TÜBİTAK BILGEM UEKAE
CENTER OF RESEARCH FOR ADVANCED TECHNOLOGIES OF INFORMATICS AND INFORMATION SECURITY

G203 - National PKI Project

E-CERTIFICATE MANAGEMENT INFRASTRUCTURE (ESYA) V1.0

SECURITY TARGET LITE

Revision No	1.0
Revision Date	07.12.2010
Document Code	ESYA1.0-ST-LITE
Certificate No	TR-14.10.01 / TSE-OKBS-004
Certicate Date	02.03.2010
Prepared by	
Murat Yasin KUBİLAY, *Chief Researcher*	
Validated by	
MA3 Project Manager, *Chief Researcher*	Ersin GÜLAÇTI

REVISION HISTORY

RevisionNo	Revision Reason	Revision Date
1.0	Public Security Target Creation	07.12.2010

CONTENT

LIST OF FIGURES

LIST OF TABLES

1 SECURITY TARGET INTRODUCTION

1.1 ST Reference

ST Title: E-Certificate Management Infrastructure (ESYA) v 1.0 Public Security Target Lite Revision 1.0, 07.12.2010

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

1.1.1 Operation Notation for Functional Requirements

There are four types of operations that can be applied on functional requirements. These are;

Selection: Shown by cornered brackets and italicized text.

Assignment: Shown by cornered brackets and regular text.

Refinement: Indicated by underlined text for additions or strikethrough text for deleted items.

Iteration: Indicated by assigning a number at the functional component level.

1.2 TOE Reference

TOE Identification: E-Certificate Management Infrastructure (ESYA) v1.0

1.3 TOE Overview

ESYA v1.0 (TOE) is an X.509 certificate generation and management system software. TOE provides the following features:

- The important TOE events are logged for further security audit in order to identify the security violations;
- TOE and user public, private and secret keys are protected against unauthorized modification and disclosure using the cryptographic functions provided by the environment;
- User data is protected by means of certificate issuance, revocation, recovery;
- Certificate and Certificate Revocation List profiles are managed;
- Persons can not perform TOE Security Functions unless they are properly identified and authenticated;
- Security functions are managed by providing distinct roles in order to maintain the security of TOE;
- The integrity of confidential data are protected from disclosure and modification by means of encryption, reliable time stamps, self tests and audit logs;
- The data transmitted between the TOE and remote users are protected against modification and disclosure.

1.4 TOE Description

ESYA v1.0 (TOE) is an X.509 certificate generation and management system software. TOE and its operational environment provides privacy, access control, integrity, confidentiality, authentication and non repudiation services.

TOE is composed of Certification Authority Services, Administration Center and Registration Authority. TOE is software and it does not include any hardware components.

TOE can be used to provide security in the electronic transactions for the organizations. By implementing asymmetric cryptography and using electronic certificates and cryptographic keys, both TOE and its operational environment enable secure communication between parties. This infrastructure is comprised of certification server and other auxiliary applications. End users are entitled to get a certificate by proving their identities and registering to the TOE. This certificate can be used for electronic signatures and data encryption. TOE and its operational environment provides authentication, non repudiation, message integrity and confidentiality services by means of this infrastructure.

In TOE three different roles are defined:

- **Administrator**

Administrators administrate Certification Authority Services and Administration Center. They use smartcards which contain signature, encryption key pairs and the corresponding administrator certificates issued by the CA in order to logon the Certification Authority Services and Administration Center applications.

- **Registrar**

Registrars register and manage the end user, device information through the Registration Authority application. They also create requests to the Certification Authority Services for issuing or revoking certificates. Registrars are not entitled to run all the services offered by the Registration Authority. The access control of the services for the registrars is configurable from the Administration Center. Registrars use smartcards which contain signature, encryption key pairs and the corresponding registrars certificates issued by the CA in order to logon the Registration Authority application.

- **Auditor**

Auditors review the audit logs and create reports using the Administration Center application. Auditors use smartcards which contain signature, encryption key pairs and the corresponding auditor certificates issued by the CA in order to logon the Administration Center application.

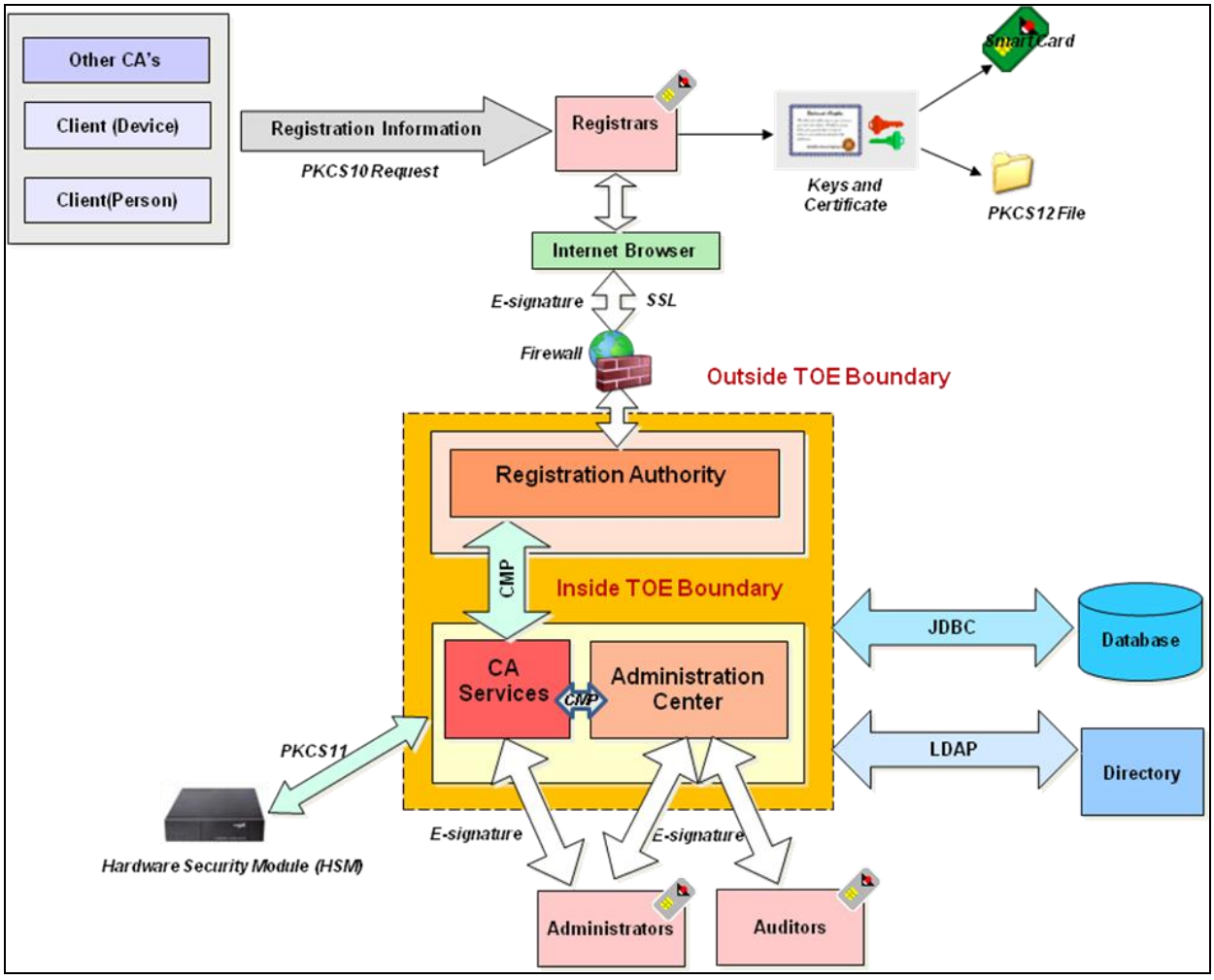
1.4.1 TOE Boundary

TOE boundary is indicated in Figure 1. The components that are included within TOE boundary are:

- Certification Authority Services
- Administration Center
- Registration Authority

Note: The servers, which are shown inside the TOE boundary at Figure 1, are not the parts of TOE. They are environmental components. TOE is completely software, it does not include any hardware or firmware components.

Figure 1 TOE Boundary



1.4.1.1 Certification Authority Services

Certification Authority Services

- Generate X.509 certificates, certificate revocation lists (CRLs),
- Distribute the up-to-date certificates and CRLS,

1.4.1.1.1 Certification Service

Certification Service is a network service which listens a specified port and generates X.509 certificates for valid requests.

1.4.1.1.2 CRL Service

CRL Service revokes the certificates for several reasons and issues CRLS.

1.4.1.1.3 Archive Service

Archive Service archives data for long term usage. Archived data is protected against unauthorized modification.

1.4.1.1.4 CMP

Certificate Management Protocol (CMP) provides on-line interactions between the CA Services and Administration Center/Registration Authority. This infrastructure component is implemented according to RFC 4210 (Internet X.509 Public Key Infrastructure Certificate Management Protocol).

1.4.1.2 Administration Center

Administration center is a GUI application which can be used by the administrators to administrate the Certification Authority. Administration center mainly provides the following functionality.

- Definition, activation, deactivation of administrators, registrars, auditors and their privilege management.
- Configuration of Certification Authority Services
- Definition of Certificate, CRL profiles
- Audit of events to be audited by auditors

1.4.1.3 Registration Authority

Registration Authority can be used by the registrars and end users. It provides the following functionality.

- Application can be started by Administrators.
- Receiving end user and device information and validation for further usage in generating certificate.
- Access through a web based interface for registrars
- Management of end user, device information
- Requesting certificate from the certification server for end user/device
- A web based interface for self requesting certificate for the end users
- Request for revoking or placing a certificate on hold.

1.4.2 TOE Operational Environment

The components excluded from the TOE boundary are given below. Also the justification reasons for exclusion are also explained.

1.4.2.1 Database

All the infrastructure and end user data is stored in the database. The following data is stored as encrypted.

- Symmetric key for DB table row signature
- Directory user's password
- End user encryption certificate private keys

This security target has no claims regarding the internal security of the database. The confidentiality and integrity of the sensitive data stored in the database is provided by TOE which uses the cryptographic functions from the environment. In addition, this document also has no claims regarding the basic database functionality. None of the database functionality is matched with the security functionality requirement.

1.4.2.2 Directory

TOE supports LDAP compatible directories. Public certificates of users and certificate revocation lists are written by the Certificate and CRL services to the directory.

This document has no claims regarding the internal security of the directory. None of the basic directory functionality is matched with the security functionality requirement.

1.4.2.3 Java Application Server

It's a java application server which runs the Registration Authority. It can be one of the COTS java application servers like Apache Tomcat, Sun ONE etc.

This document has no claims regarding the internal security of the java application server.

1.4.2.4 Hardware and Operating System Platform

- **Operating System:** It is assumed that OS works correctly. The recommended OS for the TOE is Windows 2003 which is certified with Common Criteria EAL 4 level.
- **Hardware Independence:** TOE is optimized to execute any x86-based machines, regardless of the hardware vendor. TOE can run on the hardware platform which meets the following minimum requirements.
  - **Certification Authority Services and Administration Center**
    - Windows 2003 R2 Service Pack 2 x86 32bit Pentium III 800 MHz processor
    - 512 MB RAM and minimum 300 MB disk space

- **Registration Authority**
  - Windows 2003 R2 Service Pack 2 x86 32bit Pentium III 800 MHz processor
  - 512 MB RAM and minimum 1 GB disk space

1.4.2.5 Cryptographic Modules

1.4.2.5.1 HSM

FIPS 140-2 level 3 validated hardware cryptographic modules must be used for the following cryptographic functions used by the TOE.

- Certificate Signing
- CRL Signing
- Encryption private key decryption for key recovery

1.4.2.5.2 Software Cryptographic Module

The following cryptographic functions are performed in the software cryptographic module. This module is bundled with the TOE software but it's not a part of the TOE.

- Key Generation
- Asymmetic Encryption
- Signature Verification
- Symmetric Encrption/Decryption
- Hash generation
- MACs

1.4.2.5.3 Smart Cards

At least CC EAL 4 validated smartcards are used for identification and authentication of Administrators, Registrars and Auditors.

2 CONFORMANCE CLAIM

2.1 CC Conformance Claim

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009, extended.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 3, July 2009, conformant.

2.2 **PP Claim**

In this ST, TOE does not claim any conformance to a protection profile. But it uses the following Protection Profile (PP) as a guidance:

Certificate Issuing and Management Components (CIMC) Security Level 4 PP, version 1.0, October 31, 2001.

2.3 **Package Claim**

EAL 4+ (ALC_FLR.2)

2.4 **Conformance Rationale**

The assurance level selected for this ST is EAL 4 augmented (ALC_FLR.2). EAL 4 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. 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. EAL 4 augmented is deemed appropriate to satisfy customers' expectations for trusted certificate authorities.

3 SECURITY PROBLEM DEFINITION

This section includes the following:

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

This information provides the basis for the Security Objectives specified in Section 4, the security functional requirements for the TOE and environment specified in Sections 6.1 and the TOE Security Assurance Requirements specified in Section 6.2.

3.1 Organizational Security Policies

Table 3-1 Organizational Security Policies

POLICY NAME	DESCRIPTION
P.Authorized use of information	Information shall be used only for its authorized purpose(s). Authorization and authentication management of the TOE users will be managed according to the TOE Access Control Policy.
P.Cryptography and secure storage of cryptographic assets	FIPS-approved or NIST-recommended cryptographic algorithms and devices shall be used to perform all cryptographic operations.

3.2 **Assumptions**

Table 3-2 Assumptions

ASSUMPTION NAME	DESCRIPTION
A.Auditors Review Audit Logs	Audit logs must be reviewed by the Auditors at least once a week.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that authorized users change their authentication data at least once a month with minimum 6 digit numbers.
A.Competent Administrators, Registrars and Auditors	Competent Administrators, Registrars and Auditors will be assigned to manage the TOE and the security of the information it contains.
A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
A.Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity.
A.Notify Authorities of Security Issues	Since authorized users do not intentionally perform hostile actions, Registrars and Auditors notify Administrators of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Cooperative Users	TOE users need to accomplish some task or group of tasks that require a secure IT environment. The TOE users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.
A.Operating System	The operating system has been selected to provide the functions required by the TOE.
A.Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE and the operational environment are protected from physical attack that might compromise IT security.

3.3 **Threats**

The threats are organized in three categories:

- Threats countered by TOE
- Threats countered by TOE Operational Environment
- Threats countered by both TOE and TOE Operational Environment

3.3.1 Threats Countered by TOE

Table 3-3 Threats countered by TOE

THREAT NAME	DESCRIPTION
T.Sender denies sending information	The sender (authorized users) of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

3.3.2 Threats Countered by TOE Operational Environment

Table 3-4 Threats countered by TOE Operational Environment

THREAT NAME	DESCRIPTION
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design or system operation.

3.3.3 Threats countered by both TOE and TOE Operational Environment

Table 3-5 Threats countered by both TOE and TOE Operational Environment

THREAT NAME	DESCRIPTION
T.Administrative errors of omission	Administrators, Registrars or Auditors fail to perform some function essential to security.
T.Administrators, Registrars and Auditors commit errors	An Administrator, Registrar or Auditor commits errors that change the intended security policy of the TOE and its operational environment.
T.Critical system component fails	Failure of one or more system components results in the loss of system critical functionality.
T.Malicious code exploitation	A distant hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. The malicious code is not a self running code but it is executed through a triggering event.
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. Several kinds of modification are possible: modification of a single message, deletion or reordering of selected messages, insertion of bogus messages, replay of previous messages, and modification of accompanying message security attributes.
T.Hacker gains access	A distant 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.Modification of private/secret keys	A secret/private key is modified by a distant hacker so that invalid certificates can be issued
T.Disclosure of private and secret keys	A private or secret key is improperly disclosed by a distant hacker due to insufficient security measures or errors committed by the Administrators, Registrars or Auditors so that fake certificates can be issued by unauthorized people.

4 SECURITY OBJECTIVES & RATIONALE

This section includes the security objectives for TOE and its operational environment. Also this section demonstrates that the stated security objectives counter all identified threats, organisational security policies and assumptions.

4.1 IT Security Objectives for the TOE and Rationale

This section provides information regarding:

- TOE IT Security Objectives,
- Why the identified TOE IT security objectives provide for effective countermeasures to the following threats, and:
- Why the identified TOE IT security objectives provide complete coverage to the following organizational security policy.

Table 4-1 TOE Security Objectives and Rationale to Threats and OSPs

IT Security Objective	Threats and OSPs	Rationale
O.Certificates The TSF must ensure that certificates, certificate revocation lists and certificate status information are valid.	T.Administrators, Registrars and Auditors commit errors	**O.Certificates** ensures that certificates, certificate revocation lists, and certificate status information are valid. The validation of information provided by Registrars that is to be included in certificates helps to prevent improperly entered information from appearing in certificates.
O.Control unknown source communication traffic Control (e.g., reroute or discard) communication traffic from an unknown source to prevent potential damage.	T.Hacker gains access	**O.Control unknown source communication traffic** ensures that communication traffic from an unknown source is controlled (e.g., rerouted or discarded) to prevent potential damage. Various kinds of hacker attacks can be detected or prevented by rerouting or discarding suspected hacker traffic.

IT Security Objective	Threats and OSPs	Rationale
O.Non-repudiation Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.	T.Sender denies sending information	**O.Non-repudiation** which ensures that the sender/originator of a message cannot successfully deny sending the message to the recipient.
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.	T.Administrative errors of omission	**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 fail to perform security-critical operations so they can be held accountable.
	T.Hacker gains access	**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 damage resulting from such activity can be eliminated or mitigated.
	T.Administrators, Registrars and Auditors commit errors	O.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so

IT Security Objective	Threats and OSPs	Rationale
		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 authorized users that perform inappropriate operations so they can be held accountable.
O.Integrity protection of user data and software Provide appropriate integrity protection for user data and software by e-signature.	T.Modification of private/secret keys	**O.Integrity protection of user data and software** that ensures that appropriate integrity protection is provided for secret and private keys.
	T.Malicious code exploitation	**O.Integrity protection of user data and software** ensures that appropriate integrity protection is provided for user data and software by e-signatures. This prevents malicious code from attaching itself to user data or software.
	T.Hacker gains access	**O.Integrity protection of user data and software** ensures that appropriate integrity protection is provided for user data and software by e-signatures. This helps TOE users the illegal modifications in user data and software.
O.Limitation of administrative access Design administrative functions so that Administrators, Registrars and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system	T.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.

IT Security Objective	Threats and OSPs	Rationale
by Administrators who troubleshoot the system and perform system updates.	T.Administrators, Registrars and Auditors commit errors	**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.
	P. Authorized use of information	**O.Limitation of administrative access.** The administrative operations is limited to those who have been authorized to perform those operations
O.Maintain user attributes Maintain a set of security attributes (which may include role membership. access privileges, etc.) associated with individual users. This is in addition to user identity.	T.Administrators, Registrars and Auditors commit errors	**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.
	P.Authorized use of information	**O.Maintain user attributes** ensures that users are only authorized to perform those operations that are necessary to perform their jobs.
O.Manage behavior of security functions Provide management functions to configure, operate and maintain	T.Critical system component fails	**O.Manage behavior of security functions** provides management controls/functions for security mechanisms. This ensures that critical system components do not fail as a result of improper

IT Security Objective	Threats and OSPs	Rationale
the security mechanisms.		configuration of security mechanisms.
	T.Administrators, Registrars and Auditors commit errors	**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.
O.Data import/export Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.	T.Message content modification	**O.Data Import/Export** 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 fraudulent messages.
O.Protect stored audit records Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.	T.Modification of private/secret keys	**O.Protect stored audit records** ensures that audit records are protected against unauthorized access, modification, or deletion to provide for traceability of user actions. This objective ensures that modifications to private and secret keys can be detected through the audit trail.

IT Security Objective	Threats and OSPs	Rationale
	T.Administrators, Registrars and Auditors commit errors	**O.Protect stored audit records** ensures that audit records are protected against unauthorized access, modification, or deletion to provide for traceability of user actions.
O.Protect user and TSF data during internal transfer Ensure the integrity of user and TSF data transferred internally within the system.	T.Message content modification	**O.Protect user and TSF data during internal transfer** protects data being transmitted between separated parts of the TOE. Protection of data in transit permits the TOE to detect modified messages, message replay, or fraudulent messages.
	T.Disclosure of private and secret keys	**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.
O.Respond to possible loss of stored audit records Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.	T.Administrators, Registrars and Auditors commit errors	**O.Respond to possible loss of stored audit records** ensures that only auditable events executed by the Auditor shall be audited if the audit trail is full. This ensures that operations that are performed by users other than the Auditor are audited and so can be detected.
O.Restrict actions before authentication Restrict the actions a user may perform before the TOE authenticates the identity of the user.	T.Hacker gains access	**O.Restrict actions before authentication** ensures that only a limited set of actions may be performed before a user is authenticated. This prevents a hacker who is unable to circumvent the access control mechanisms from performing security-relevant operations.

IT Security Objective	Threats and OSPs	Rationale
	T.Administrators, Registrars and Auditors commit errors	**O.Restrict actions before authentication** ensures that only a limited set of actions may be performed before a user is authenticated.
	P.Authorized use of information	**O.Restrict actions before authentication** ensures that the capability to perform security-relevant operations is limited to those who have been authorized to perform those operations.
O.Security roles Maintain security-relevant roles and the association of users with those roles.	T.Administrators, Registrars and Auditors commit errors	**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.
	P.Authorized use of information	**O.Security Roles** ensures that users are only authorized to perform those operations that are necessary to perform their jobs.
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.	T.Administrative errors of omission	**O.Security-relavant configuration management** ensures that system security policy data and enforcement functions, and other security-relevant configuration data are managed and updated. This ensures that they are consistent with organizational security policies and that all changes are properly tracked and implemented.
O.User authorization management Manage and update	P.Authorized use of information	**O.User authorization management** ensures that users are only authorized to perform those operations that are necessary

IT Security Objective	Threats and OSPs	Rationale
user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.		to perform their jobs.

4.2 Security Objectives for the Operational Environment and Rationale

This section provides information regarding:

- Operational Environment IT and Non-IT Security Objectives,
- Why the identified security objectives provide for effective countermeasures to the following threats,
- Why the identified security objectives uphold each assumption, and:
- Why the identified security objectives provide complete coverage to the following organizational security policy.

Table 4-2 Non-IT and IT security objectives for the operational environment and Rationale to threats, assumptions and OSPs

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
Non-IT-OE. Administrators, Registrars and Auditors guidance documentation Prevent Administrator, Registrar or Auditor errors by providing adequate documentation on securely configuring and operating the TOE.	T.Disclosure of private and secret keys	**OE.Administrators, Registrars and Auditors guidance documentation** ensures that adequate documentation on securely configuring and operating the TOE is available to Administrators, Registrars and Auditors. This documentation will minimize errors committed by those users.
	T.Administrators, Registrars and Auditors commit errors	**OE.Administrators, Registrars and Auditors guidance documentation** which deters authorized personnel errors by providing adequate guidance.
	T.Social engineering	**OE.Administrators, Registrars and Auditors guidance documentation** which deters authorized personnel errors by providing adequate guidance.

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
Non-IT-OE. Competent Administrators, Registrars and Auditors Provide capable management of the TOE by assigning competent Administrators, Registrars and Auditors to manage the TOE and the security of the information it contains.	T.Administrators, Registrars and Auditors commit errors	**OE.Competent Administrators, Registrars and Auditors** ensures that users are capable of maintaining effective security practices. This reduces the likelihood that they will commit errors.
	A.Competent Administrators, Registrars and Auditors	**A.Competent Administrators, Registrars and Auditors** is addressed by **OE.Competent Administrators, Registrars and Auditors**, which ensures that the system managers will be competent in its administration.
Non-IT-OE. CPS All Administrators, Registrars and Auditors shall become familiar by reading the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.	T.Administrative errors of omission	**OE.CPS** provides Administrators, Registrars, and Auditors with information regarding the policies and practices used by the system. Providing this information ensures that these authorized users of the system are aware of their responsibilities, thus reducing the likelihood that they will fail to perform a security-critical operation.
Non-IT-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.	T.Critical system component fails	**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.

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
Non-IT-OE. Lifecycle security Provide tools and techniques used during the development phase to ensure security is designed into the TOE. Detect and resolve flaws during the operational phase.	T.Critical system component fails	**OE.Lifecycle security** provides tools and techniques that are used throughout the development phase reducing the likelihood of hardware or software imperfections. OE.Lifecycle security also addresses the detection and resolution of flaws discovered during the operational phase that may result in failure of a critical system component.
	T.Malicious code exploitation	**OE.Lifecycle security** provides tools and techniques that are used throughout the development phase, reducing the likelihood that malicious code was included in the product during the operational phase. OE.Lifecycle security also addresses the detection and resolution of flaws discovered during the operational phase, such as modifications of components by malicious code.
Non-IT-OE. Notify Authorities of Security Issues Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.	T.Hacker gains access	**OE.Notify Authorities of Security Issues** ensures that proper authorities are notified regarding any security issues that impact their systems. This minimizes the potential for the loss or compromise of data.
	A.Notify Authorities of Security Issues	**A.Notify Authorities of Security Issues** is addressed by **OE.Notify Authorities of Security Issues** which ensures that user notify proper authorities of any security issues that impact their systems.

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
Non-IT-OE. Social Engineering Training Provide training for Administrators, Registrars and Auditors in techniques to prevent social engineering attacks.	T.Social Engineering	**OE.Social Engineering Training** which ensures that Administrators, Registrars and Auditors are trained in techniques to thwart social engineering attacks.
Non-IT-OE. Procedures for preventing malicious code Incorporate malicious code prevention procedures and mechanisms.	T.Social engineering	**OE.Procedures for preventing malicious code** provides a set of procedures and mechanisms that work to prevent incorporation of malicious code into the system. The introduction of malicious code into the system may be a goal of the social engineering attack.
IT-OE. Cryptographic functions The environment must implement NIST-recommended cryptographic algorithms for encryption/decryption, authentication, and signature generation/verificatio	T.Disclosure of private and secret keys	**OE.Cryptographic functions** ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and uses validated cryptographic modules. Use of validated cryptographic modules ensures that cryptographic keys are adequately protected when they are stored within cryptographic modules.

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
n; approved key generation techniques and use validated hardware cryptographic modules. (Validated is defined as FIPS 140-2 validated.)		
	T.Modification of private/secret keys	**OE.Cryptographic functions** ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and uses validated cryptographic modules. Use of validated cryptographic modules ensures that cryptographic keys are adequately protected when they are stored within cryptographic modules.
	P.Cryptography and secure storage of cryptographic assets	**OE.Cryptographic functions** ensures that NIST-recommended cryptographic algorithms and validated hardware cryptographic modules are used and the cryptographic assets which are not stored in an hardware cryptographic module are stored in an encrypted form
IT-OE. Periodically check integrity Provide periodic integrity checks on both system, software and backup data.	T.Malicious code exploitation	**OE.Periodically check integrity** ensures that periodic integrity checks are performed on both system, software and backup data. If these checks fail, malicious code may have been introduced into the system.
IT-OE. Trusted Path Provide a trusted path between the user and the system. Provide a trusted path to	T.Hacker gains access	**OE.Trusted Path** ensures that a trusted path is established between the user and the system. The trusted path is used to protect authentication data, thus reducing the likelihood that a hacker can masquerade as an

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
security-relevant TSF data in which both end points have assured identities.		authorized user.
	T.Message content modification	**OE.Trusted Path** ensures that a trusted path is established between the user and the system. The trusted path protects messages from interception or modification by a hacker.
IT-OE. Validation of security function Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.	T.Malicious code exploitation	**OE.Validation of security function** ensures that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as underlying machine testing and integrity checks.
	T.Administrators, Registrars and Auditors commit errors	**OE.Validation of security function** ensures that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as underlying machine testing and integrity checks.
IT-OE. Configuration Management Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components	T.Critical system component fails	**OE.Configuration Management** assures that a configuration management program is implemented. The configuration management program includes configuration identification and change control. This ensures that critical system components do not fail as a result of improper configuration.
	T.Malicious code exploitation	**OE.Configuration Management** assures that a configuration management program is implemented. The configuration

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
(software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.		management program includes configuration identification and change control. This ensures that malicious code is not introduced during the configuration process.
IT-OE. Object and data recovery free from malicious code Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.	T.Modification of private/secret keys	**OE.Object and data recovery free from malicious code** ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. If the malicious code cause private or secret keys to be revised in an unauthorized manner, this objective ensures that they are recovered to their correct values.
	T.Malicious code exploitation	**OE.Object and data recovery free from malicious code** ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removed as part of the process.
IT-OE. React to detected attacks Implement responses to the authorized user discovered attacks to create an attack deterrent.	T.Hacker gains access	**OE.React to detected attacks** ensures that necessary precautions will be taken for the authorized user detected attacks to create an attack deterrent. This objective is relevant if actions that the organization deems essential also pose a potential attack that could be exploited.

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
IT-OE. Time stamps Provide reliable time.	T.Critical system component fails	**OE.Time stamps** provides time stamps to ensure that the sequencing of events can be verified. If the system must be reconstructed, it may be necessary to establish the order in which transactions were performed to return the system to a state consistent with the state when a critical component failed.
	T.Administrators, Registrars and Auditors commit errors	**OE.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.
IT-OE. Preservation/trusted recovery of secure state Preserve the secure state of the system in the event of a secure component failure and/or recover to a secure state.	T.Critical system component fails	**OE.Preservation/trusted recovery of secure state** ensures that the system remains in a secure state throughout operation in the presence of failures and subsequent system recovery. This objective is relevant when system failures could result in insecure states that, when the system returns to operational mode (or continues to operate), could lead to security compromises.
IT-OE. Sufficient backup storage and effective restoration Provide sufficient backup storage and effective restoration to ensure that the system can be	T.Critical system component fails	**OE.Sufficient backup storage and effective restoration** ensures that there is sufficient backup storage and effective restoration to recreate the system, when required. 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).

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
recreated.		
Non-IT-OE. Authentication Data Management Ensure that users change their authentication data at least once a month with minimum 6 digit numbers	A.Authentication Data Management	**A.Authentication Data Management** is addressed by **OE.Authentication Data Management**, which ensures that users modify their authentication data in accordance with appropriate security policy.
Non-IT-OE. Communications Protection Protect the system against a physical attack on the communications capability by providing adequate physical security.	A.Communications Protection	**A.Communications Protection** is addressed by **OE.Communications Protection**, which ensures that adequate physical protections are afforded the necessary communications infrastructure.
Non-IT-OE. Cooperative Users Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE.	A.Cooperative Users	**A.Cooperative Users** is addressed by **OE.Cooperative Users**, which ensures that users will cooperate with the constraints established.

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
Non-IT-OE. Disposal of Authentication Data Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).	A.Disposal of Authentication Data	**A.Disposal of Authentication Data** is addressed by **OE.Disposal of Authentication Data**, which ensures that access to the system will be denied after a user's privileges have been removed.
Non-IT-OE. Malicious Code Not Signed Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.	A.Malicious Code Not Signed	**A.Malicious Code Not Signed** is addressed by **OE.Malicious Code Not Signed**, which ensures that code must be signed by a trusted party or it will not be loaded onto the system.
Non-IT-OE. Physical Protection Those responsible for the TOE must ensure that the TOE and the operational environment are protected from physical attack that might compromise IT security.	A.Physical Protection	**A.Physical Protection** is addressed by **OE.Physical Protection**, which ensures that adequate physical protection will be provided.
Non-IT-OE. Operating System The operating system	A.Operating System	**A.Operating System** is addressed by **OE.Operating System**, which ensures that an operating system that meets the minimum CC assurance

IT and Non-IT Security Objective	Threats, Assumptions and OSPs	Rationale
used is validated to provide adequate security, including domain separation and nonbypassability, in accordance with minimum CC assurance level EAL 4 certified.		level EAL 4 will be used.
Non-IT-OE. Auditors Review Audit Logs Identify and monitor security-relevant events by requiring auditors to review audit logs at least once a week.	P.Authorized use of information	**OE.Auditors Review audit logs** deters users from misusing the authorizations they have been provided.
	A.Auditors Review Audit Logs	**A.Auditors Review Audit Logs** is addressed by **OE.Auditors Review Audit Logs**, which ensures that security-relevant events recorded in audit logs are reviewed by auditors.

5 EXTENDED COMPONENT DEFINITION

5.1 **Communication**

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

Hierarchical to: FCO_NRO.2

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO_TOE.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_TOE.3.2 The TSF shall be able to relate the identity of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

FCO_NRO_TOE.4 **Advanced verification of origin**

Hierarchical to: No other components.

Dependencies: FCO_NRO_TOE.3

FCO_NRO_TOE.4.1 The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using [selection: *an authentication code, keyed hash, digital signature algorithm*].

FCO_NRO_TOE.4.2 The TSF shall, for all other security-relevant information, only accept the information if it was signed using a digital signature algorithm.

5.2 User Data Protection

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

Hierarchical to: No other components
Dependencies: No dependencies

FDP_ACF_TOE.2.1 TOE personnel private keys shall be stored in smartcard.

FDP_ACF_TOE.2.2 If certificate subject private keys are stored in the environment(database), they shall be encrypted using CMSEnvelope(AES256 symmetric key for subject private key encryption, TOE asymmetric key for symmetric key encryption).

FDP_TOE_CER.1 **Certificate Generation**

Hierarchical to: No other components
Dependencies: No dependencies

FDP_TOE_CER.1.1 The TSF shall only generate certificates whose format complies with the X.509 standard for public key certificates.

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

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

FDP_TOE_CER.1.4 TSF generates X.509 public key certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. The TSF shall ensure that:

- The version field shall contain the integer 2.
- The serialNumber shall be unique with respect to the issuing Certification Authority.
- The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.

- If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
- 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.
- The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID (object identifier) for a FIPS-approved or recommended algorithm.

FDP_TOE_CRL.1 Certificate revocation list validation

Hierarchical to: No other components

Dependencies: No dependencies

FDP_TOE_CRL.1.1 A TSF that issues CRLs shall verify that all mandatory fields in any CRL issued contain values in accordance with ITU-T Recommendation X.509. The following items shall be validated:

- If the version field is present, then it shall contain a 1.
- If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
- If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.
- The signature and signatureAlgorithm fields shall contain the OID (object identifier) for a FIPS-approved digital signature algorithm.
- The thisUpdate field shall indicate the issue date of the CRL.
- The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

FDP_TOE_CSE.1 Certificate status export

Hierarchical to: No other components

Dependencies: No dependencies

FDP_TOE_CSE.1.1	Certificate status information shall be exported from the TOE in messages whose format complies with the X.509 standard for CRLs.

FDP_ETC_TOE.5	**Extended user private and secret key export** Hierarchical to: FDP_ETC_TOE.4 Dependencies: No dependencies
FDP_ETC_TOE.5.1	Private and secret keys shall only be exported from the TOE in encrypted form. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.
FDP_SDI_TOE.3	**Stored public key integrity monitoring and action** Hierarchical to: No other components Dependencies: No dependencies
FDP_SDI_TOE.3.1	Public keys stored within the environment, but not within a FIPS 140-2 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures.
FDP_SDI_TOE.3.2	The digital signature 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.

5.3 **Security Management**

FMT_MOF_TOE.3 **Extended certificate profile management**

Hierarchical to: FMT_MOF_TOE.2

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

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

FMT_MOF_TOE.3.2 The TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

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

FMT_MOF_TOE.3.3 The TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions in the X.509 public key certificates:

- keyUsage;
- basicConstraints;
- certificatePolicies

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

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

Hierarchical to: FMT_MOF_TOE.4

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

FMT_MOF_TOE.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_TOE.5.2 If the TSF issues CRLs, the TSF shall require the

	Administrator to specify the set of acceptable values for the following fields and extensions: • issuer; • nextUpdate (i.e., lifetime of a CRL).
FMT_MOF_TOE.5.3	If the TSF issues CRLs, the Administrator shall specify the acceptable set of CRL and CRL entry extensions.
FMT_MTD_TOE.5	**TSF secret key confidentiality protection** Hierarchical to: No other components Dependencies: No dependencies
FMT_MTD_TOE.5.1	TSF secret keys stored by the TOE shall be stored in encrypted form. The encryption shall be performed by NIST approved algorithms.
FMT_MTD_TOE.7	**Extended TSF private and secret key export** Hierarchical to: No other components Dependencies: No dependencies
FMT_MTD_TOE.7.1	Private and secret keys shall only be exported from the TOE in encrypted form.

5.4 **Protection of the TSF**

FPT_TOE_TSP.1	**Audit log signing event** Hierarchical to: No other components. Dependencies: FAU_GEN.1 Audit data generation FMT_MOF.1 Management of security function behavior
FPT_TOE_TSP.1.1	The TSF shall create an audit log signing event in which it computes keyed hash over the entries in the audit log.
FPT_TOE_TSP.1.2	The keyed hash shall be computed over, at least, every entry that has been added to the audit log since the previous audit log signing event and the keyed hash from the previous audit log signed event.
FPT_TOE_TSP.1.3	The keyed hash from the audit log signing event shall be included in the audit log.

6 SECURITY REQUIREMENTS

6.1 Security Functional Requirements

6.1.1 Security Functional Requirements for the IT Environment

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

Table 6-1 IT Environment Functional Security Requirements

Security Requirement		Component
Cryptographic Support (FCS)	Cryptographic key generation	FCS_CKM.1
	Cryptographic key destruction	FCS_CKM.4
	Cryptographic operation	FCS_COP.1
Protection of the TSF (FPT)	Reliable time stamps	FPT_STM.1
Trusted Path/Channel (FTP)	Trusted path	FTP_TRP.1

6.1.1.1 Cryptographic Support

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The ~~TSF~~ IT environment shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA, ECDSA and AES] and specified cryptographic key sizes [RSA 1024/2048/4096, ECDSA 163/176/191/208/272/304/359/368/431/192/239/256, AES 128/192/256] that meet the following: [FIPS PUB 186-2 (RSA), ANSI X9.62 (ECDSA), FIPS 186-2 APPENDIX 3 (AES) and PUB 197 (AES)].

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The ~~TSF~~ IT environment shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [FIPS 140-2].

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The ~~TSF~~ IT Environment shall perform [decryption, digital signature generation and verification, hashing, Message Authentication Code (MAC) generation and verification] in accordance with a specified cryptographic algorithm [RSA, ECDSA, SHA and AES] and cryptographic key sizes [RSA 1024/2048/4096, ECDSA 163/176/191/208/272/304/359/368/431/192/239/256, SHA 160/224/256/384/512, AES 128/192/256] that meet the following: [FIPS PUB 186-2 (RSA, ECDSA), FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA-2), FIPS PUB 113 (MAC) and FIPS PUB 197 (AES)].

6.1.1.2 Protection of The TSF

FPT_STM.1 Reliable time stamps

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

6.1.1.3 Trusted Path/Channel

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The ~~TSF~~ IT environment shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*].

FTP_TRP.1.2 The ~~TSF~~ IT environment shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The ~~TSF~~ IT environment shall require the use of the trusted path for [*initial user authentication, access to any TOE services authorized for the authenticated operator*].

6.1.2 TOE Security Functional Requirements

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

Table 6-2 TOE Functional Security Requirements

Security Requirement		Component
Security Audit (FAU)	Audit data generation	FAU_GEN.1
	User identity association	FAU_GEN.2
	Selective audit	FAU_SEL.1
	Protected audit trail storage	FAU_STG.1
	Prevention of audit data loss	FAU_STG.4
Communication (FCO)	Enforced proof of origin and verification of Remote Data Entry and Export	FCO_NRO_TOE.3
	Advanced verification of origin Remote Data Entry and Export	FCO_NRO_TOE.4
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_TOE.2
	Certificate Generation	FDP_TOE_CER.1
	Certificate Revocation	FDP_TOE_CRL.1
	Certificate status export	FDP_TOE_CSE.1
	Extended user private and secret key export	FDP_ETC_TOE.5
	Basic internal transfer protection (Iteration 1 and 2)	FDP_ITT.1
	Stored public key integrity monitoring and action	FDP_SDI_TOE.3
	Basic data exchange confidentiality	FDP_UCT.1
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)	Specification of Management Functions	FMT_SMF.1
	Management of security functions behavior	FMT_MOF.1
	Extended certificate profile management	FMT_MOF_TOE.3
	Extended certificate revocation list profile management	FMT_MOF_TOE.5
	Management of security attributes	FMT_MSA.1
	Static attribute initialization	FMT_MSA.3
	Management of TSF data	FMT_MTD.1
	TSF secret key confidentiality protection	FMT_MTD_TOE.5
	Extended TSF private and secret key export	FMT_MTD_TOE.7
	Restrictions on security roles	FMT_SMR.2
Protection of the TSF (FPT)	Audit log signing event	FPT_TOE_TSP.1
	Inter-TSF confidentiality during transmission	FPT_ITC.1
	Basic internal TSF data transfer protection (Iteration 1 and 2)	FPT_ITT.1

6.1.2.1 Security Audit

FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [The events listed in Table 6-3 below].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, 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 6-3 below].

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

Table 6-3 Auditable Events and Audit Data

Section/Function	Event	Additional Details
Local Data Entry	All security-relevant data that is entered in the system	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an "accept" button). This shall be included with the accepted data.
Remote Data Entry	All security-relevant messages that are received by the system	
Data Export and Output	All successful and unsuccessful requests for confidential and security relevant information	
Private Key Load	The loading of Component private keys	
Private Key Storage	All access to certificate subject private keys retained within the TOE for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage	All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key

Section/Function	Event	Additional Details
Secret Key Storage	The manual entry of secret keys used for authentication	
Certificate Status Change Approval	All requests to change the status of a certificate.	Whether the request was accepted or rejected.
TOE Configuration	Any security-relevant changes to the configuration of the TSF	
Security Audit	Any changes to the audit parameters, e.g., audit frequency, type of event audited	
	Any attempt to delete the audit log	
	Audit log signing event	Digital signature, keyed hash, or authentication code shall be included in the audit log.
	Actions taken due to the audit storage failure.	
User Data Protection and Security Management	The export of private and secret keys (keys used for a single session or message are excluded)	
User Data Protection	All certificate requests.	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Registrar, etc.).
Security Management	All changes to the certificate Profile.	The changes made to the profile.
	All changes to the certificate revocation list profile	The changes made to the profile

FAU_GEN.2 User identity association

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_SEL.1 Selective audit

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

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

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*detect*] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [*prevent audited events, except those taken by the authorised user with special rights*] and [no additional action] if the audit trail is full.

6.1.2.2 Communication

FCO_NRO_TOE.3 Enforced proof of origin and verification of origin

FCO_NRO_TOE.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_TOE.3.2 The TSF shall be able to relate the identity of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

FCO_NRO_TOE.4 Advanced verification of origin

FCO_NRO_TOE.4.1 The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using [*an authentication code, keyed hash, digital signature algorithm*].

FCO_NRO_TOE.4.2 The TSF shall, for all other security-relevant information, only accept the information if it was signed using a digital signature algorithm.

6.1.2.3 User Data Protection

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [TOE Access Control Policy:

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

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

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

Subject identification includes:

- Individuals with different access authorizations
- Roles with different access authorizations
- Individuals assigned to one or more roles with different access authorizations

Access type, with explicit allow or deny:

- Read
- Write
- Execute

For each object, an explicit owning subject and role will be identified. Also, the assignment and management of authorizations will be the responsibility of the owner of an object or a role(s), as specified in this ST.
] on [all users, data and files].

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [TOE Access Control Policy specified in FDP_ACC.1] to objects based on the following: [the identity of the subject and the set of roles that the subject is authorized to assume].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [specified in Table 6-4].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

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

Table 6-4 Access Controls

Section/Function	Event
Certificate Request Remote and Local Data Entry	The entry of certificate request data shall be restricted to Registrars and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry	The entry of certificate revocation request data shall be restricted to Registrars and the subject of the certificate to be revoked.
Data Export and Output	The export or output of confidential and security-relevant data shall only be at the request of authorized users.
Key Generation Request	The capability to request the generation of Component keys (used to protect data in more than a single session or message) shall be restricted to Administrators.
Private Key Load	The capability to request the loading of Component private keys into cryptographic modules shall be restricted to Administrators.
Private Key Storage	The capability to request the decryption of certificate subject private keys shall be restricted to Registrars. The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. At least two Registrars or one Registrar and an Administrator or Auditor shall be required to request the decryption of a certificate subject private key.
Trusted Public Key Entry, Deletion, and Storage	The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators.
Secret Key Storage	The capability to request the loading of TOE secret keys into cryptographic modules shall be restricted to Administrators.

Section/Function	Event
Private and Secret Key Destruction	The capability to zeroize TOE plaintext private and secret keys shall be restricted to Administrators, Auditors and Registrars.
Private and Secret Key Export	The capability to export a component private key shall be restricted to Administrators. The capability to export certificate subject private keys shall be restricted to Registrars. The export of a certificate subject private key shall require the authorization of at least two Registrars or one Registrar and an Administrator or Auditor.
Certificate Status Change Approval	Only Registrars and the subject of the certificate shall be capable of requesting that a certificate be placed on hold. Only Registrars shall be capable of removing a certificate from on hold status. Only Registrars shall be capable of approving the placing of a certificate on hold. Only Registrars and the subject of the certificate shall be capable of requesting the revocation of a certificate. Only Registrars shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

FDP_ACF_TOE.2 User private key confidentiality protection

FDP_ACF_TOE.2.1 TOE personnel private keys shall be stored in smartcard.

FDP_ACF_TOE.2.2 If certificate subject private keys are stored in the environment (database), they shall be encrypted using CMSEnvelope (AES256 symmetric key for subject private key encryption, TOE asymmetric key for symmetric key encryption).

FDP_TOE_CER.1 Certificate Generation

FDP_TOE_CER.1.1 The TSF shall only generate certificates whose format complies with the X.509 standard for public key certificates.

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

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

FDP_TOE_CER.1.4 TSF generates X.509 public key certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. The TSF shall ensure that:

- The version field shall contain the integer 2.
- The serialNumber shall be unique with respect to the issuing Certification Authority.
- The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
- If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
- 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.
- The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID (object identifier) for a FIPS-approved or recommended algorithm.

FDP_TOE_CRL.1 Certificate revocation list validation

FDP_TOE_CRL.1.1 A TSF that issues CRLs shall verify that all mandatory fields in any CRL issued contain values in accordance with ITU-T Recommendation X.509. The following items shall be validated:

- If the version field is present, then it shall contain a 1.
- If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
- If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.
- The signature and signatureAlgorithm fields shall contain the OID (object identifier) for a FIPS-approved digital signature algorithm.
- The thisUpdate field shall indicate the issue date of the CRL.
- The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

FDP_TOE_CSE.1 Certificate status export

FDP_TOE_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with the X.509 standard for CRLs.

FDP_ETC_TOE.5 Extended user private and secret key export

FDP_ETC_TOE.5.1 Private and secret keys shall only be exported from the TOE in encrypted form. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

FDP_ITT.1 Basic internal transfer protection (iteration 1)

FDP_ITT.1.1 The TSF shall enforce the [TOE Access Control Policy specified in FDP_ACC.1] to prevent the [*modification*] of security-relevant user data when it is transmitted between physically-separated parts of the TOE.

Refinement: [Security-relevant user data are the user data apart from user private keys, passwords and authentication codes]

FDP_ITT.1 Basic internal transfer protection (iteration 2)

FDP_ITT.1.1 The TSF shall enforce the [TOE Access Control Policy specified in FDP_ACC.1] to prevent the [*disclosure, modification*] of confidential user data when it is transmitted between physically separated parts of the TOE.

Refinement: [Confidential user data are user private keys, passwords and authentication codes]

FDP_SDI_TOE.3 Stored public key integrity monitoring and action

FDP_SDI_TOE.3.1 Public keys stored within the environment, but not within a FIPS 140-2 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures.

FDP_SDI_TOE.3.2 The digital signature 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.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the [TOE Access Control Policy specified in FDP_ACC.1] to [*transmit*] user data in a manner protected from unauthorised disclosure.

6.1.2.4 Identification and Authentication

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [user identification smartcard, smartcard password, user identifier, asymmetric key pairs and the corresponding certificates in the smartcard issued by the Certification Authority].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [access to the login screen] on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [access to the login screen] on behalf of the user to be performed before the user is identified.

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

FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [user identification smartcard, smartcard password, user identifier, asymmetric key pairs and the corresponding certificates in the smartcard issued by the Certification Authority].

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: [user identifier/smartcard/password validation, user asymmetric key validation].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [user identifier/smartcard/password validation, user asymmetric key validation].

6.1.2.5 Security Management

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [Administrator, Registrar, Auditor creation, authorization, TOE secret keys management, Certificate, CRL profile management, Audit parameters management].

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behavior of*] the functions [listed in Table 6-5] to [the authorized roles as specified in Table 6-5].

Table 6-5 Authorized Roles for Management of Security Functions Behavior

Section/Function	Function/Authorized Role
Security Audit	The capability to configure the audit parameters shall be restricted to Administrators. The capability to change the frequency of the audit log signing event shall be restricted to Administrators.
Certificate Registration	The capability to approve fields or extensions to be included in a certificate shall be restricted to Registrars. If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Registrars.
Data Export and Output	The export of TOE private keys shall require the authorization of at least two Administrators or one Administrator and one Registrar or Auditor.
Certificate Status Change Approval	Only Registrars shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Registrars shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.
TOE Configuration	The capability to configure any TSF functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)
Security Management	The capability to modify the certificate profile shall be restricted to Administrators. The capability to modify the certificate revocation list profile shall be restricted to Administrators.
Revocation Profile Management	The capability to modify the revocation profile shall be restricted to Administrators.

FMT_MOF_TOE.3 Extended certificate profile management

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

FMT_MOF_TOE.3.2 The TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

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

FMT_MOF_TOE.3.3 The TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions in the X.509 public key certificates:

- keyUsage;
- basicConstraints;
- certificatePolicies

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

FMT_MOF_TOE.5 Extended certificate revocation list profile management

FMT_MOF_TOE.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_TOE.5.2 If the TSF issues CRLs, the TSF shall require the Administrator to specify the set of acceptable values for the following fields and extensions:

- issuer;
- nextUpdate (i.e., lifetime of a CRL).

FMT_MOF_TOE.5.3 If the TSF issues CRLs, the Administrator shall specify the acceptable set of CRL and CRL entry extensions.

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [TOE Access Control Policy specified in FDP_ACC.1] to restrict the ability to [*modify*] the security attributes [Role assignment for users and access control privileges for objects] to [Administrators].

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [TOE Access Control Policy specified in FDP_ACC.1] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [*query*] the [audit logs] to [Auditors].

FMT_MTD_TOE.5 TSF secret key confidentiality protection

FMT_MTD_TOE.5.1 TSF secret keys stored by the TOE shall be stored in encrypted form. The encryption shall be performed by NIST approved algorithms.

FMT_MTD_TOE.7 Extended TSF private and secret key export

FMT_MTD_TOE.7.1 Private and secret keys shall only be exported from the TOE in encrypted form.

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: [Administrator, Auditor and Registrar].

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 is authorized to assume both an Administrator and an Registrar role;
- no identity is authorized to assume both an Auditor and an Registrar role; and
- no identity is authorized to assume both an Administrator and an Auditor role] are satisfied.

6.1.2.6 Protection of the TSF

FPT_TOE_TSP.1 Audit log signing event

FPT_TOE_TSP.1.1 The TSF shall create an audit log signing event in which it computes keyed hash over the entries in the audit log.

FPT_TOE_TSP.1.2 The keyed hash shall be computed over, at least, every entry that has been added to the audit log since the previous audit log signing event and the keyed hash from the previous audit log signed event.

FPT_TOE_TSP.1.3 The keyed hash from the audit log signing event shall be included in the audit log.

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1)

FPT_ITT.1.1 The TSF shall protect security-relevant TSF data from [*modification*] when it is transmitted between separate parts of the TOE.

Refinement: [Security-relevant user data are the user data apart from user private keys, passwords and authentication codes]

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 2)

FPT_ITT.1.1 The TSF shall protect confidential TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

Refinement: [Confidential user data are user private keys, passwords and authentication codes]

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.

Table 6-6 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists 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 6-6 Assurance Requirements

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

6.3 Security Requirements Rationale

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

6.3.1 Security Functional Requirements Rationale

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 is covered by at least one security requirement. The first table in this section, Table 6-7, addresses the mapping of security functional requirements to security objectives. The second table, Table 6-10, addresses the mapping of security assurance requirements to security objectives.

Table 6-7 Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
FAU_GEN.1 Audit data generation	O.Individual accountability and audit records
FAU_GEN.2 User identity	O.Individual accountability and audit records
FAU_SEL.1 Selective audit	O.Individual accountability and audit records
FAU_STG.1 Protected audit trail	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss	O.Respond to possible loss of stored audit records.
FCO_NRO_TOE.3 Enforced proof of origin and verification of origin	O.Non-repudiation, O.Control unknown source communication traffic
FCO_NRO_TOE.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM.1 Cryptographic key generation	OE.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction	OE.React to detected attacks
FCS_COP.1 Cryptographic operation	OE.Cryptographic functions
FDP_ACC.1 Subset access control	O.Limitation of administrative access
FDP_ACF.1 Security attribute based access control	O.Limitation of administrative access
FDP_ACF_TOE.2 User private key confidentiality protection	O.Certificates
FDP_TOE_CER.1 Certificate Generation	O.Certificates
FDP_TOE_CRL.1 Certificate revocation list validation	O.Certificates
FDP_TOE_CSE.1 Certificate status export	O.Certificates
FDP_ETC_TOE.5 Extended user private and secret key export	O.Data import/export
FDP_ITT.1 Basic internal transfer protection	O.Integrity protection of user data and software,

Functional Requirement	Objective
(iteration 1)	O.Protect user and TSF data during internal transfer
FDP_ITT.1 Basic internal transfer protection (iteration 2)	O.Protect user and TSF data during internal transfer
FDP_SDI_TOE.3 Stored public key integrity monitoring and action	O.Integrity protection of user data and software
FDP_UCT.1 Basic data exchange confidentiality	O.Data import/export
FIA_ATD.1 User attribute definition	O.Maintain user attributes
FIA_UAU.1 Timing of authentication	O.Limitation of administrative access, O.Restrict actions before authentication
FIA_UID.1 Timing of identification	O.Individual accountability and audit records, O.Limitation of administrative access
FIA_USB.1 User-subject binding	O.Maintain user attributes
FMT_MOF.1 Management of security functions behavior	O.Manage behavior of security functions, O.Security-relavant configuration management
FMT_MOF_TOE.3 Extended certificate profile management	O.Security-relevant configuration management
FMT_MOF_TOE.5 Extended certificate revocation list profile management	O.Security-relevant configuration management
FMT_MSA.1 Management of security attributes	O.Maintain user attributes, O.User authorization management
FMT_MSA.3 Static attribute initialisation	O.Security-relavant configuration management
FMT_MTD.1 Management of TSF data	O.Individual accountability and audit records, O.Protect stored audit records
FMT_MTD_TOE.5 TSF secret key confidentiality protection	O.Integrity protection of user data and software
FMT_MTD_TOE.7 Extended TSF private and secret key export	O.Data import/export
FMT_SMF.1 Specification of Management Functions	O.Manage behavior of security functions
FMT_SMR.2 Restrictions on security roles	O.Security Roles
FPT_TOE_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_ITC.1 Inter-TSF confidentiality during transmission	O.Data import/export
FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1-2)	O.Protect user and TSF data during internal transfer
FPT_STM.1 Reliable time stamps	OE. Time stamps
FTP_TRP.1 Trusted path	OE.Trusted Path

6.3.1.1 Security Functional Requirements Sufficiency

6.3.1.1.1 Security Objectives for the TOE

O.Certificates is provided by **FDP_TOE_CER.1 (Certificate Generation)** which ensures that certificates are valid, **FDP_TOE_CRL.1 (Certificate revocation list validation)** and **FDP_TOE_CSE.1 (Certificate status export)** which ensure that certificate revocation lists and certificate status information are

valid. **FDP_ACF_TOE.2 (User private key confidentiality protection)** ensures that the certificate is not invalidated by the disclosure of the private key by the TOE.

O.Limitation of administrative access is provided by **FDP_ACC.1 (Subset access control), FDP_ACF.1 (Security attribute based access control), FIA_UAU.1 (Timing of authentication)**, and **FIA_UID.1 (Timing of identification). FIA_UAU.1 (Timing of authentication)** and **FIA_UID.1 (Timing of identification)** ensure that Administrators, Registrars, and Auditors can not perform any security-relevant operations until they have been identified and authenticated and **FDP_ACC.1 (Subset access control)** and **FDP_ACF.1 (Security attribute based access control)** ensure that Administrators, Registrars, and Auditors can only perform those operations necessary to perform their jobs.

O.Maintain user attributes is provided by **FIA_ATD.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' behalves. Also **O.Maintain user attributes** is provided by **FMT_MSA.1 (Management of security attributes)** which ensures that only authorized users can modify security attributes.

O.Manage behavior of security functions is provided by **FMT_SMF.1 (Specification of Management Functions)** which specifies the security mechanisms and **FMT_MOF.1 (Management of security functions behavior)** which covers the requirement that authorized users be able to configure, operate, and maintain the specified security mechanisms.

O.Restrict actions before authentication is provided by **FIA_UAU.1 (Timing of authentication)** which covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.

O.Individual accountability and audit records is provided by a combination of requirements. **FIA_UID.1 (Timing of identification)** covers the requirement that users be identified before performing any security-relevant operations. **FAU_GEN.1 (Audit data generation)** and **FAU_SEL.1 (Selective audit)** cover the requirement that security-relevant events be audited while **FAU_GEN.2 (User identity association)** covers the requirement that the identities of the entities responsible for the actions are recorded in the audit records. **FMT_MTD.1 (Management of TSF data)** covers the requirement that audit data be available for review by ensuring that users, other than Auditors, cannot delete audit logs.

O.Integrity protection of user data and software is provided by **FDP_ITT.1 (Basic internal transfer protection) (iteration 1)** and **FDP_SDI_TOE.3 (Stored public key integrity monitoring and action)** which cover the

requirement that user data be protected, **FMT_MTD_TOE.5 (TSF secret key confidentiality protection)** is required to protect the confidentiality of the secret keys used to protect the data.

O.Protect stored audit records is provided by **FAU_STG.1 (Protected audit trail storage)** which covers the requirement that audit records be protected against modification or unauthorized deletion and **FMT_MTD.1 (Management of TSF data)** which covers the requirement that audit records be protected from unauthorized access. **FPT_TOE_TSP.1 (Audit log signing event)** is required so that modifications to the audit logs can be detected.

O.Protect user and TSF data during internal transfer is provided by **FDP_ITT.1 (Basic internal transfer protection) (iteration 1-2)** which covers the requirement that user data be protected during internal transfer and **FPT_ITT.1 (Basic internal TSF data transfer protection) (iteration 1-2)** which covers the requirement that TSF data be protected during internal transfer.

O.Respond to possible loss of stored audit records is provided by **FAU_STG.4 (Prevention of audit data loss)** which covers the requirement that no auditable events, except those taken by the Auditor, can be performed when audit trail storage is full.

O.Data import/export is provided by **FDP_UCT.1 (Basic data exchange confidentiality)** and **FPT_ITC.1 (Inter-TSF confidentiality during transmission)** which cover the requirement that data other than private and secret keys be protected when they are transmitted and from the **FDP_ETC_TOE.5 (Extended user private and secret key export)**, and **FMT_MTD_TOE.7 (Extended TSF private and secret key export)** cover the requirement that private and secret keys be protected when they are transmitted to and from the TOE.

O.User authorization management is provided by **FMT_MSA.1 (Management of security attributes)** which covers the requirement that Administrators manage and update user's security attributes.

O.Security Roles is provided by **FMT_SMR.2 (Restrictions on security roles)** which covers the requirement that a set of security roles be maintained and that users be associated with those roles.

O.Security-relavant configuration management is provided by **FMT_MSA.3 (Static attribute initialisation)** which covers the requirement that security attributes have secure values. **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. **FMT_MOF_TOE.3 (Extended certificate profile management)** covers the requirement that Administrators be able to control the types of information that are included in

generated certificates. **FMT_MOF_TOE.5 (Extended certificate revocation list profile management)** covers the requirement that Administrators be able to control to the types of information that are included in generated certificate revocation lists.

O.Control unknown source communication traffic is provided by **FCO_NRO_TOE.3 (Enforced proof of origin and verification of origin)** which covers the requirement that the TOE discard messages from an unknown source that contain security-relevant information.

O.Non-repudiation is provided by FCO_NRO_TOE.3 (Enforced proof of origin and verification of origin) which covers the requirement that messages containing security-relevant data are not accepted by the TOE unless they contain evidence of origin and **FCO_NRO_TOE.4 (Advanced verification of origin)** which covers the requirement that digital signatures be used so that the evidence of origin for a message may be verified by a third-party.

6.3.1.1.2 IT Security Objectives for the Environment

OE.Trusted Path is provided by **FTP_TRP.1 (Trusted path)** which covers the requirement that a trusted path between the user and the system be provided.

OE.React to detected attacks is provided by **FCS_CKM.4 (Cryptographic key destruction)** which covers the requirement that the authorized user who detected the attack be able to destroy TOE private keys stored in HSM and the secret/encryption private keys stored in the database in order to prevent the attacker from obtaining copies of these keys**.**

OE.Cryptographic functions is provided by **FCS_CKM.1 (Cryptographic key generation)** and **FCS_COP.1 (Cryptographic operation)** which cover the requirement that approved algorithms be used for encryption/decryption, authentication and signature generation/verification and that approved key generation techniques be used.

OE.Time Stamps is provided by **FPT_STM.1 (Reliable time stamps)** which covers the requirement that the time stamps be reliable.

6.3.1.2 Rationale that Dependencies are Satisfied

The selected security requirements include related dependencies, both direct and indirect. The indirect dependencies are those required by the direct dependencies. All of these dependencies must be met or their exclusion justified.

Table 6-8 and 6-9 below provides a summary of the security functional requirements dependency analysis.

Table 6-8 Summary of IT Environment Security Functional Requirements Dependencies

Component	Dependencies	Which is:
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.4 Cryptographic key destruction	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.1 Included
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	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.1 included
FPT_STM.1 Reliable time stamps	None	-
FTP_TRP.1 Trusted path	None	-

Table 6-9 Summary of TOE Security Functional Requirements Dependencies

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	FPT_STM.1 is included as an IT Environment requirement
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_TOE.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification Included	Included
FCO_NRO_TOE.4 Advanced verification of origin	FCO_NRO_TOE.3	Included
FDP_ACC.1 Subset access	FDP_ACF.1 Security attribute based access	Included

Component	Dependencies	Which is:
control	control	
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_TOE.2 User private key confidentiality protection	None	-
FDP_TOE_CER.1 Certificate Generation	None	-
FDP_TOE_CRL.1 Certificate revocation list validation	None	-
FDP_TOE_CSE.1 Certificate status export	None	-
FDP_ETC_TOE.5 Extended user private and secret key export	None	-
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_TOE.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path	FTP_TRP.1 is included as an IT environment requirement
FIA_ATD.1 User attribute definition	None	-
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	-
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_SMF.1 Specification of Management Functions	None	-
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
	FMT_SMF.1 Specification of Management Functions	Included
FMT_MOF_TOE.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_TOE.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
	FMT_SMF.1 Specification of Management	Included

Component	Dependencies	Which is:
	Functions	
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
	FMT_SMF.1 Specification of Management Functions	Included
FMT_MTD_TOE.5 TSF secret key confidentiality protection	None	-
FMT_MTD_TOE.7 Extended TSF private and secret key export	None	-
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_TOE_TSP.1 Audit log signing event	FAU_GEN.1 Audit data generation	Included
	FMT_MOF.1 Management of security functions behavior	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	-
FPT_ITT.1 Basic internal TSF data transfer protection	None	-

6.3.2 Assurance Measures Rationale

This part of the ST rationale is to show that the identified assurance measures are appropriate to meet the assurance requirements. This is best demonstrated in the form of a table, mapping the identified assurance measures onto the assurance requirements, as shown below in Table 6-10.

In this case, the specification of assurance measures is done by reference to the appropriate document. Rationale is provided to show that the referenced document (assurance measure) meets the requirements of the associated assurance requirement.

Table 6-10 Assurance measures

CC Assurance Component		Assurance Measure (TOE document)	Rationale
ADV_ARC.1	Security architecture Description	TOE Design Document	The assurance measure addresses the requirement for secure TOE architecture.

CC Assurance Component		Assurance Measure (TOE document)	Rationale
ADV_FSP.4	Complete functional specification	TOE Functional Specification	The assurance measure addresses the requirement for an informal functional specification. A detailed description of the external interfaces and rationale that the TSF is completely represented is provided.
ADV_IMP.1	Implementation representation of the TSF	TOE Source Code	The assurance measure addresses the requirements for providing the implementation representation for a the TSFs.
ADV_TDS.3	Basic modular design	TOE Design Document	The assurance measure addresses the requirement for the design documentation that describes the informal TOE design, subsystem interfaces ,the security functionality provided by each subsystem, modules of the subsytems, including purpose of each module, interrelationship between the modules and module interfaces.
AGD_OPE.1	Operational user guidance	TOE User Guide	The assurance measure addresses the requirement for administration guidance that is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment. It is also adequate to provide users with the required knowledge to securely access the TOE within the environment.
AGD_PRE.1	Preparative procedures	TOE InstallationGuide TOE Operational Environment Installation Guide	The assurance measure addresses the requirement for installation procedures that are adequate to ensure that the user starts the TOE into a secure configuration.
ALC_CMC.4	Production support, acceptance procedures and automation	TOE Configuration Management Plan	The assurance measure describes the automated means by which only authorized changes are made to the TOE implementation and addresses the requirements for automatic generation of the TOE and automated tools used in the CM system. TOE releases are adequately identified with the version number. All Configuration Items (CI's) that comprise the TOE are under Configuration Management and are included on a CI List. The CM system is effective at ensuring that only authorized changes are made to CI's. The CM system generates records that will demonstrate that the CM system is used and include an acceptance plan.
ALC_CMS.4	Problem tracking CM coverage	TOE Configuration Management Plan	The assurance measure addresses the documentation required to be under configuration control and describes the problem tracking system.
ALC_DEL.1	Delivery procedures	TOE Delivery Procedures	The assurance measure addresses the requirement for secure delivery of the TOE. Secure delivery refers to tamper-evident delivery and detection of modification.

CC Assurance Component		Assurance Measure (TOE document)	Rationale
ALC_DVS.1	Identification of security measures	TOE Development Environment Security and Development Tools	The assurance measure addresses the requirement for site development security procedures.
ALC_FLR.2	Flaw Reporting Procedures	TOE Flaw Remediaton Consumer Guide TOE Flaw Remediation Procedure	The assurance measure addresses the requirement for flaw reporting and correction procedures.
ALC_LCD.1	Developer defined life-cycle model	TOE Life Cycle Model	This assurance addresses the requirements for life-cycle model used in the development and maintenance of the TOE.
ALC_TAT.1	Well-defined development tools	TOE Development Environment Security and Development Tools	This assurance measure addresses the requirements for definition of development tools and configuration used for the TOE.
ASE_CCL.1	Conformance claims	ESYA Security Target	This assurance measure addresses the requirements for conformance claims of the security target for the TOE.
ASE_ECD.1	Extended components definition	TOE Security Target	This assurance measure addresses the extended functional requirements for the TOE and its environment.
ASE_INT.1	ST introduction	TOE Security Target	This assurance measure addresses the requirements for the security target introduction
ASE_OBJ.2	Security objectives	TOE Security Target	This assurance measure addresses the security objectives for the TOE and its environment.
ASE_REQ.2	Derived security requirements	TOE Security Target	This assurance measure addresses the derived security requirements for the TOE and its environment.
ASE_SPD.1	Security problem definition	TOE Security Target	This assurance measure addresses the requirements for the security problem definition of the TOE.
ASE_TSS.1	TOE summary specification	TOE Security Target	This assurance measure addresses the TOE summary specification.
ATE_COV.2	Analysis of coverage	TOE Test Coverage	The assurance measure addresses the requirement for analysis that demonstrates that the TOE was tested to the Functional Specification documentation.
ATE_DPT.1	Testing: basic design	TOE Test Depth	The assurance measure addresses the requirement for analysis that demonstrates that the TOE was tested to the TOE design documentation.
ATE_FUN.1	Functional testing	TOE Test Documents	The assurance measure addresses the requirement for test documentation produced by the TOE developer.
ATE_IND.2	Independent testing – Sample	None	Evaluator action.

CC Assurance Component		Assurance Measure (TOE document)	Rationale
AVA_VAN.3	Focused vulnerability analysis	None	Evaluator action.

7 TOE SUMMARY SPECIFICATION

7.1 IT Security Functions

This section describes the IT security functions provided by TOE to meet the SFRs specified for the TOE in Section 6.1.2. Each security function described in this section contributes to meeting one or several SFRs. A mapping of security functions and SFRs can be found at following security functions section.

7.1.1 Security Audit

7.1.1.1 Audit Data Generation

TOE provides the capability to define new or exclude audit events through Administration Center, but definition of new audit events, requires software changes in the TOE. The TOE records all the auditable events to the database whenever it starts up until shut down. Log number, event accomplishment status, log date, log description, application name, log signature date, accountable person and log signature information are stored in the database. TOE audits all the events specified in Table 7-1.

Table 7-1 Audited events

Event	TOE Functional Specification
Any changes to the audit parameters, e.g., audit frequency, type of event audited.	Audit events can be configurable from the Administration Center. But these changes are recorded as audit records.
Any attempt to delete the audit log.	There's no interface to delete audit log.
Audit log signing event	A symmetric signature is created for each of the audit event.
All security-relevant data that is entered in the system	TOE generates an audit event for each entry of security-relevant data.
All security-relevant messages that are received by the system	TOE generates an audit event for any receipt of security-relevant messages including certificate request, key update request, cross-certification request and error messages.
All successful and unsuccessful requests for confidential and security relevant information	As above.
Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	Cryptographic key generation is not audited in TOE.
The loading of Component private keys	It is not applicable in TOE.

Event	TOE Functional Specification
All access to certificate subject private keys retained within the TOE for key recovery purposes	TOE generates an audit event for any key recovery.
All changes to the trusted public keys, including additions and deletions	There are no defined trusted public keys in TOE.
The manual entry of secret keys used for authentication (Security Levels 3 and 4)	It is not applicable in TOE
The export of private and secret keys (keys used for a single session or message are excluded)	TOE exports private keys during encryption key recovery which is audited.
All certificate requests	TOE generates an audit event for all certificate requests.
All requests to change the status of a certificate.	TOE generates an audit event for all requests to revoke, place on hold, remove from hold certificates.
Any security-relevant changes to the configuration of the TSF	TOE generates an audit event for any security-relevant changes to the configuration of the TSF
All changes to the certificate profile	TOE generates an audit event for any changes to the certificate profile.
All changes to the revocation profile	TOE generates an audit event for any changes to the revocation profile
All changes to the certificate revocation list profile	TOE generates an audit event for any changes to the revocation list profile.

This security function addresses the following SFR: FAU_GEN.1

7.1.1.2 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

7.1.1.3 Audit Data Selection

In Administration Center the auditable events can be included or excluded from the set of audited events.

This security function addresses the following SFR: FAU_SEL.1

7.1.1.4 Audit Data Protection

TOE stores all audit entries in database. Each entry contains log number, event accomplishment status, log date, log description, application name, log signature date, accountable person and log signature information. A keyed message authentication code is created on the appended values of the entry, so that the

integrity of the entry is provided. In addition, the exact number of rows in the signed tables is maintained in another table.

Since the integrity of the audit log entry in the audit table, and the integrity of the whole audit table is provided, the audit logs are protected against unauthorized modification and deletion. It addresses the following SFR : FAU_STG.1

The integrity of the audit logs are provided by keyed hash, the hash is generated in every log creation and the hash is also included in the audit log. This security function addresses the following SFR: FPT_TOE_TSP.1

7.1.1.5 Prevention of Audit Data Loss

Before starting an audited event, the row in the audit database table is reserved so that it is guaranteed that the log for the event can be stored. If the reservation is not possible due to the insufficient disk space or database problem, then the TOE does not execute the event.

This security function addresses the following SFR: FAU_STG.4

7.1.1.6 Query of Audit Logs

The audit logs can be queried from Administration Center only by Auditors.

This security function addresses the following SFR: FMT_MTD.1

7.1.2 Roles

7.1.2.1 Role Definition

Administrator, Registrar, Auditor are the roles defined in TOE. These roles are defined in detail below.

- **Administrator** administrates Certification Authority Services and Administration Center. They use smartcards which contain signature, encryption key pairs and the corresponding administrator certificates issued by the CA in order to logon the aforementioned applications. Minimum two administrators have to be defined during the setup of TOE: After setup, new administrators can be created, or existing administrators deactivated using the Administration Center with the approval of other administrators. Administrators can also create, deactivate Registrars and Auditors. They are responsible for administration of Certification Authority Services. They may modify the directory content.

- **Registrar** can be defined by the Administrators from the Administration Center. Registrars register and manage the end user information through the Registration Authority application. They create requests to the Certification Authority Services for issuing or revoking certificates. They may view the directory content.

- **Auditor** can be defined by the Administrators from the Administration Center. Auditors review the audit logs and create reports using the Administration Center application.

Administrators have no privilege restriction while using CA Services and Administration Center. But some of the operations require the approval of more than one administrator. Auditors have the privilege only to check the audit logs and create reports from the Administration Center. Different set of privileges can be assigned to the Registrars from the Administration Center.

All users are created with their default security attributes in the Administration Center. Registrar security attributes can be overridden by the Administrators. It addresses the SFR : FMT_MSA.3

The above roles are maintained, they are associated with the users and each user can have only one role. It addresses the SFR : FMT_SMR.2.

This security function, in conjunction with the security function Management of security functions behavior described below in Section 7.1.2.2, addresses the following SFR: FMT_MOF.1

7.1.2.2 Management of security functions behavior

Certain operations are only available to certain operators and the role restrictions are described in Table 7-2. This security function, in conjunction with the security function Role Definition described above in Section 7.1.2.1, addresses the following SFR: FMT_MOF.1

Table 7-2 Role Restrictions

Section/Function	Function/Authorized Role
Security Audit	The audited event types can be modified by the Administrators.
Certificate Registration	Adding certificate profiles to the End User Company is restricted to the Administrators. The capability to select the certificate profiles for an end user is restricted to Registrars.
Data Export and Output	The export of TOE private keys is not provided.
Certificate Status Change Approval	Only Registrars are allowed to approve the certificate status change. End Users can also approve the status change through the end user services which is out of TOE boundary.
TOE Configuration	The capability to configure any TSF functionality is restricted to Administrators.
Certificate Profile Management	The capability to modify the certificate profile is restricted to Administrators.
Revocation Profile Management	The capability to modify the certificate profile is restricted to Administrators.
Certificate Revocation List Profile Management	The capability to modify the certificate profile is restricted to Administrators.
Management of Security Attributes	Modifications of security attributes (role assignment for users and access control privileges for objects) and changing the default security attributes is restricted to Administrators

Administrator, Registrar, Auditor creation, authorization, TOE secret keys management, Certificate, CRL profile management, Audit parameters management can be performed by the security functions. It addresses the SFR: FMT_SMF.1

Security attributes can be modified only by the Administrators. It addresses the SFR: FMT_MSA.1

The default security attributes are assigned to the users, and the Administrators can override the default attributes of the Registrars. It addresses the SFR: FMT_MSA.3

7.1.2.3 Seperation of Roles

All users are authorized to assume only the assigned roles. More than one role is not allowed. It addresses the following SFR : FMT_SMR.2

7.1.3 Scope of Policy and Access Rules

Certification Authority Services and Administration Center can be only used by Administrators, and Registration Authority can be only used by Registrars. Auditors can use only the audit related functionality in Administration Center. Registrars can use Registration Authority according to the privileges they are assigned. The privilege assignments to Registrars are managed in Administration Center.

Table 7-3 describes the operations and the related enforcing rules.

Table 7-3 Access Control Rules

Section/Function	Event
Certificate Request Remote and Local Data Entry	The entry of certificate request data is restricted to Registrars.
Certificate Revocation Request Remote and Local Data Entry	The entry of certificate revocation request data is restricted to Registrars.
Data Export and Output	The export or output of confidential and security-relevant data is only at the request of authorized users.
Key Generation	The capability to request the generation of Component keys (used to protect data in more than a single session or message) is restricted to the authorized users.
Private Key Load	The capability to request the loading of Component private keys into cryptographic modules is not provided.
Private Key Storage	The capability to request the decryption of certificate subject private keys is restricted to Registrars. The TSF does not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. The end users decryption private keys are stored in the database in an encrypted form and are not accessible to any administrators. These keys can be requested during a key recovery process initiated by a registrar. The keys are either imported into the end user smartcards or given as PKCS#12 file to the end user. There is no capability provided to decrypt the private keys.
Trusted Public Key Entry, Deletion, and Storage	There's no trusted public key storage provided.
Secret Key Storage	TOE secret keys are created during setup and encrypted with Administrators encryption certificates. The encrypted secret keys are stored in DB. No capability is provided to request the loading of TOE secret keys into cryptographic modules.
Private and Secret Key Destruction	Private keys never leaves cryptographic module and there is no user interface to zeroize them.

Section/Function	Event
Private and Secret Key Export	The capability to export a component private key is not provided. The end users decryption private keys are stored in the database in an encrypted form and are not accessible to any administrators. These keys can be requested during a key recovery process initiated by a registrar. The keys are either imported into the end user smartcards or given as PKCS#12 file to the end user.
Certificate Status Change Approval	Only Registrars and the subject of the certificate are capable of requesting that a certificate be placed on hold. Only Registrars are capable of removing a certificate from on hold status. Only Registrars are capable of approving the placing of a certificate on hold. Only Registrars and the subject of the certificate are capable of requesting the revocation of a certificate. Only Registrars are capable of approving the revocation of a certificate and all information about the revocation of a certificate.

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

Only the authorized roles can manage the security functions behavior. This security function addresses the following SFR: FMT_MOF.1

7.1.4 Identification and Authentication

Administrators, Registrars and Auditors need smartcards in order to login to the aforementioned applications. They have signature and encryption key pairs and the corresponding certificates in the smartcards.

All functions in the TOE require the user to be authenticated as described above before allowing any TOE mediated action. This security function addresses the following SFR: FIA_UAU.1

All functions require the user to be identified before allowing any TOE-mediated action. This security function addresses the following SFR: FIA_UID.1

TOE associates the user identity with subjects acting on behalf of the user. The user identity is authenticated at login and remains associated with subjects acting on behalf of the user as long as the login session is valid. This security function addresses the following SFR: FIA_USB.1

TOE uses user identification smartcard, smartcard password, user identifier, asymmetric key pairs and the corresponding certificates in the smartcard issued by the Certification Authority for identification and authentication of the user. This security function addresses the following SFR: FIA_ATD.1

7.1.5 Remote Data Entry and Export

TOE generates certificates and the revocation status for them. The security of the transmission of this information to the end users depends on the SSL protocol provided by the IT environment.

During the certificate request and the key recovery, CMP protocol is used which enforces mutual authentication and integrity verification. In TOE, no user has direct access rights to the database. The requests are sent by the Registrars from Registration Authority to CA Services.

7.1.5.1 Enforced Proof of Origin and Verification of Origin

The integrity of the information which will be used for generation of a certificate is validated with the table row signature. In the login process of the administrators, registrars and auditors, certificates issued by the CA are used, thus the certificates are validated according to the entries in the trusted database. TOE provides the revocation information by publishing CRLs or giving answers to OCSP request. Integrity, validity and the proof of origin of the certificate status information is provided with the CA signature on the CRLs and OCSP answers.

This security function addresses the following SFR: FCO_NRO_TOE.3

7.1.5.2 Protection of data communications between CA Services and Registration Authority

While TSF transfers security relevant and confidential data between TOE components, CMP is used so that authentication, confidentiality and integrity protection is provided against unauthorized modification and disclosure.

The security of the user data transmitted between the TOE and the outside world is provided with the SSL protocol. TOE Access Control policy is enforced during the transmission.

This security function addresses the following SFRs: FDP_ITT.1 (Iteration 1 and 2) and FPT_ITT.1 (Iteration 1 and 2)

7.1.5.3 Trusted channel

The security of the sensitive data transmitted between the TOE and remote entities are provided with the CMP and SSL protocol. To initate any key management or certificate management transactions a valid authentication code is required. This security function addresses the following SFRs: FPT_ITC.1 and FCO_NRO_TOE.4

Protection against unauthorized disclosure and modification is provided with encryption and digital signatures. This security function addresses the following SFRs: FDP_UCT.1

7.1.6 Certificate Management

7.1.6.1 Certificate Generation

TOE only generates certificates whose format complies with X.509 version 3 consistent with the related certificate profile. Proof of possession is always established before a certificate can be made available to an end-user. TOE ensures that

- SerialNumber is unique;
- notBefore is set to current date and the notAfter value is set current date + validity of the certificate;
- Issuer is set to CA's DN and never contains a null name;
- Subject is set to subject's DN and never contains a null name;

In addition, subjectPublicKeyInfo can be set to contain the OID (object identifier) for FIPS-approved algorithms (RSA/{SHA-1, SHA256, SHA384, SHA512}, ECDSA/{SHA-1, SHA256, SHA384, SHA512}).

This security function addresses the following SFR: FDP_TOE_CER.1

7.1.6.2 Certificate Status Export

TOE publishes Certificate Revocation Lists (CRLs) in a format that complies with X.509v2.

This security function addresses the following SFR: FDP_TOE_CSE.1

7.1.6.3 Certificate Profile Management

Using TOE certificate profiles only certificates which comply with X.509 version 3 can be generated. The certificate profiles are stored in the database, and new profiles can be created by the Administrators. This security function addresses the following SFRs: FMT_MOF_TOE.3, FMT_SMF.1

The user private keys are stored in the database if their certificate profile is created accordingly. This security function addresses the following SFR: FDP_ACF_TOE.2

7.1.7 Certificate Revocation

7.1.7.1 CRL Profile Management

Using TOE CRL profiles only CRLs which comply with X.509 version 2 can be generated. The CRL profiles are stored in the database, and new profiles can be created by the Administrators.

This security function addresses the following SFR: FMT_MOF_TOE.5

7.1.7.2 CRL Validation

CRLs issued by TOE are compliant with X.509 version 2. **Issuer** is never set to null and set to CA's DN. **subjectPublicKeyInfo** can be set to contain the OID (object identifier) for FIPS-approved algorithms (RSA/{SHA-1, SHA256, SHA384, SHA512}, ECDSA/{SHA-1, SHA256, SHA384, SHA512}). **thisUpdate** indicates the issue date of the CRL, **nextUpdate** is always after **thisUpdate**.

This security function addresses the following SFR: FDP_TOE_CRL.1

7.1.8 Key Management

7.1.8.1 Private Key Protection

Only end user encryption certificates private keys are stored on demand. These keys are stored in the database in a FIPS approved encrypted form. The encryption is performed by the cryptographic module. These keys are exported to end user with CMP protocol. This security function addresses the following SFRs: FDP_ACF_TOE.2 and FDP_ETC_TOE.5.

TOE secret keys are stored in database in an encrypted form. The encryption is performed by the cryptographic module. This security function addresses the following SFRs: FMT_SMF.1, FMT_MTD_TOE.5.

TOE triggers cryptographic modules (hardware and software) to perform all cryptographic operations. In the cryptographic modules TOE private and secret key export is not allowed. This security function addresses the following SFR: FMT_MTD_TOE.7.

7.1.8.2 Public Key Protection

TOE does not store end user public keys, but certificates. The user certificates are digitally signed which protects the exported public keys against unauthorized modifications.

This security function addresses the following SFRs: FDP_SDI_TOE.3, FMT_SMF.1