Table 28: Physical Assumptions Supported by Objectives

Assumption	Supported by
A.Physical Protection The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical access.	OE.Physical Protection Ensures that adequate physical protection will be provided to protect the TOE from a physical attack.

9.3 Security Requirements Rationale

This section provides the rationale for necessity and sufficiency of security requirements, demonstrating that each of the SOs for the TOE is addressed by at least one security requirement, and that every security requirement is directed toward solving at least one objective.

9.3.1 Security Requirements Coverage

The following tables provide a mapping of the relationships of security requirements to objectives, illustrating that each security requirement covers at least one objective and that each objective for the TOE is covered by at least one security requirement.

Table 29: Mapping SFRs to Security Objectives

Security Objective / SFR	O.Certificates	O.Cryptographic functions	O.Non-repudiation	O.Data import/export	O.Individual accountability and audit records	O.Integrity protection of user data and software	O.Limitation of administrative access	O.Maintain user attributes	O.Manage behavior of security functions	O.Protect stored audit records	O.Protect user and TSF data during internal transfer	O.Restrict actions before authentication	O.Security-relevant configuration management	O.Security roles	O.Time stamps
FAU_GEN.1					X										
FAU_GEN.2					X										
FAU_SAR1					X										
FAU_SEL.1					X										
FAU_STG_EXT.1										X					
FCO_NRO_EXT.3			X												
FCO_NRO_EXT.4			X												
FCS_CKM.1		X													
FCS_CKM.4		X													
FCS_COP.1		X													
FCS_CPT_EXT.1				X		X					X				
FCS_KDF_EXT.1		X													
FDP_ACC.1							X								
FDP_ACF.1							X								
FDP_ACF_EXT.2	X														
FDP_ACF_EXT.3	X														
FDP_CER_EXT.1	X														
FDP_CRL_EXT.1	X														
FDP_CSE_EXT.1	X														
FDP_ETC_EXT.5				X											
FDP_SDI_EXT.3						X									

Security Objective SFR	O.Certificates	O.Cryptographic functions	O.Non-repudiation	O.Data import/export	O.Individual accountability and audit records	O.Integrity protection of user data and software	O.Limitation of administrative access	O.Maintain user attributes	O.Manage behavior of security functions	O.Protect stored audit records	O.Protect user and TSF data during internal transfer	O.Restrict actions before authentication	O.Security-relevant configuration management	O.Security roles	O.Time stamps
FIA_ATD.1	X							X							
FIA_UAU.1							X					X			
FIA_UID.1					X		X								
FIA_USB.1								X							
FMT_MOF.1								X	X				X	X	
FMT_MOF_EXT.3	X														
FMT_MOF_EXT.5	X														
FMT_MSA.1									X						
FMT_MSA.3									X						
FMT_MTD.1									X						
FMT_MTD_EXT.4						X									
FMT_MTD_EXT.5						X									
FMT_MTD_EXT.7				X											
FMT_SMF.1								X	X				X	X	
FMT_SMR.2														X	
FPT_STM.1					X										X
FTP_ITC.1				X							X				

9.3.2 Security Requirements Sufficiency

Table 30: Rationale for SFRs Supporting Security Objectives

Objective	Supporting SFRs
O.Certificates The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid and up to date.	**FDP_CER_EXT.1 (Certificate Generation)** which ensures that certificates generated by the TSF are valid.
	FDP_CRL_EXT.1 (Certificate revocation list validation) ensures that certificate revocation lists and certificate status information are valid.
	FDP_CSE_EXT.1 (Certificate status export) ensures that certificate revocation lists can be exported from the TOE as CRLs or exported to an OCSP responder to generate an OCSP response.
	FDP_ACF_EXT.2 (User private key confidentiality protection) ensures that the user private keys are stored in a protected manner so that the certificate is not invalidated by the disclosure of the private key by the TOE.
	FDP_ACF_EXT.3 (User secret key confidentiality protection) ensures that user secret keys are stored in encrypted form in the TOE.
	FMT_MOF_EXT.3 Extended certificate profile management ensures that certificates contain the correct information as specified in the certificate profile and as per administrator-defined settings.
	FMT_MOF_EXT.5 Extended certificate revocation list profile management ensures that TOE-generated CRLs contain the correct information as specified in the CRL profile and as per administrator-defined settings.
O.Cryptographic functions The TSF must implement all cryptographic functionality underpinned by the approved cryptographic standards for encryption/decryption, authentication, signature generation/verification algorithms, and key generation techniques. The TSF must use hardened cryptographic modules.	**FCS_CKM.1 (Cryptographic key generation)** and **FCS_COP.1 (Cryptographic operations)** ensure that approved algorithms be used for encryption/decryption, authentication, signature generation/verification, and that key generation techniques be used.
	FCS_KDF_EXT.1 (Cryptographic Key Derivation) ensures that password-based (or secret-based) key derivation operations comply with NIST SP 800-132.
	FCS_CKM.4 (Cryptographic key destruction) covers the requirement that cryptographic keys that are no longer used be destroyed.
O.Non-repudiation Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.	**FCO_NRO_EXT.3 (Enforced proof of origin and verification of origin)** covers the requirement that messages containing security-relevant data are not accepted by the TOE unless they contain evidence of origin
	FCO_NRO_EXT.4 (Advanced verification of origin) covers the requirement that digital signatures be used so that the evidence of origin for a message may be verified by a third-party.
O.Data import/export Protect keys and certificates when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.	**FCS_CPT_EXT.1 (Cryptographic Parameter Transfer)**covers the requirement that keys and certificates be protected when they are transmitted between the TOE and PKI end-user applications..
	FDP_ETC_EXT.5 (Extended user private and secret key export) and **FMT_MTD_EXT.7 (Extended TSF private and secret key export)** cover the requirement that private and secret keys for both users and the TSF be protected when they are transmitted to and from the TOE by requiring private and secret keys to be exported in either encrypted form.

Objective	Supporting SFRs
	FTP_ITC.1 (Inter-TSF trusted channel) covers the requirement that keys and certificates be protected when transmitted to and from the TOE by requiring a trusted channel for write operations between the ECA and the directory and for all operations between the ECA and administrative end user client.
O.Individual accountability and audit records Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.	**FIA_UID.1 (Timing of identification)** covers the requirement that users be identified before performing any security-relevant operations which allows their identify to be audited.
	FAU_GEN.1 (Audit data generation) and **FAU_SEL.1 (Selective audit)** cover the requirement that security-relevant events be audited
	FAU_GEN.2 (User identity association) **FPT_STM.1 (Reliable time stamps)** cover the requirement that the date and time of audited events are recorded in the audit records along with the identities of the entities responsible for the actions.
	FAU_SAR.1 (Audit review) covers the requirement by ensuring administrators can review the audit trail to hold individuals accountable for their actions.
O.Integrity protection of user data and software Provide appropriate integrity protection using checksums for user data and software.	**FCS_CPT_EXT.1 (Cryptographic Parameter Transfer)**covers the requirement that keys and certificates be protected from unauthorized modification when transmitted between physically separate parts of the TOE. **FDP_SDI_EXT.3 (Stored public key integrity monitoring and action)** cover the requirement that public keys stored in the PKI be protected against undetected modification.
	FMT_MTD_EXT.4 (TSF private key confidentiality protection) and **FMT_MTD_EXT.5 (TSF secret key confidentiality protection)** are required to protect the confidentiality of the TSF private and secret keys used to protect the data and software since data and software are protected using cryptography.
O.Limitation of administrative access Design administrative functions so that administrative users do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Administrators who troubleshoot the system and perform system updates.	**FIA_UAU.1 (Timing of authentication)** and **FIA_UID.1 (Timing of identification)** ensure that administrative users cannot perform any security-relevant operations until they have been identified and authenticated.
	FDP_ACC.1 (Subset access control) and **FDP_ACF.1 (Security attribute based access control)** ensure that Administrators, Officers, and Auditors can only perform those operations necessary to perform their jobs.
O.Maintain user attributes Maintain a set of security attributes (which may include role membership. access permissions, etc.) associated with individual users. This is in addition to user identity.	**FIA_ATD.1.1 (User attribute definition)** and **FIA_USB.1 (User-subject binding) which** cover the requirement to maintain a set of security attributes associated with individual users and/or subjects acting on users' behaves.
	FIA_USB.1 (User subject binding) ensures that the TSF associates user security attributes with subjects.
	FMT_MOF.1 (Management of security functions behavior) covers this objective by identifying the roles that can maintain user security attributes.

Objective	Supporting SFRs
	FMT_SMF.1 (Specification of management functions) ensures that the TSF provides the management functions necessary to maintain user security attributes.
O.Manage behavior of security functions Provide management functions to configure, operate, and maintain the security mechanisms.	**FMT_MOF.1 (Management of security functions behavior)** covers the objective by defining the functions whose behavior can be modified and what roles can modify that behavior..
	FMT_MSA.1 (Management of security attributes) covers the objective by defining the policy for who can read and modify security attributes.
	FMT_MSA.3 (Static attribute initialisation) covers the objective by defining the policy for who can set the default values for security attributes used to enforce the security policy.
	FMT_MTD.1 (Management of TSF data) covers this objective by defining which roles can access the TSF data.
	FMT_SMF.1 (Specification of management functions) ensures that the TSF provides the management functions necessary to administer a CA and RA.
O.Protect stored audit records Protect audit records against unauthorized access or modification to ensure accountability of user actions.	**FAU_STG_EXT.1 (Audit trail storage integrity)** covers the objective that audit records be protected against unauthorized modification.
O.Protect user and TSF data during internal transfer Ensure the integrity and confidentiality of user and TSF data transferred internally within the system using CMP.	**FCS_CPT_EXT.1 (Cryptographic Parameter Transfer)** covers the requirement that all keys and certificates be protected during internal transfer.
O.Restrict actions before authentication Restrict the actions a user may perform before the TOE authenticates the identity of the user.	**FIA_UAU.1 (Timing of authentication)** covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.
O.Security-relevant configuration management Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.	**FMT_MOF.1 (Management of security functions behavior)** ensures that security-relevant configuration data can only be modified by those who are authorized to do so.
O.Security roles	**FMT_SMR.2 (Restrictions on security roles)** ensures that a set of security roles be maintained and that users be associated with those roles.

Objective	Supporting SFRs
Maintain security-relevant roles and the association of users with those roles.	**FMT_MOF.1 (Management of security functions behavior)** and **FMT_SMF.1 (Specification of management functions)** cover this requirement be ensuring that the TSF provides a mechanism for assigning roles to users.
O.Time stamps Provide time stamps to ensure that the sequencing of events can be verified.	**FPT_STM.1 (Reliable time stamps)** covers the requirement that the time stamps be reliable.

9.3.3 Security Requirements Dependencies

The following table demonstrates that the dependencies for all of the SFRs specified in section 6.1 of this ST are met directly by this ST.

Table 31: SFR Dependencies

SFR	Dependencies	Dependency Coverage in ST
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	FPT_STM.1 Reliable time stamps
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation
	FIA_UAU.1 Timing of authentication	FIA_UAU.1 Timing of authentication
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 Management of TSF data
FAU_STG_EXT.1 Audit trail storage integrity	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation
FCO_NRO_EXT.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	FIA_UID.1 Timing of identification
FCO_NRO_EXT.4 Advanced verification of origin	FCO_NRO_EXT.3 Enforced proof of origin and verification of origin	FCO_NRO_EXT.3 Enforced proof of origin and verification of origin
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution OR FCS_COP.1 Cryptographic operation	FCS_COP.1 Cryptographic operation
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Cryptographic key destruction
FCS_CKM.4 Cryptographic key destruction	FDP_ITC1 Import of user data without security attributes OR FDP_ITC.2 Import of user data with security attributes OR FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Cryptographic key generation
FCS_COP.1 Cryptographic operation	FDP_ITC1 Import of user data without security attributes OR FDP_ITC.2 Import of user data with security attributes OR FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Cryptographic key generation

SFR	Dependencies	Dependency Coverage in ST
	FCS_CKM.4 Cryptographic key destruction	FCS_CKM.4 Cryptographic key destruction
FCS_CPT_EXT.1 Cryptographic Parameter Transfer	No dependencies	Not applicable
FCS_KDF_EXT.1 Cryptographic key derivation	FCS_COP.1 Cryptographic operation	FCS_COP.1 Cryptographic operation
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 Security attribute based access control
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	FDP_ACC.1 Subset access control
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 Static attribute initialization
FDP_ACF_EXT.2 User private key confidentiality protection	No dependencies	Not applicable
FDP_ACF_EXT.3 User secret key confidentiality protection	No dependencies	Not applicable
FDP_CER_EXT.1 Certificate Generation	No dependencies	Not applicable
FDP_CRL_EXT.1 Certificate revocation list validation	No dependencies	Not applicable
FDP_CSE_EXT.1 Certificate status export	No dependencies	Not applicable
FDP_ETC_EXT.5 Extended user private and secret key export	No dependencies	Not applicable
FDP_SDI_EXT.3 Stored public key integrity monitoring and action	No dependencies	Not applicable
FIA_ATD.1 User attribute definition	No dependencies	Not applicable
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	FIA_UID.1 Timing of identification
FIA_UID.1 Timing of identification	No dependencies	Not applicable
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	FIA_ATD.1 User attribute definition
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security Roles	FMT_SMR.2 Restrictions on security roles
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 Specification of Management Functions
FMT_MOF_EXT.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 Management of security functions behavior
	FMT_SMR.1 Security roles	FMT_SMR.2 Restrictions on security roles
FMT_MOF_EXT.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	FMT_MOF.1 Management of security functions behavior
	FMT_SMR.1 Security roles	FMT_SMR.2 Restrictions on security roles
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control OR FDP_IFC.1 Subset information flow control	FDP_ACC.1 Subset access control
	FMT_SMR.1 Security roles	FMT_SMR.2 Restrictions on security roles

SFR	Dependencies	Dependency Coverage in ST
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 Specification of Management Functions
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles	FMT_SMR.2 Restrictions on security roles
FMT_MTD.1 Management of TSF Data	FMT_SMR.1 Security roles	FMT_SMR.2 Restrictions on security roles
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 Specification of Management Functions
FMT_MTD_EXT.4 TSF private key confidentiality protection	No dependencies	Not applicable
FMT_MTD_EXT.5 TSF secret key confidentiality protection	No dependencies	Not applicable
FMT_MTD_EXT.7 Extended TSF private and secret key export	No dependencies	Not applicable
FMT_SMF.1 Specification of Management Functions	No dependencies	Not applicable
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	FIA_UID.1 Timing of identification
FPT_STM.1 Reliable time stamps	No dependencies	Not applicable
FTP_ITC.1 Inter-TSF trusted channel	No dependencies	Not applicable

9.3.4 TOE Security Function Coverage

The rationales for this section can be found in the TSS section.

Table 32: SFRs to TOE Security Functions Mapping

SFR / TSF	Security Audit	Remote Data Entry and Export	Identification and Authentication	Certificate Management	Certificate Revocation	Security Management	Key Management
FAU_GEN.1 Audit data generation	X						
FAU_GEN.2 User identity association	X						
FAU_SAR.1 Audit review	X						
FAU_SEL.1 Selective audit	X						

SFR / TSF	Security Audit	Remote Data Entry and Export	Identification and Authentication	Certificate Management	Certificate Revocation	Security Management	Key Management
FAU_STG_EXT.1 Audit trail storage integrity	X						
FCO_NRO_EXT.3 Enforced proof of origin and verification of origin		X					
FCO_NRO_EXT.4 Advanced verification of origin		X					
FCS_CKM.1 Cryptographic key generation							X
FCS_CKM.4 Cryptographic key destruction							X
FCS_COP.1 Cryptographic operation							X
FCS_CPT_EXT.1 Cryptographic Parameter Transfer		X					
FCS_KDF_EXT.1 Cryptographic key derivation							X
FDP_ACC.1 Subset access control						X	
FDP_ACF.1 Security attribute based access control						X	
FDP_ACF_EXT.2 User private key confidentiality protection							X
FDP_ACF_EXT.3 User secret key confidentiality protection							X
FDP_CER_EXT.1 Certificate Generation				X			
FDP_CRL_EXT.1 Certificate revocation list validation					X		
FDP_CSE_EXT.1 Certificate status export				X			
FDP_ETC_EXT.5 Extended user private and secret key export							X
FDP_SDI_EXT.3 Stored public key integrity monitoring and action							X
FIA_ATD.1 User attribute definition						X	
FIA_UAU.1 Timing of authentication			X				
FIA_UID.1 Timing of identification			X				
FIA_USB.1 User-subject binding			X				
FMT_MOF.1 Management of security functions behavior						X	
FMT_MOF_EXT.3 Extended certificate profile management				X			
FMT_MOF_EXT.5 Extended certificate revocation list profile management					X		
FMT_MSA.1 Management of security attributes						X	

SFR \ TSF	Security Audit	Remote Data Entry and Export	Identification and Authentication	Certificate Management	Certificate Revocation	Security Management	Key Management
FMT_MSA.3 Static attribute initialisation						X	
FMT_MTD.1 Management of TSF data						X	
FMT_MTD_EXT.4 TSF private key confidentiality protection							X
FMT_MTD_EXT.5 TSF secret key confidentiality protection							X
FMT_MTD_EXT.7 Extended TSF private and secret key export							X
FMT_SMF.1 Specification of management functions						X	
FMT_SMR.2 Restrictions on security roles						X	
FPT_STM.1 Reliable time stamps	X						
FTP_ITC.1 Inter-TSF trusted channel		X					

9.3.5 Security Assurance Requirements Rationale

PKIs are designed to meet a security level that may be appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. Integrity controls to ensure data is not modified; protections against someone with physical access to the components, and assurances that the PKI is functioning securely are required.

The assurance that satisfies these requirements is EAL 4 augmented.

The assurance level selected for this ST is EAL 4 augmented. EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. Augmentation results from the selection of ALC_FLR.2 Flaw Reporting Procedures as described above. Since the TOE is security-related, the tracking of security flaws is a very reasonable expectation and within the bounds of standard, best commercial practice. EAL4 augmented is deemed appropriate to satisfy customers' expectations for trusted certificate authorities.

10 Acronyms and Terminology

10.1 CC Acronyms

The following table defines CC specific acronyms used within this Security Target.

Table 33: CC Acronyms

Acronym	Definition
CC	Common Criteria
CM	Cryptographic Module
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
RBAC	Role-Based Access Control
RFC	Request for Comment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SO	Security Objective
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

10.2 CC Terminology

The following table defines CC-specific terminology used within this Security Target.

Table 34: CC Terminology

Terminology	Definition
Access Control	A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism.
Authorized Administrator	A term synonymous with “Administrator”, used because some Common Criteria SFRs use the specific terminology.
Operational Environment	The collection of hardware and software resources in an enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.

Terminology	Definition
Role-Based Access Control	A means of access control that authorizes subject requests based on the roles to which they are assigned and the authorizations that are associated with those roles.
User	A blanket term for a generic user of the TOE; any entity that is identified and authenticated to ECA or ECAA.

10.3 Product Acronyms and Terminology

The following table defines Product-specific acronyms and terminology used within this Security Target.

Table 35: Product Acronyms

Terminology	Definition
AES	Advanced Encryption Standard
ASH	Administration Service Handler
CA	Certification Authority
CMP	IETF PKIX Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CV	Card Verifiable
CVCA	Country Verifying Certification Authority
DN	Distinguished Name
DSA	Digital Signature Algorithm
DV	Document Verifier
EA	Entrust Authority
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECA	Entrust Certificate Authority
ECAA	Entrust Certificate Authority Administration
ECDSA	Elliptic Curve Digital Signature Algorithm
GUI	Graphical User Interface
HMAC	Keyed-hash message authentication code
HSM	Hardware Security Module
IS	Inspection System
ISO	International Organization for Standardization

Terminology	Definition
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
OCSP	Online Certificate Status Protocol
ODBC	Open Database Connectivity
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest, Shamir, Adleman [public key algorithm]
SHA	Secure Hash Algorithm
XAP	XML Administration Protocol (XAP)
XML	Extensible Markup Language

11 References

The following are references used within this Security Target.

Table 36: References

Short form	Reference
CC	Common Criteria for Information Security Evaluation. Version 3.1 Revision 5, April, 2017
CMP	RFC 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocol, September 2005
FIPS 46-3	U.S. National Institute of Standards and Technology – Data Encryption Standard (DES), October 25, 1999
FIPS 186-4	U.S. National Institute of Standards and Technology – Digital Signature Standard, July 19, 2013
FIPS 180-1	U.S. National Institute of Standards and Technology - Secure Hash Standard, April 1995
FIPS 180-4	U.S. National Institute of Standards and Technology - Secure Hash Standard, August 4, 2015
FIPS 197	U.S. National Institute of Standards and Technology – Advanced Encryption Standard, November 2001
ICAO	International Civil Aviation Organization Standards
ISO 7816	ISO/IEC 7816: Identification Cards – Integrated Circuit Cards (Parts 10, 11 & 12)
NIST SP 800-132	Recommendation for Password-Based Key Derivation: Part 1: Storage Applications
NIST SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques
NIST SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
NIST SP 800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
NIST SP 800-90A Rev1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols
RFC 2511	Internet X.509 Certificate Request Message Format
RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
TR-03110-3	European Union – Article 6 Committee - Brussels Interoperability Group – Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control, Version 2.21 , Dec 2016
X.509	ITU-T Recommendation X.509 (2005 | ISO/IEC 9594-8: 2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks