TÜBİTAK BİLGEM UEKAE
ULUSAL ELEKTRONİK VE KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

KRİPTOLOJİ UYGULAMALARI
G030 - Anahtar Yönetim Sistemleri ve MA3 Birimi

ELEKTRONİK SERTİFİKA YÖNETİM ALTYAPISI(ESYA) V2.0

(ELECTRONIC CERTIFICATE MANAGEMENT INFRASTRUCTURE)

SECURITY TARGET

Revision No	1.6
Revision Date	13.08.2015
Document Code	ESYA2.0-ST
File Name	ESYA V2.0SECURITYTARGET ENGLISH.DOC
Prepared by	
DindarÖZ,*Chief Researcher* Mehmet BERBER, *Senior Researcher*	
Validated by	
MA3 ProjectManager,*Chief Researcher*	Murat YasinKUBİLAY

REVISION HISTORY

RevisionNo	Revision Reason	Revision Date
1.0	First release	17.09.2013
1.1	Revision made according to “GÖZLEM RAPORU(GR) – 1”	10.10.2013
1.2	Some corrections on sections 6.1 and 7; format changes	11.10.2013
1.3	Revision made according to “GÖZLEM RAPORU(GR) – 2”	23.10.2013
1.4	Revision made according to “GÖZLEM RAPORU(GR) – 3”	05.11.2013
1.5	Section 7.1.1.6 revised, Roles Operator and Officer changed with Registrar	14.03.2014
1.6	Spelling corrections, English naming of TOE Identification added and Figure 1 changed	13.08.2015

CONTENT

LIST OF FIGURES

LIST OF TABLES

1 SECURITY TARGET INTRODUCTION

1.1 ST Reference

ST Title: Elektronik Sertifika Yönetim Altyapısı (ESYA) v 2.0 (Electronic Certificate Management Infrastructure v2.0) Security Target Revision 1.6, 13August2015

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.

1.2 TOE Reference

TOE Identification: Elektronik Sertifika Yönetim Altyapısı (ESYA) v2.0(Electronic Certificate Management Infrastructure v2.0)

1.3 TOE Overview

ESYA v2.0(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;
    - TOE does not store end user public keys, but certificates are digitally signed to protect the exported public keys against unauthorized modifications;
    - Only end user encryption certificates private keys are stored on demand. These keys are stored in the database in a FIPS approved encrypted form which is performed by the hardware cryptographic module;
    - TOE secret keys are stored in the database in an encrypted form which is performed by the soft cryptographic module;
- 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 Functionsunless 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 and audit logs;
    - Protection against unauthorized disclosure and modification is provided with encryption and digital signatures;
    - The TOE relies on the system clock of the host for a reliable time stamp. A date/time stamp is included and associated with each audit entry;
    - 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.
- The data transmitted between the TOE and remote users are protected against modification and disclosure.

1.4 TOE Description

ESYA v2.0(TOE) is an X.509 certificate generation and management system software. TOEand 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.

TOEcan 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. TOEand its operational environmentprovides 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 registrarscertificates 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.

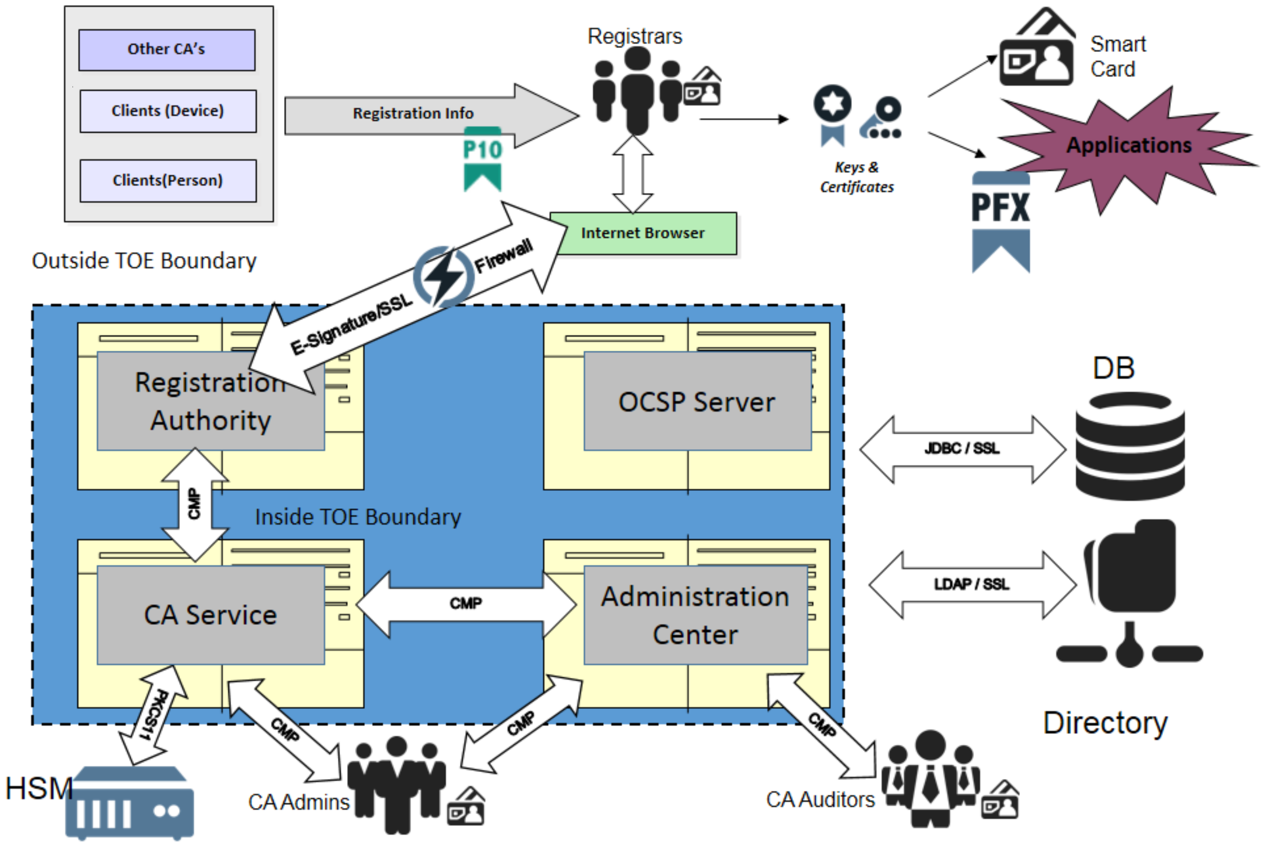
1.4.1 TOE Boundary

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

- Certification Authority Services
- Administration Center
- Registration Authority
- OCSP Server

Note: 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.

1.4.1.4 OCSP(Online Certificate Status Protocol) Server

OCSP Server generates BasicOCSP responses compliant to RFC 2560 in order to give the online certificate status. OCSP Server uses the database as the certificate status source, so that the freshest certificate status can be queried.

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.

- HMACkey for DB table row signature
- Directory users passwords
- 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 byTOE 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 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 2008 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, Administration Center, Registration Authority**
  - Windows 2003 R2 Service Pack 2 x86/x64Pentium III 800 MHz processor
  - 1GB 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 security modules must be used for the following cryptographic functions usedby the TOE.

- Key Generation
- Certificate Signing
- CRL Signing
- Key Wrap/Unwrap

1.4.2.5.2 Software Cryptographic Module

The following cryptographic functions are performed in aFIPS 140-2 level 2 validated software cryptographic module(Network Security Services – NSS version 3.12.4).This module is bundled with the TOE software but it's not a part of the TOE.

- Short term key generation
- Asymmetic Encryption
- Signature Verification
- Key wrap/unwrap
- 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 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended.

- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012, conformant.

2.2 PP Claim

In this ST, TOE claims conformance to the following protection profile.

Certificate Issuing and Management Components (CIMC) Protection Profile, version 1.5, August 11, 2011.

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

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 1Organizational Security Policies

POLICY NAME	DESCRIPTION
P.Authorized use of information	Information shall be used only for its authorized purpose(s).
P.Cryptography and secure storage of cryptographic assets	FIPS-approved or NIST-recommended cryptographic functionsshall be used to perform all cryptographic operations.

3.2 Assumptions

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

3.2.1 Personnel Assumptions

Table 2Assumptions

ASSUMPTION NAME	DESCRIPTION
A.Auditors Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Auditors.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change theirauthentication data at appropriate intervals and to appropriate values (e.g., proper lengths,histories, variations, etc.) (Note: this assumption is not applicable to biometricauthentication data.)
A.Competent Administrators, Registrars and Auditors	Competent Administrators, Registrars and Auditors will be assigned to managethe TOE and the security of the information it contains.

ASSUMPTION NAME	DESCRIPTION
A.Cooperative Users	Users need to accomplish some task or group of tasks that require a secure ITenvironment. The users require access to at least some of the information managed by theTOE and are expected to act in a cooperative manner.
A.CPS	All Administrators, Registrars, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
A.Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity. TOE assumes that codes signed by any trusted entity is not malicious.
A.Notify Authorities of Security Issues	Administrators, Registrars, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Social Engineering Training	General users, administrators, registrarsand auditors are trained in techniques to thwart social engineering attacks.

3.2.2 Connectivity

ASSUMPTION NAME	DESCRIPTION
A.Operating System	The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats identified in this ST.

3.2.3 Physical

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

3.3 Threats

The threats are organized in fourcategories:

- Authorized Users
- System
- Cryptography
- External Attacks

3.3.1 Authorized Users

Table 3Authorized Users

THREAT NAME	DESCRIPTION
T.Administrative errors of omission	Administrators, Registrars or Auditors fail to perform some function essential to security.
T.Administrators, Registrarsand Auditors commit errors or hostile actions	An Administrator, Registraror Auditor commits errors that change the intendedsecurity policy of the system or application or maliciously modify the system'sconfiguration to allow security violations to occur.
T.User abuses authorization to collect and/or send data	User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.
T.User error makes data inaccessible	User accidentally deletes user data rendering user data inaccessible.

3.3.2 System

Table 4 System

THREAT NAME	DESCRIPTION
T.Critical system component fails	Failure of one or more system components results in the loss of system criticalfunctionality. Threat agent in this case is the CIMC hardware. Adverse action can becompromise of the security of the CIMC and/or relying party systems that rely on thePKI objects such as certificates, CRLs, or OCSP Responses.
T.Flawed code	A system or applications developer delivers code that does not perform according tospecifications or contains security flaws. Threat agent in this case is the TOE developer.Adverse action can be compromise of the security of the CIMC and/or relying partysystems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

T.Malicious code exploitation	An authorized user, IT system, or hacker downloads and executes malicious code, whichcauses abnormal processes that violate the integrity, availability, or confidentiality of thesystem assets. Threat agent could be an authorized user, TOE itself, or an unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relyingparty systems that rely on the PKI objects such as certificates, CRLs, or OCSPResponses.
T.Message content modification	A hacker modifies information that is intercepted from a communications link betweentwo unsuspecting entities before passing it on to the intended recipient. Threat agent isan unauthorized user. Adverse action can be compromise of the security of the CIMCand/or relying party systems that rely on the PKI objects such as certificates, CRLs, orOCSP Responses.

3.3.3 Cryptography

Table 5 Cryptography

THREAT NAME	DESCRIPTION
T.Disclosure of private and secret keys	A private or secret key is improperly disclosed. Threat agent is the authorized user or erroneous protocol. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Modification of private/secret keys	A secret/private key is modified. Threat agent is the authorized user or erroneousprotocol. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSPResponses.
T.Sender denies sending information	The sender of a message denies sending the message to avoid accountability for sendingthe message and for subsequent action or inaction. Threat agent is a subscriber toCIMC. Adverse action can be reduced trust in CIMC.

3.3.4 External Attacks

Table 6 External Attacks

THREAT NAME	DESCRIPTION
T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributedto the authorized user or a system process or gains undetected access to a system due tomissing, weak and/or incorrectly implemented access control causing potential violationsof integrity, confidentiality, or availability. Threat agent is the unauthorized user.Adverse action can be compromise of the security of the CIMC and/or relying partysystems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Hacker physical access	A hacker physically interacts with the system to exploit vulnerabilities in the physicalenvironment, resulting in arbitrary security compromises. Threat agent is theunauthorized user. Adverse action can be compromise of the security of the CIMCand/or relying party systems that rely on the PKI objects such as certificates, CRLs, orOCSP Responses.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry,system use, system design, or system operation. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying partysystems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses..

4 SECURITY OBJECTIVES

This section includes the security objectives including security objectives for the TOE, security objectives for the environment, and security objectives for both the TOE and environment.

4.1 Security Objectives for the TOE

This section includes the security objectives for the TOE, divided among four categories: authorized users, system,cryptography, and external attacks.

Table 7 Security Objectives for the TOE

Authorized Users	
O.Certificates	The TSF must ensure that certificates, certificate revocation lists, and certificate statusinformation are valid.
System	
O.Preservation/trusted recovery of secure state	Preserve the secure state of the system in the event of a secure component failure and/orrecover to a secure state.
Cryptography	
O.Non-repudiation	Prevent user from avoiding accountability for sending a message by providing evidencethat the user sent the message.
External Attacks	
O.Control unknown source communication traffic	Control (e.g., reroute or discard) communication traffic from an unknown source toprevent potential damage.

4.2 Security Objectives for the Environment

This section specifies the security objectives for the environment.

Table 8 Security Objectives for the Environment

O.Administrators, Registrarsand Auditors guidance documentation	Deter Administrator, Registraror Auditor errors by providing adequatedocumentation on securely configuring and operating the CIMC.
O.Auditors Review Audit Logs	Identify and monitor security-relevant events by requiring auditors to review audit logson a frequency sufficient to address level of risk.
O.Authentication Data Management	Ensure that users change their authentication data at appropriate intervals and toappropriate values (e.g., proper lengths, histories, variations, etc.) through

	enforcedauthentication data management (Note: this objective is not applicable to biometricauthentication data.)
O.Communications Protection	Protect the system against a physical attack on the communications capability byproviding adequate physical security.
O.Competent Administrators, Registrarsand Auditors	Provide capable management of the TOE by assigning competent Administrators,Registrarsand Auditors to manage the TOE and the security of the informationit contains.
O.Cooperative Users	Ensure that users are cooperative so that they can accomplish some task or group of tasksthat require a secure IT environment and information managed by the TOE.
O.CPS	All Administrators, Registrarsand Auditors shall be familiar with the certificatepolicy (CP) and the certification practices statement (CPS) under which the TOE isoperated. A Certificate Policy, is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. A Certification Practice Statement (CPS) is a statement of the practices that a CA employs in managing the certificates that it issues. The CPS should describe how the Certificate Policy is interpreted in the context of the system architecture and operating procedures of the organization.
O.Cryptographic functions	The TOE must implement approved cryptographic algorithms for encryption/decryption,authentication, and signature generation/verification; approved key generation techniquesand use validated cryptographic modules. (Validated is defined as FIPS 140-2 validated.)
O.Disposal of Authentication Data	O.Disposal ofAuthentication DataProvide proper disposal of authentication data and associated privileges after access hasbeen removed (e.g., job termination, change in responsibility).
O.Installation	Those responsible for the TOE must ensure that the TOE is delivered, installed,managed, and operated in a manner which maintains IT security.
O.Lifecycle security	Provide tools and techniques used during the development phase to ensure security isdesigned into the CIMC. Detect and resolve flaws during the operational phase.
O.Malicious Code Not Signed	Protect the TOE from malicious code by ensuring all code is signed by a trusted entityprior to loading it into the system.
O.Notify Authorities of Security Issues	Notify proper authorities of any security issues that impact their systems to minimize thepotential for the loss or compromise of data.
O.Operating System	The operating system used is validated to provide adequate security, including domainseparation and non-bypassability, in accordance with security requirementsrecommended by the

	National Institute of Standards and Technology.
O.Periodically check integrity	Provide periodic integrity checks on both system and software.
O.Physical Protection	Those responsible for the TOE must ensure that the security-relevant components of theTOE are protected from physical attack that might compromise IT security.
O.Repair identified security flaws	The vendor repairs security flaws that have been identified by a user.
O.Security roles	Maintain security-relevant roles and the association of users with those roles.
O.Social Engineering Training	Provide training for general users, Administrators, Registrars and Auditors intechniques to thwart social engineering attacks.
O.Sufficient backup storage and effective restoration	Provide sufficient backup storage and effective restoration to ensure that the system canbe recreated.
O.Trusted Path	Provide a trusted path between the user and the system. Provide a trusted path tosecurity-relevant (TSF) data in which both end points have assured identities.
O.Validation of security function	Ensure that security-relevant software, hardware, and firmware are correctly functioningthrough features and procedures.

4.3 Security Objectives for both the TOE and the Environment

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

Table 9Security Objectives for both the TOE and the Environment

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

audit records	responsible for the action.
O.Integrity protection of user data and software	Provide appropriate integrity protection for user data and software.
O.Limitation of administrative access	Design administrative functions so that Administrators, Registrarsand Auditorsdo not automatically have access to user objects, except for necessary exceptions.Control access to the system by Operators and Administrators who troubleshoot thesystem and perform system updates.
O.Maintain user attributes	Maintain a set of security attributes (which may include role membership. accessprivileges, etc.) associated with individual users. This is in addition to user identity.
O.Manage behavior of security functions	Provide management functions to configure, operate, and maintain the securitymechanisms.
O.Object and data recovery free from malicious code	Recover to a viable state after malicious code is introduced and damage occurs. Thatstate must be free from the original malicious code.
O.Procedures for preventing malicious code	Incorporate malicious code prevention procedures and mechanisms.
O.Protect stored audit records	Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.
O.Protect user and TSF data during internal transfer	Ensure the integrity of user and TSF data transferred internally within the system.
O.React to detected attacks	Implement automated notification (or other responses) to the TSF-discovered attacks inan effort to identify attacks and to create an attack deterrent.
O.Require inspection for downloads	Require inspection of downloads/transfers.
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 byrestricting auditable events.
O.Restrict actions before authentication	Restrict the actions a user may perform before the TOE authenticates the identity of theuser.
O.Security-relevant configuration management	Manage and update system security policy data and enforcement functions, and othersecurity-relevant configuration data, to ensure they are consistent with organizationalsecurity policies.
O.Time stamps	Provide time stamps to ensure that the sequencing of events can be verified.
O.User authorization management	Manage and update user authorization and privilege data to ensure they are consistentwith organizational security and personnel policies.

4.4 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, policies, or assumptions.The following tables provide a mapping of security objectives to the environment defined by the threats, policies,and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and thateach threat, policy or assumption is covered by at least one security objective. Table 10 maps security objectives forthe TOE to threats, Table 11 maps security objectives for the environment to threats, and Table 12 maps securityobjectives for both the TOE and the environment to threats. Table 13 maps the organizational security policies tosecurity objectives. Table 14 maps assumptions to IT security objectives, listing which objectives each assumptionhelps to cover. The items in the tables are ordered alphabetically, sorted on the first column.

Table 10Relationship of Security Objectives for the TOE to Threats

IT Security Objective	Threat
O.Certificates	T.Administrators, Registrarsand Auditors commit errors or hostile actions
O.Control unknown source communication traffic	T.Hacker gains access
O.Non-repudiation	T.Sender denies sending information
O.Preservation/trusted recovery of secure state	T.Critical system component fails
O.Sufficient backup storage and effective restoration	T.Critical system component fails, T.User error makes data inaccessible

Table 11Relationship of Security Objectives for the Environment to Threats

Non-IT Security Objective	Threat
O.Administrators, Registrars and Auditors guidance documentation	T.Disclosure of private and secret keys, T.Administrators, Registrarsand Auditorscommit errors or hostile actions, T.Social engineering
O.Competent Administrators, Registrarsand Auditors	T.Administrators, Registrarsand Auditorscommit errors or hostile actions
O.CPS	T.Administrative errors of omission
O.Cryptographic functions	T.Disclosure of private and secret keys, T.Modification of secret/private keys
O.Installation	T.Critical system component fails
O.Lifecycle security	T.Critical system component fails, T.Malicious code exploitation
O.Notify Authorities of Security Issues	T.Hacker gains access
O.Periodically check	T.Malicious code exploitation

integrity	
O.Physical Protection	T.Hacker physical access
O.Repair identified security flaws	T.Flawed code, T.Critical system component fails
O.Security roles	T.Administrators, Registrarsand Auditorscommit errors or hostile actions
O.Social Engineering Training	T.Social Engineering
O.Trusted path	T.Hacker gains access, T.Message content modification
O.Validation of security function	T.Malicious code exploitation, T.Administrators, Registrarsand Auditorscommit errors or hostile actions

Table 12Relationship of Security Objectives for Both the TOE and the Environment to Threats

Non-IT Security Objective	Threat
O.Configuration management	T.Critical system component fails, T.Malicious code exploitation
O.Data import/export	T.Message content modification
O.Detect modifications of firmware, software, and backup data	T.User error makes data inaccessible, T.Administrators, Registrarsand Auditors commit errors or hostile actions
O.Individual accountability and audit records	T.Administrative errors of omission, T.Hacker gains access, T.Administrators, Registrarsand Auditors commit errors or hostile actions, T.User abuses authorization to collect and/or send data
O.Integrity protection of user data and software	T.Modification of private/secret keys, T.Malicious code exploitation
O.Limitation of administrative access	T.Disclosure of secret and private keys, T.Administrators, Registrarsand Auditorscommit errors or hostile actions
O.Maintain user attributes	T.Administrators, Registrarsand Auditors commit errors or hostile actions
O.Manage behavior of security functions	T.Critical system component fails, T.Administrators, Registrarsand Auditors commit errors or hostile actions
O.Object and data recovery free from malicious code	T.Modification of secret/private keys, T.Malicious code exploitation
O.Procedures for preventing malicious code	T.Malicious code exploitation, T.Social engineering
O.Protect stored audit records	T.Modification of secret/private keys, T.Administrators, Registrarsand Auditors commit errors or hostile actions

O.Protect user and TSF data during internal transfer	T.Message content modification, T.Disclosure of private and secret keys
O.React to detected attacks	T.Hacker gains access
O.Require inspection for downloads	T.Malicious code exploitation
O.Respond to possible loss of stored audit records	T.Administrators, Registrarsand Auditors commit errors or hostile actions
O.Restrict actions before authentication	T.Hacker gains access, T.Administrators, Registrarsand Auditors commit errors or hostile actions
O.Security-relevant configuration management	T.Administrative errors of omission
O.Time stamps	T.Critical system component fails, T.Administrators, Registrarsand Auditors commit errors or hostile actions

Table 13Relationship of Organizational Security Policies to Security Objectives

Security Policy	Objective
P.Authorized use of information	O.Auditors review audit logs O.Maintain user attributes O.Restrict actions before authentication O.Security roles O.User authorization management
P.Cryptography	O.Cryptographic functions

Table 14Relationship of Assumptions to IT Security Objectives

Assumption	IT Security Objective
A.Auditors Review Audit Logs	O.Auditors Review Audit Logs
A.Authentication Data Management	O.Authentication Data Management
A.Communications Protection	O.Communications Protection
A.Competent Administrators, Registrarsand Auditors	O.Competent Administrators, Registrars and Auditors, O.Installation, O.Security-relevant configuration management, O.User authorization management, O.Configuration Management
A.Cooperative Users	O.Cooperative Users
A.CPS	O.CPS, O.Security-relevant configuration management, O.User authorization management, O.Configuration Management
A.Disposal of Authentication	O.Disposal of Authentication Data

Data	
A.Malicious Code Not Signed	O.Procedures for preventing malicious code, O.Require inspection for downloads, O.Malicious Code Not Signed
A.Notify Authorities of Security Issues	O.Notify Authorities of Security Issues
A.Operating System	O.Operating System
A.Physical Protection	O.Physical Protection
A.Social Engineering Training	O.Social Engineering Training

4.4.1 Security Objectives Sufficiency

The following discussions provide information regarding:

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

4.4.1.1 Threats and Objectives Sufficiency

4.4.1.1.1 Authorized users

T.Administrative errors of omission addresses errors that directly compromise organizational security objectivesor change the technical security policy enforced by the system or application. It is countered by:

> **O.CPS** provides Administrators, Registrars, and Auditors with information regarding the policies andpractices used by the system. Providing this information ensures that these authorized users of the system are awareof their responsibilities, thus reducing the likelihood that they will fail to perform a security-critical operation.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user isuniquely identified so that auditable actions can be traced to a user. Audit records provide information about pastuser behavior to an authorized individual throughsystem mechanisms. These audit records will exposeadministrators that fail to performsecurity-critical operations so they can be held accountable.
>
> **O.Security-relevant configuration management** ensures that system security policy data and enforcementfunctions, and other security-relevant configuration data are managed and updated. This ensures that they areconsistent with organizational security policies and that all changes are properly tracked and implemented.

T.User abuses authorization to collect and/or send data addresses the situation where an authorized user abusesgranted authorizations by browsing files in order to collect data and/or violates export control policy by sending datato a recipient who is not authorized to receive the data.

It is countered by:

O.Individual accountability and audit records provides individual accountability for audited events. Each user isuniquely identified so that auditable actions can be traced to a user. Audit records provide information about pastuser behavior to an authorized individual through system mechanisms. This audit records will expose users whoabuse their authorized to collect and/or send data.

T.User error makes data inaccessible addresses a user accidentally deleting user data. Consequently, the user datais inaccessible. Examples include the following:
User accidentally deletes data by striking the wrong key on the keyboard or by striking the enter key as an automaticresponse.
User does not understand the implications of the prompt at hand and inadvertently gives a response that deletes userdata.
User misunderstands a system command and issues a command that unintentionally deletes user data.
It is countered by:

O.Sufficient backup storage and effective restoration ensures that there is sufficient backup storage and effectiverestoration to recreate the system, when required. This ensures that user data is available from backup, even if thecurrent copy is accidentally deleted.

O.Detect modifications of firmware, software, and backup data ensures that if the backup components have beenmodified, that it is detected. If modifications of backup data can not be detected, the backup copy is not a reliablesource for restoration of user data.

T.Administrators, Registrarsand Auditors commit errors or hostile actions addresses:
Errors committed by administrative personnel that directly compromise organizational security objectives, changethe technical security policy enforced by the system or application, or
Malicious obstruction by administrative personnel of organizational security objectives or modification of thesystem's configuration to allow security violations to occur.
It is countered by:

O.Competent Administrators, Registrarsand Auditors ensures that users are capable of maintainingeffective security practices. This reduces the likelihood that they will commit errors.

O.Administrators, Registrarsand Auditors guidance documentation which deters administrativepersonnel errors by providing adequate guidance.

O.Certificates ensures that certificates, certificate revocation lists, and certificate status information are valid. Thevalidation of information provided by Registrarsthat is to be included in certificates helps to prevent improperlyentered information from appearing in certificates.

O.Detect modifications of firmware, software, and backup data ensures that if the backup components have beenmodified, that it is detected.

O.Individual accountability and audit records provides individual accountability for audited events. Each user isuniquely identified so that auditable actions can be traced to a user. Audit records provide information about pastuser behavior to an authorized individual through system mechanisms. These audit records will exposeadministrators that perform inappropriate operations so they can be held accountable.

O.Limitation of administrative access. The administrative functions are designed in such a way that administrativepersonnel do not automatically have access to user objects, except for necessary exceptions. In general, theexceptions tend to be role specific. Limiting the set of operations that a user may perform limits the damage that auser may cause.

O.Maintain user attributes. Maintains a set of security attributes (which may include group membership, accessrights, etc.) associated with individual users in addition to user identity. This prevents users from performingoperations that they are not authorized to perform.

O.Manage behavior of security functions provides management controls/functions for security mechanisms. Thisensures that security mechanisms which protect against hostile users are properly configured.

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.Respond to possible loss of stored audit records ensures that only auditable events executed by the Auditorshall be audited if the audit trail is full. This ensures that operations that are performed by users other than theAuditor are audited and so can be detected.

O.Restrict actions before authentication ensures that only a limited set of actions may be performed before a useris authenticated.

O.Security roles ensures that security-relevant roles are specified and that users are assigned to one (or more) of thedefined roles. This prevents users from performing operations that they are not authorized to perform.

O.Time stamps ensures that time stamps are provided to verify a sequence of events. This allows the reconstructionof a timeline of events when performing an audit review.

O.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctlyfunctioning through features and procedures such as underlying machine testing and integrity checks.

4.4.1.1.2 System

T.Critical system component fails addresses the failure of one or more system components that results in the lossof system-critical functionality. This threat is relevant when there are components that may faildue to hardwareand/or software imperfections and the availability of system functionality is important.

It is countered by:

O.Configuration management assures that a configuration management program is implemented. Theconfiguration management program includes configuration identification and change control. This ensures thatcritical system components do not fail as a result of improper configuration.

O.Installation ensures that the TOE is delivered, installed, managed, and operated in a manner which maintains ITsecurity. This ensures that critical system components do not fail as a result of improper installation.

O.Manage behavior of security functions provides management controls/functions for security mechanisms. Thisensures that critical system components do not fail as a result of improper configuration of security mechanisms.

O.Preservation/trusted recovery of secure state ensures that the system remains in a secure state throughoutoperation in the presence of failures and subsequent system recovery. This objective is relevant when system failurescould result in insecure states that, when the system returns to operational mode (or continues to operate), could leadto security compromises.

O.Sufficient backup storage and effective restoration ensures that there is sufficient backup storage and effectiverestoration to recreate the system, when required. This ensures that data is available from backup, even if the currentcopy is lost through failure of a system component (e.g., a disk drive).

O.Time stamps provides time stamps to ensure that the sequencing of events can be verified. If the system must bereconstructed, it may be necessary to establish the order in which transactions were performed to return the systemto a state consistent with the state when a critical component failed..

O.Lifecycle security provides tools and techniques that are used throughout the development phase reducing thelikelihood of hardware or software imperfections. **O.Lifecycle security** also addresses the detection and resolutionof flaws discovered during the operational phase that may result in failure of a critical system component.

O.Repair identified security flaws. The vendor repairs security flaws that have been identified by a user. Suchsecurity flaws may result in critical system component failures if not repaired.

T.Flawed code addresses accidental or deliberate flaws in code made by the developer. Examples of accidentalflaws are lack of engineering detail or bad design. An example of a deliberate flaw would be the inclusion of atrapdoor for later entry into the TOE.

It is countered by:

O.Repair identified security flaws ensures that identified security flaws are repaired.

T.Malicious code exploitation addresses the threat where an authorized user, IT system, or hacker downloads andexecutes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentialityof the system assets. The execution of malicious code is done through a triggering event.

It is countered by:

O.Configuration management assures that a configuration management program is implemented. Theconfiguration management program includes configuration identification and change control. This ensures thatmalicious code is not introduced during the configuration process.

O.Integrity protection of user data and software ensures that appropriate integrity protection is provided for userdata and software. This prevents malicious code from attaching itself to user data or software.

O.Object and data recovery free from malicious code ensures that the system recovers to a viable state aftermalicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removedas part of the process.

O.Periodically check integrity ensures that periodic integrity checks are performed on both system and software. Ifthese checks fail, malicious code may have been introduced into the system.

O.Procedures for preventing malicious code provides a set of procedures and mechanisms that work to preventincorporation of malicious code into the system.

O.Require inspection for downloads ensures that software that is downloaded/transferred is inspected prior tobeing made operational.

O.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctlyfunctioning through features and procedures such as underlying machine testing and integrity checks.

O.Lifecycle security provides tools and techniques that are used throughout the development phase, reducing thelikelihood that malicious code was included in the product by the developer.

O.Lifecycle security also addresses thedetection and resolution of flaws discovered during the operational phase, such as modifications of components bymalicious code.

T.Message content modification addresses the situation where a hacker modifies information that is interceptedfrom a communications link between two unsuspecting entities before passing it on to the intended recipient. Severalkinds 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 securityattributes.

It is countered by:

O.Data Import/Export protects data when being transmitted to or from the TOE. Protection of data in transitpermits the TOE or the external user to detect modified messages, message replay, or fraudulent messages.

O.Protect user and TSF data during internal transfer protects data being transmitted between separated parts ofthe TOE. Protection of data in transit permits the TOE to detect modified messages, message replay, or fraudulentmessages.

O.Trusted path ensures that a trusted path is established between the user and the system. The trusted path protectsmessages from interception or modification by a hacker.

4.4.1.1.3 Cryptography

T.Disclosure of private and secret keys addresses the unauthorized disclosure of secret and/or private keys.

It is countered by:

O.Administrators, Registrarsand Auditors guidance documentation ensures that adequatedocumentation on securely configuring and operating the CIMC is available to Administrators, Registrarsand Auditors. This documentation will minimize errors committed by those users.

O.Cryptographic functions ensures that TOE implements approved cryptographic algorithms forencryption/decryption, authentication, and signature generation/verification; approved key generation techniquesand uses validated cryptographic modules. Use of validated cryptographic modules ensures that cryptographic keysare adequately protected when they are stored within cryptographic modules.

O.Limitation of administrative access. The administrative functions are designed in such a way that administrativepersonnel do not automatically have access to user objects, except for necessary exceptions. In general, theexceptions tend to be role specific.

Limiting the number of users who have access to cryptographic keys reducingthe likelihood of unauthorized disclosure.

O.Protect user and TSF data during internal transfer protects private and secret keys from unauthorizeddisclosure during transmission between separated parts of the TOE.

T.Modification of private/secret keys addresses the unauthorized revision of a secret and/or private key.

It is countered by:

O.Cryptographic functions ensures that TOE implements approved cryptographic algorithms forencryption/decryption, authentication, and signature generation/verification; approved key generation techniquesand uses validated cryptographic modules. Use of validated cryptographic modules ensures that cryptographic keysare adequately protected when they are stored within cryptographic modules.

O.Integrity protection of user data and software that ensures that appropriate integrity protection is provided forsecret and private keys.

O.Object and data recovery free from malicious code ensures that the system recovers to a viable state aftermalicious code has been introduced and damage has occurred. If the malicious code cause private or secret keys tobe revised in an unauthorized manner, this objective ensures that they are recovered to their correct values.

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 secretkeys can be detected through the audit trail.

T.Sender denies sending information addresses the situation where the sender of a message denies sending themessage to avoid accountability for sending the message and for subsequent action or inaction.

It is countered by:

O.Non-repudiation which ensures that the sender/originator of a message cannot successfully deny sending themessage to the recipient.

4.4.1.1.4 External Attacks

T.Hacker gains access addresses:

- Weak system access control mechanisms or user attributes
- Weak implementation methods of the system access control
- Vulnerabilities found in system or application code that allow a hacker to break into a system undetected.

It is countered by:

O.Restrict actions before authentication ensures that only a limited set of actions may be performed before a useris authenticated. This prevents a hacker who is unable to circumvent the access control mechanisms fromperforming security-relevant operations.

O.Control unknown source communication traffic ensures that communication traffic from an unknown source iscontrolled (e.g., rerouted or discarded) to prevent potential damage. Various kinds of hacker attacks can be detectedor prevented by rerouting or discarding suspected hacker traffic.

O.Individual accountability and audit records provides individual accountability for audited events. Each user isuniquely identified so that auditable actions can be traced to a user. Audit records provide information about pastuser behavior to an authorized individual through system mechanisms. This allows for the detection of unauthorizedactivity. Once detected, the damage resulting from such activity can be eliminated or mitigated.

O.Notify Authorities of Security Issues ensures that proper authorities are notified regarding any security issuesthat impact their systems. This minimizes the potential for the loss or compromise of data.

O.React to detected attacks ensures that automated notification or other reactions to the TSFdiscovered attacks isimplemented in an effort to identify attacks and to create an attack deterrent. This objective is relevant if actions thatthe organization deems essential also pose a potential attack that could be exploited.

O.Trusted path ensures that a trusted path is established between the user and the system. The trusted path is usedto protect authentication data, thus reducing the likelihood that a hacker can masquerade as an authorized user.

T.Hacker physical access addresses the threat where an individual exploits physical security weaknesses to gainphysical control of system components.

It is countered by:

O.Physical Protection ensures that physical access controls are sufficient to thwart a physical attack on systemcomponents.

T.Social Engineering addresses the situation where a hacker uses social engineering techniques to gain informationabout system entry, system use, system design, or system operation.

It is countered by:

O.Administrators, Registrarsand Auditors guidance documentation which deters administrativepersonnel errors by providing adequate guidance.

O.Procedures for preventing malicious code provides a set of procedures and mechanisms that work to preventincorporation of malicious code into the system. The introduction of malicious code into the system may be a goalof the social engineering attack.

O.Social Engineering Training which ensures that general users, Administrators, Registrarsand Auditorsare trained in techniques to thwart social engineering attacks.

4.4.1.2 Policies and Objectives Sufficiency

P.Authorized use of information establishes that information is used only for its authorized purpose(s). This isaddressed by the following objectives: **O.Maintain user attributes**, **O.Restrict actions before authentication**,**O.Security roles**, and **O.User authorization management**. **O.Restrict actions before authentication** ensures thatthe capability to perform security-relevant operations is limited to those who have been authorized to perform thoseoperations. **O.Maintain user attributes**, **O.Security roles**, and **O.User authorization management** ensure thatusers are only authorized to perform those operations that are necessary to perform their jobs. Finally, **O.Auditorsreview audit logs** deters users from misusing the authorizations they have been provided.

P.Cryptography establishes that accepted cryptographic standards and operations shall be used in the design of theTOE. This is addressed by **O.Cryptographic functions** which ensures that such standards are used.

4.4.1.3 Assumptions and Objectives Sufficiency

4.4.1.3.1 Personnel

A.Auditors Review Audit Logs establishes that audit logs are necessary for security-relevant events and that theymust be reviewed by auditors. This is addressed by **O.Auditors Review Audit Logs**, which ensures that security-relevantevents recorded in audit logs are reviewed by auditors.

A.Authentication Data Management establishes that management of user authentication data is external to theTOE. This is addressed by **O.Authentication Data Management**, which ensures that users modify theirauthentication data in accordance with appropriate security policy.

A.Competent Administrators, Registrarsand Auditors establishes that security of the TOE isdependent upon those that manage it. This is addressed by **O.Competent Administrators, RegistrarsandAuditors**, which ensures that the system managers will be competent in its administration.

A.CPS establishes that Administrators, Registrars, and Auditors are familiar with the CP and CPS underwhich the TOE is operated. This is addressed by **O.CPS,** which ensures that Administrators, Registrars,and Auditors are familiar with the CP and CPS under which the TOE is operated.

A.Disposal of Authentication Data establishes that users shall not retain access to the system after theirauthorization has been removed. This is addressed by **O.Disposal of Authentication Data**, which ensures thataccess to the system will be denied after a user's privileges have been removed.

A.Malicious Code Not Signed establishes that code not designed for the TOE will not be signed by a trusted party.This is addressed by **O.Malicious Code Not Signed,** which ensures that code must be signed by a trusted party or itwill not be loaded onto the system.

A.Notify Authorities of Security Issues establishes that users notify proper authorities of any security issues thatimpact their systems to minimize the potential for the loss of compromise of data. This is addressed by **O.NotifyAuthorities of Security Issues** which ensures that user notify proper authorities of any security issues that impacttheir systems.

A.Social Engineering Training establishes that individuals will attempt to gain access to the system using socialengineering practices. This is addressed by **O.Social Engineering Training**, which ensures that all users will betraining to thwart social engineering attacks.

A.Cooperative Users establishes that a secure IT environment is required to securely operate the TOE, and thatusers must work within the constraints of that environment. This is addressed by **O.Cooperative Users**, whichensures that users will cooperate with the constraints established.

4.4.1.3.2 Connectivity

A.Operating System establishes that an insecure operating system will compromise system security. This isaddressed by **O.Operating System**, which ensures that an operating system that meets security requirementsrecommended by the National Institute of Standards and Technology will be used.

4.4.1.3.3 Physical

A.Communications Protection establishes that the communications infrastructure is outside the TOE. This isaddressed by **O.Communications Protection**, which ensures that adequate physical protections are afforded thenecessary communications infrastructure.

A.Physical Protection establishes that physical modification of the TOE hardware, software, and firmware willcompromise system security.

5 EXTENDED COMPONENT DEFINITION

5.1 User Data Protection

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

Hierarchical to: No other components
Dependencies: No dependencies

FDP_ACF_CIMC.2.1 CIMS personnel private keys shall be stored in a FIPS 140-2 validated cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-2 validated cryptographic module.

FDP_ACF_CIMC.2.2 If certificate subject private keys are stored in the TOE, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

FDP_CIMC_CER.1 **Certificate Generation**

Hierarchical to: No other components
Dependencies: No dependencies

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

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

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

FDP_CIMC_CER.1.4 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_CIMC_CRL.1 **Certificate revocation list validation**

Hierarchical to: No other components

Dependencies: No dependencies

FDP_CIMC_CRL.1.1 A TSF that issues CRLs shall verify that all mandatory fields in any CRL issued contain values in accordance with ITU-T Recommendation X.509. 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_CIMC_CSE.1 **Certificate status export**

Hierarchical to: No other components

Dependencies: No dependencies

FDP_CIMC_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_CIMC.5 **Extended user private and secret key export**

Hierarchical to: FDP_ETC_CIMC.4

Dependencies: No dependencies

FDP_ETC_CIMC.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_CIMC.3 **Stored public key integrity monitoring and action**

Hierarchical to: No other components

Dependencies: No dependencies

FDP_SDI_CIMC.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, keyed hashes, or authentication codes.

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

FDP_CIMC_OCSP.1 **OCSP basic response validation**

Hierarchical to: No other components

Dependencies: No dependencies

FDP_CIMC_OCSP.1.1 If a TSF is configured to allow OCSP responses of the basic response type, the TSF shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 2560. At a minimum, the following items shall be validated:

- The **version** field shall contain a **0**.
- If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical **issuerAltName** extension.
- The **signatureAlgorithm** field shall contain the OID for a FIPS-approved digital signature algorithm.
- The **thisUpdate** field shall indicate the time at which the status being indicated is known to be correct.
- The **producedAt** field shall indicate the time at which the OCSP responder signed the response.
- The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.

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

Hierarchical to: No other components

Dependencies: No dependencies

FDP_ACF_CIMC.3.1 User secret keys stored within the CIMC, but not within a FIPS 140-2 validatedcryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

5.2 Security Management

FMT_MOF_CIMC.3 **Extended certificate profile management**

Hierarchical to: FMT_MOF_CIMC.2

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

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

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

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

FMT_MOF_CIMC.3.3 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_CIMC.3.4 The Administrator shall specify the acceptable set of certificate extensions.

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

Hierarchical to: FMT_MOF_CIMC.4

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

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

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

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

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

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

Hierarchical to: No other components
Dependencies: No dependencies

FMT_MTD_CIMC.5.1 TSF secret keys stored within the TOE, but not within a FIPS 140-2 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

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

Hierarchical to: No other components

Dependencies: No dependencies

FMT_MTD_CIMC.7.1 Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

FMT_MOF_CIMC.6 **OCSP profile management**

Hierarchical to: No other components

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

FMT_MOF_CIMC.6.1 If the TSF issues OCSP responses, the TSF shall implement an OCSP profile and ensure that issued OCSP responses are consistent with the OCSP profile.

FMT_MOF_CIMC.6.2 If the TSF issues OCSP responses, the TSF shall require the Administrator to specify the set of acceptable values for the **responseType** field (unless the CIMC can only issue responses of the basic response type).

FMT_MOF_CIMC.6.3 If the TSF is configured to allow OCSP responses of the basic response type, the TSF shall require the Administrator to specify the set of acceptable values for the **ResponderID** field within the basic response type.

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

Hierarchical to: No other components

Dependencies: No dependencies

FMT_MTD_CIMC.4.1 CIMC private keys shall be stored in a FIPS 140-2 validated cryptographic module or stored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-2 validated cryptographic module.

5.3 Protection of the TSF

FPT_CIMC_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_CIMC_TSP.1.1 The TSF shall periodically create an audit log signing event in which it computes a digital signature, keyed hash, or authentication code over the entries in the audit log.

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

FPT_CIMC_TSP.1.3 The specified frequency at which the audit log signing event occurs shall be configurable.

FPT_CIMC_TSP.1.4 The digital signature, keyed hash, or authentication code from the audit log signing event shall be included in the audit log.

5.4 Communication

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

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

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

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity and [none] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

FCO_NRO_CIMC.4 **Advanced verification of origin**

Hierarchical to: No other components.

Dependencies: FCO_NRO_CIMC.3Enforced proof of origin and verification of origin

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

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

5.5 Cyroptographic Support

FCS_CKM_CIMC.5 **CIMC private and secret key zeroization**

Hierarchical to: No other components.
Dependencies: FCS_CKM.4 Cryptographic key destruction
FDP_ACF.1 Security attribute based access control

FCS_CKM_CIMC.5.1 The TSF shall provide the capability to zeroize plaintext secret and private keys within the FIPS 140-2 validated cryptographic module.

FCS_SOF_CIMC.1 **CIMC Strength of Functions**

Hierarchical to: No other components.
Dependencies: No dependencies

FCS_SOF_CIMC.1.1 The TSF shall provide cryptographic mechanisms that fulfill the specific Strength of Function requirements of section 8.1.

6 SECURITY REQUIREMENTS

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.

6.1 Security Functional Requirements

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

Table 15TOE 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 origin***	***FCO_NRO_CIMC.3***
	Advanced verification of origin	***FCO_NRO_CIMC.4***
Cryptographic Support (FCS)	***CIMC private and secret key zeroization***	***FCS_CKM_CIMC.5***
	CIMC Strength of Functions	***FCS_SOF_CIMC.1***
User Data Protection (FDP)	Subset access control	FDP_ACC.1
	Security attribute based access control	FDP_ACF.1
	User private key confidentiality protection	***FDP_ACF_CIMC.2***
	User secret key confidentiality protection	***FDP_ACF_CIMC.3***
	Certificate Generation	***FDP_CIMC_CER.1***
	Certificate Revocation	***FDP_CIMC_CRL.1***
	Certificate status export	***FDP_CIMC_CSE.1***
	Basic Response Validation	***FDP_CIMC_OCSP.1***
	Extended user private and secret key export	***FDP_ETC_CIMC.5***
	Basic internal transfer protection (Iteration 1 and 2)	FDP_ITT.1
	Stored public key integrity monitoring and action	***FDP_SDI_CIMC.3***
	Basic data exchange confidentiality	FDP_UCT.1
Identification and Authentication (FIA)	Verification of secrets	FIA_SOS.1
	Timing of authentication	FIA_UAU.1
	Timing of identification	FIA_UID.1
	User-subject binding	FIA_USB.1

Security Requirement		Component
Security Management (FMT)	Management of security functions behavior	FMT_MOF.1
	Extended certificate profile management	***FMT_MOF_CIMC.3***
	Extended certificate revocation list profile management	***FMT_MOF_CIMC.5***
	TSF private key confidentiality protection	***FMT_MTD_CIMC.4***
	TSF secret key confidentiality protection	***FMT_MTD_CIMC.5***
	Extended TSF private and secret key export	***FMT_MTD_CIMC.7***
	OCSP Profile Management	***FMT_MOF_CIMC.6***
Protection of the TSF (FPT)	***Audit log signing event***	***FPT_CIMC_TSP.1***
	Inter-TSF confidentiality during transmission	FPT_ITC.1
	Basic internal TSF data transfer protection (Iteration 1 and 2)	FPT_ITT.1
	Reliable time stamps	FPT_STM.1

6.1.1 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 **[*minimum*]** level of audit; and

c) [The events listed in Table 16below].

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 inTable 16below].***

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

Table 16Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
Security Audit	FAU_GEN.1 Audit data generation	Any changes to the audit parameters, e.g., audit frequency, type of event audited	
		Any attempt to delete the audit log	
	FPT_CIMC_TSP.1 Audit log signing event	Audit log signing event	Digital signature, keyed hash, or authentication code shall be included in the audit log.

Section/Function	Component	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	
Key Generation		Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
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
Secret Key Storage		The manual entry of secret keys used for authentication	
Private and Secret Key Export	FDP_ETC_CIMC.5 Extended user private and secret key export; FMT_MTD_CIMC.7 Extended TSF private and secret key export	The export of private and secret keys (keys used for a single session or message are excluded)	
Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Registrar, etc.).
Certificate Status Change Approval		All requests to change the status of a certificate.	Whether the request was accepted or rejected.
CIMC Configuration		Any security-relevant changes to the configuration of the TSF	

Section/Function	Component	Event	Additional Details
Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	All changes to the certificate Profile.	The changes made to the profile.
Revocation Profile Management		All changes to the revocation profile.	The changes made to the profile.
Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile
Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP Profile Management	All changes to the OCSP profile	The changes made to the Profile

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) [none].

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 Auditor]*** and ***[no additional action]*** if the audit trail is full.

6.1.2 Communication

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

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

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity and ***[none]***of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

Rationale: This component is necessary to specify a unique requirement for certificate issuing and managementcomponents that is not addressed by existing CC requirements. It supports the security objective O.Non-repudiation and O.Control unknown source communication traffic.
NOTE: Based on FCO_NRO_CIMC.3, the TSF shall reject any information whose origin cannot be verifiedunless:

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

b) Acceptance of the data will not cause the TSF to output or export any confidential information.
The TSF may, for example, accept information whose origin can not be verified under in the followingcases:

a) The received information is a request for public information (e.g., an Online Certificate StatusProtocol (OCSP) request).

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

FCO_NRO_CIMC.4 Advanced verification of origin

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

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

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

6.1.3 Crypographic Support

FCS_CKM_CIMC.5CIMC private and secret key zeroization

FCS_CKM_CIMC.5.1 The TSF shall provide the capability to zeroize plaintext secret and private keys withinthe FIPS 140-2 validated cryptographic module.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FCS_SOF_CIMC.1 CIMC Strength of Functions

FCS_SOF_CIMC.1.1 The TSF shall provide cryptographic mechanisms that fulfill the specific Strength ofFunction requirements of section 8.

Rationale: This component is necessary to require specific Strength of Function metrics for cryptographic mechanisms of the TSF.

6.1.4 User Data Protection

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce [***TOE Access Control Policy specified in section 9 of this ST***] on [***all users, data and files***].

Application Note: The terms object and subject refer to generic elements in the TSF. For a policy to beimplemented, these entities must be clearly identified. For most systems there is only one type ofsubject, usually called a process or task, which needs to be specified in the ST. For a PP, the objectsand operations might be expressed as types such as: named objects, data repositories, observe accesses,etc. The ST author should specify the list of subjects, objects, and operations among subjects andobjects covered by the SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the[***TOE Access Control Policy specified in section 9 of this ST***] 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 177*].

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 17Access 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 Registrarsshall 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.
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.
Certificate Status Change Approval Note: Every request to change certificate status, for example, revoke a certificate, place a certificate on hold, or remove acertificate from hold must be accepted or rejected. If a request is accepted, any information about the request that may be exported from the TOE must be approved. Approval may be manual or automated.	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_CIMC.2 User private key confidentiality protection

FDP_ACF_CIMC.2.1CIMS personnel private keys shall be stored in a FIPS 140-2 validated cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-2 validated cryptographic module.

FDP_ACF_CIMC.2.2 If certificate subject private keys are stored in the TOE, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and managementcomponents that is not addressed by the CC.

FDP_ACF_CIMC.3 User secret key confidentiality protection

FDP_ACF_CIMC.3.1 User secret keys stored within the CIMC, but not within a FIPS 140-2 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FDP_CIMC_CER.1 Certificate Generation

FDP_CIMC_CER.1.1 The TSF shall only generate certificates whose format complies with [***theX.509standard for public key certificates***].

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

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

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

- The **version** field shall contain the integer **0, 1** or **2**.
- If the certificate contains an **issuerUniqueID** or **subjectUniqueID** then the **version** field shall contain the integer **1** or **2**.
- If the certificate contains **extensions** then 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.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FDP_CIMC_CRL.1 Certificate revocation list validation

FDP_CIMC_CRL.1.1 A TSF that issues CRLs shall verify that all mandatory fields in any CRL issued contain values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated:

- 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.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FDP_CIMC_CSE.1 Certificate status export

FDP_CIMC_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with ***[the X.509 standard for CRLs, the OCSP standard as defined by RFC 2560]***.

FDP_CIMC_OCSP.1 OCSP basic response validation

FDP_CIMC_OCSP.1.1 If a TSF is configured to allow OCSP responses of the basic response type, the TSF shallverify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 2560. At aminimum, the following items shall be validated:

- The **version** field shall contain a **0**.
- If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then theresponse shall contain a critical **issuerAltName** extension.
- The **signatureAlgorithm** field shall contain the OID for a FIPS-approved digital signature algorithm.

- The **thisUpdate** field shall indicate the time at which the status being indicated is known to be correct.
- The **producedAt** field shall indicate the time at which the OCSP responder signed the response.
- The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the**thisUpdate**field.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FDP_ETC_CIMC.5 Extended user private and secret key export

FDP_ETC_CIMC.5.1 Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FDP_ITT.1 Basic internal transfer protection (iteration 1)

FDP_ITT.1.1 The TSF shall enforce the [***TOE Access Control Policy specified in section 9 of this ST***] 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 section 9 of this ST***] to prevent the ***[disclosure]*** 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_CIMC.3 Stored public key integrity monitoring and action

FDP_SDI_CIMC.3.1 Public keys stored within the CIMC, but not within a FIPS 140-2 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_CIMC.3.2 The digital signature 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.]***

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1 The TSF shall enforce the [***TOE Access Control Policy specified in section 9 of this ST***] to [***transmit***] user data in a manner protected from unauthorised disclosure.

6.1.5 Identification and Authentication

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [

1. For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods.) and
2. For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur].

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***].

6.1.6 Security 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 18***] to [***the authorized roles as specified in Table 18***].

Table 18Authorized 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 beincluded 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.
Online Certificate Status Protocol (OCSP) Profile Management	The capability to modify the OCSP profile shall be restricted to Administrators.

FMT_MOF_CIMC.3 Extended certificate profile management

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

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

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

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

- keyUsage;
- basicConstraints;
- certificatePolicies

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

Rationale: This component is necessary to specify a unique requirement of certificate issuing and managementcomponents that is not addressed by the CC. It supports the security objective O.Configuration management.

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

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

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

- issuer;
- issuerAltName (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within thecertificate revocation list profile.)
- nextUpdate (i.e., a promise of next CRL in specified time).

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

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the CC. It supports the security objective O.Configuration management.

FMT_MOF_CIMC.6 OCSP profile management

FMT_MOF_CIMC.6.1 If the TSF issues OCSP responses, the TSF shall implement an OCSP profile and ensurethat issued OCSP responses are consistent with the OCSP profile.

FMT_MOF_CIMC.6.2 If the TSF issues OCSP responses, the TSF shall require the Administrator to specify theset of acceptable values for the **responseType** field (unless the CIMC can only issue responses of the basicresponse type).

FMT_MOF_CIMC.6.3 If the TSF is configured to allow OCSP responses of the basic response type, the TSFshall require the Administrator to specify the set of acceptable values for the **ResponderID** field within the basicresponse type.

Rationale: This component is necessary to specify a unique requirement of certificate issuing and managementcomponents that is not addressed by the CC. It supports the security objective O.Configuration management.

FMT_MTD_CIMC.4 TSF private key confidentiality protection

FMT_MTD_CIMC.4.1 CIMC private keys shall be stored in a FIPS 140-2 validated cryptographic module orstored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed bythe FIPS 140-2 validated cryptographic module.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

FMT_MTD_CIMC.5.1 TSF secret keys stored by the TOE, but not within a FIPS 140-2 validatedcryptographic module,shall be stored in encrypted form. The encryption shall be performed by FIPS 140-2 validated cryptographic module.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

FMT_MTD_CIMC.7 Extended TSF private and secret key export

FMT_MTD_CIMC.7.1 Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC.

6.1.7 Protection of the TSF

FPT_CIMC_TSP.1 Audit log signing event

FPT_CIMC_TSP.1.1 The TSF shall periodically create an audit log signing event in which it computes adigital signature, keyed hash, or authentication code over the entries in the audit log.

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

FPT_CIMC_TSP.1.3 The specified frequency at which the audit log signing event occurs shall be configurable.

FPT_CIMC_TSP.1.4 The digital signature, keyed hash, or authentication code from the audit log signing eventshall be included in the audit log.

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing CC requirements. It supports the security objective O.Protect stored audit records, by providing additional protection for stored audit records.

FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all confidential 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***]

FPT_STM.1 Reliable time stamps

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

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 19below 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 19Assurance 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
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 functionalrequirement is directed toward solving at least one objective.

6.3.1 Security Requirements Coverage

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

NOTE: There are 2 exceptions to this. In compliance with the PP, the “O.Object and data recovery free from malicious code” and “O.Preservation/trusted recovery of secure state” objectives are not covered by any security requirements.

The first table in this section, Table 20, addresses the mapping of security functional requirements tosecurity objectives. The second table, Table 21, addresses the mapping of security assurance requirements tosecurity objectives.

Table 20Security 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 association	O.Individual accountability and audit records
FAU_SEL.1 Selective audit	O.Individual accountability and audit records
FAU_STG.1 Protected audit trail storage	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss	O.Respond to possible loss of stored audit records
FCO_NRO_CIMC.3 Enforced proof of origin andverification of origin	O.Non-repudiation, O.Control unknown sourcecommunication traffic
FCO_NRO_CIMC.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM_CIMC.5 CIMC private and secret keyzeroization	O.Procedures for preventing malicious code, O.React todetected attacks
FCS_SOF_CIMC.1 CIMC Strength of Functions	O.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_CIMC.2 User private key confidentiality protection	O.Certificates, O.Procedures for preventing maliciouscode
FDP_ACF_CIMC.3 User secret key	O.Certificates,

confidentialityprotection	O.Procedures for preventing maliciouscode
FDP_CIMC_CER.1 Certificate Generation	O.Certificates
FDP_CIMC_CRL.1 Certificate revocation list validation	O.Certificates
FDP_CIMC_CSE.1 Certificate status export	O.Certificates
FDP_CIMC_OCSP.1 OCSP basic response validation	O.Certificates
FDP_ETC_CIMC.5 Extended user private and secretkey export	O.Data import/export
FDP_ITT.1 Basic internal transfer protection (iteration 1)	O.Integrity protection of user data and software, 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_CIMC.3 Stored public key integritymonitoring and action	O.Integrity protection of user data and software
FDP_UCT.1 Basic data exchange confidentiality	O.Data import/export
FIA_SOS.1 Verification of secrets	O.Limitation of administrative access
FIA_UAU.1 Timing of authentication	O.Limitation of administrative access, O.Restrict actionsbefore 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 functionsbehavior	O.Configuration management, O.Manage behavior ofsecurity functions, O.Security-relevant configurationmanagement
FMT_MOF_CIMC.3 Extended certificate profilemanagement	O.Configuration management
FMT_MOF_CIMC.5 Extended certificate revocation listprofile management	O.Configuration management
FMT_MOF_CIMC.6 OCSP Profile Management	O.Configuration management
FMT_MTD_CIMC.4 TSF private key confidentialityprotection	O.Detect modifications of firmware, software, andbackup data, O.Integrity protection of user data andsoftware
FMT_MTD_CIMC.5 TSF secret key confidentialityprotection	O.Detect modifications of firmware, software, andbackup data, O.Integrity protection of user data andsoftware
FMT_MTD_CIMC.7 Extended TSF private and secretkey export	O.Data import/export
FPT_CIMC_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_ITC.1 Inter-TSF confidentiality	O.Data import/export

duringtransmission	
FPT_ITT.1 Basic internal TSF data transfer protection(iterations 1-2)	O.Protect user and TSF data during internal transfer
FPT_STM.1 Reliable time stamps	O.Individual accountability and audit records, O.Timestamps

Table 21Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
ADV_ARC.1: Security architecture description	selection of EAL 4, O.Lifecycle security
ADV_FSP.4 Complete functional specification	selection of EAL 4, O.Lifecycle security
ADV_IMP.1 Implementation representation of the TSF	selection of EAL 4, O.Lifecycle security
ADV_TDS.3 Basic modular design	selection of EAL 4, O.Lifecycle security
AGD_ OPE.1: Operational user guidance	selection of EAL 4, O.Administrators, Registrars and Auditorsguidance documentation, O.Auditors Review AuditLogs, O.Competent Administrators, Registrarsand Auditors, O.Configuration Management, O.Installation, O.Malicious Code Not Signed, O.Procedures for preventing malicious code, O.Requireinspection for downloads, O.Security-relevantconfiguration management, O.User authorizationmanagement,
AGD_PRE.1: Preparative procedures	selection of EAL 4, O.Installation
ALC_CMC.4: Production support, acceptanceprocedures and automation	selection of EAL 4, O.Configuration management
ALC_CMS.4: Problem tracking CM coverage	selection of EAL 4, O.Configuration management
ALC_DEL.1: Delivery procedures	selection of EAL 4
ALC_DVS.1 Identification of security measures	selection of EAL 4
ALC_FLR.2 Flaw reporting procedures	O.Lifecycle security, O.Repair identified security flaws
ALC_LCD.1 Developer defined life-cycle model	selection of EAL 4
ALC_TAT.1 Well-defined development	selection of EAL 4

tools	
ATE_COV.2 Analysis of coverage	selection of EAL 4
ATE_DPT.1 Testing: Basic Design	selection of EAL 4
ATE_FUN.1 Functional testing	selection of EAL 4
ATE_IND.2 Independent Testing – Sample	selection of EAL 4
AVA_VAN.3 Focused vulnerability analysis	selection of EAL 4

6.3.2 Security Requirements Sufficiency

6.3.2.1 Security Objectives for the TOE

6.3.2.1.1 Authorized Users

O.Certificates is provided by **FDP_CIMC_CER.1 (Certificate Generation)** which ensures that certificates are valid.
FDP_CIMC_CRL.1 (Certificate revocation list validation), FDP_CIMC_CSE.1 (Certificate status export), and**FDP_CIMC_OCSP.1 (OCSP basic response validation)** which ensure that certificate revocation lists and certificatestatus information are valid.
FDP_ACF_CIMC.2 (User private key confidentiality protection) ensures that the certificate is not invalidated by thedisclosure of the private key by the TOE.
FDP_ACF_CIMC.3 (User secret key confidentiality protection) ensures thatan attacker can not obtain a bad certificate by obtaining a user's authenticator from the TOE and then using thatauthenticator to obtain a bad certificate.

6.3.2.1.2 External Attacks

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

6.3.2.1.3 Cryptography

O.Non-repudiation is provided by **FCO_NRO_CIMC.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 unlessthey contain evidence of origin and **FCO_NRO_CIMC.4 (Advanced verification of origin)** which covers therequirement that digital signatures be used so that the evidence of origin for a message may be verified by a thirdparty.

6.3.2.2 Security Objectives for the TOE and Environment

O.Configuration Management is provided by **FMT_MOF.1 (Management of security functions behavior)** which covers the requirement that only authorized users can change the configuration of the system.

FMT_MOF_CIMC.3 (Extended certificate profile management) covers the requirement that Administrators be ableto control the types of information that are included in generated certificates.
FMT_MOF_CIMC.5 (Extendedcertificate revocation list profile management) covers the requirement that Administrators be able to control to thetypes of information that are included in generated certificate revocation lists.
FMT_MOF_CIMC.6 (OCSP ProfileManagement) covers the requirement that Administrators be able to control to the types of information that areincluded in generated OCSP responses.
O.Configuration Management is supported by **AGD_OPE.1 (Operationaluser guidance)** which covers the requirement that Administrators be provided with documentation describing theconfiguration management features of the TOE and by **A.Competent Administrators, RegistrarsandAuditors** and **A.CPS** which ensure that Administrators are competent and are familiar with the CPS under which theTOE is to be operated.
O.Configuration Management is also supported by **ALC_CMC.4 (Production support,acceptance procedures and automation)** and **ALC_CMS.4 (Problem tracking CM coverage)** which ensure that aconfiguration management system is implemented and used.

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 thatdata other than private and secret keys be protected when they are transmitted and from the CIMC.
FDP_ETC_CIMC.5 (Extended user private and secret key export) and **FMT_MTD_CIMC.7 (Extended TSF privateand secret key export)** cover the requirement that private and secret keys be protected when they are transmitted toand from the TOE.

O.Detect modifications of firmware, software, and backup data is provided by
FMT_MTD_CIMC.4 (TSF private key confidentiality protection) and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** ensure that an attacker who has modified firmware, software, or backup data cannot prevent detection of the modification by computing a new digital signature, keyed hash, or authentication code.

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 performingany 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)** and **FPT_STM.1 (Reliable time stamps)**cover the requirement that the date and time of audited events are recorded in the audit recordsalong with the identities of the entities responsible for the actions.Finally, **FAU_SAR.1 (Audit review)** and **FAU_SAR.3 (Selectable audit review)** cover therequirement that the audit records are made available for review so that individuals can be held accountable for theiractions.

O.Integrity protection of user data and software is provided by **FDP_ITT.1 (Basic internal transfer protection)(iteration 1)** and **FDP_SDI_CIMC.3 (Stored public key integrity monitoring and action)** which cover therequirement that user data be protected Since data and software are protected using cryptography, **FMT_MTD_CIMC.4 (TSF private**

keyconfidentiality protection) and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are required toprotect the confidentiality of the private and secret keys used to protect the data and software.

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

O.Maintain user attributes is provided by **FIA_USB.1 (User-subject binding)** covers the requirement to maintain a set of security attributes associated with individual users and/or subjects acting on users' behalves.

O.Manage behavior of security functions is provided by **FMT_MOF.1 (Management of security functionsbehavior)** which covers the requirement that authorized users be able to configure, operate, andmaintain the security mechanisms.

O.Procedures for preventing malicious code is provided and supported by **FDP_ACF_CIMC.2 (User private key confidentiality protection)**, **FDP_ACF_CIMC.3 (User secret key confidentiality protection)**and **FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** ensure that an untrusted entity cannot use a trusted entity's key to sign malicious code.
AGD_OPE.1 (Operational user guidance) ensures proper checks are done prior to code installation.
This objective is also supported by assumption **A.Malicious Code Not Signed** that ensures those who are capable of signing code do not to sign malicious code.

O.Protect stored audit records is provided by **FAU_STG.1 (Protected audit trail storage)** whichcovers the requirement that audit records be protected against modification or unauthorized. Where the threat of malicious activity is greater, **FPT_CIMC_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)(iterations 1-2)** which covers the requirement that user data be protected during internal transfer and **FPT_ITT.1(Basic internal TSF data transfer protection) (iterations 1-2)** which covers the requirement that TSF data beprotected during internal transfer.

O.React to detected attacks is provided by **FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** which cover the requirement that the user who detected the attack be able to destroy any plaintext keys within the TOE in order to prevent the attacker from obtaining copies of these keys.

O.Require inspection for downloads is provided by **AGD_OPE.1 (Operational user guidance)** ensures that those who are capable of signing code do not to sign malicious code.
This objective is also supported by assumption **A.Malicious Code Not Signed.**

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, canbe performed when audit trail storage is full.

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 thatuser has been authenticated.

O.Security-relevant configuration management is provided **FMT_MOF.1 (Management of security functions behavior)** which ensures that security-relevantconfiguration data can only be modified by those who are authorized to do so. **O.Security-relevant configurationmanagement** is also supported by **AGD_OPE.1 (Operational user guidance)** which covers the requirement thatAdministrators be provided with documentation describing the configuration management features of the TOE andby **A.Competent Administrators, Registrarsand Auditors** and **A.CPS** which ensure that Administrators arecompetent and are familiar with the CPS under which the TOE is to be operated.

O.Time stamps is provided by **FPT_STM.1 (Reliable time stamps)** which covers therequirement that the time stamps be reliable.

O.User authorization management is provided and supported by **AGD_OPE.1 (Operational user guidance)** covers the requirement that Administrators be provided with documentation describing the user authorization management features of the TOE.
This objective is also supported by assumptions **A.Competent Administrators, Registrarsand Auditors** and **A.CPS** that ensure Administrators are competent and are familiar with the CPS under which the TOE is to be operated.

6.4 Requirement Dependency Rational

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 22below provides a summary of the security functional requirements dependency analysis.

Note that security functional requirements assigned to the IT environment by the CIMC PP are identified in bold-italics. Essentially those dependencies are fulfilled via the security objectives for the TOE environment that correspond to those requirements.

Table 22Summary 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 Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	***FMT_MTD.1***
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification Included	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3	Included
FCS_CKM_CIMC.5CIMC private and secret key zeroization	FCS_CKM.4	***FCS_CKM.4***
	FDP_ACF.1	Included
FCS_SOF_CIMC.1 CIMC Strength of Functions	None	
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Not included, no default profile is present in TOE.
FDP_ACF_CIMC.2 User private key confidentiality protection	None	-
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_CER.1 Certificate Generation	None	-
FDP_CIMC_CRL.1 Certificate revocation list validation	None	-
FDP_CIMC_CSE.1 Certificate status export	None	-
FDP_CIMC_OCSP.1OCSP basic response validation	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	None	-
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path	***FTP_TRP.1***
FIA_SOS.1 Verification of	None	-

Component	Dependencies	Which is:
secrets		
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	***FIA_ATD.1***
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	***FMT_SMR.2***
	FMT_SMF.1 Specification of Management Functions	Not included but covered by FMT_MOF_CIMC.3, FMT_MOF_CIMC.5 and FMT_MOF_CIMC.3
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	***FMT_SMR.2***
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	***FMT_SMR.2***
FMT_MOF_CIMC.6OCSP Profile Management	FMT_MOF.1Management of security functions behavior	Included
	FMT_SMR.1 Security roles	***FMT_SMR.2***
FMT_MTD_CIMC.4TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	-
FMT_MTD_CIMC.7 Extended TSF private and secret key export	None	-
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1 Audit data generation	Included
	FMT_MOF.1 Management of security functions behavior	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	-
FPT_ITT.1 Basic internal TSF data transfer protection	None	-
FPT_STM.1	None	

Justification of Unsupported Dependencies Regarding FTP_ITC.1 or FTP_TRP.1

Component FDP_UCT.1 Basic data exchange confidentiality has a direct dependency on FTP_ITC.1 Inter- TSFtrusted channel or FTP_TRP.1 Trusted path that is unmet. This product uses basic encryption to ensure basic dataexchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path forthe TOE. Note that FTP_TRP.1 Trusted path is included in the IT Environment requirements.

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. 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 AdministrationCenter, 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 23.

Table 23Audited 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 AdministrationCenter. 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.
All changes to the access control privileges of a user account or a role	TOE generates an audit event for any changes to the access control privileges of a user account or a role
Roles and users are added or deleted	Roles are embedded into the system hence not added from gui but TOE generates an audit event when adding users
Login and logoff attempts	TOE generates an audit event for login and logoff attempts
System start-up and shutdown	TOE generates an audit event when authorized user logins the system and logouts from the system
CA application start-up and shutdown	TOE generates an audit event for CA start-up and shutdown
An Administrator unlocks an account that has been locked as a result of unsuccessful attempts	It is not applicable in TOE

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 AdministrationCenter the auditable events can be included or excluded from the set of audited events according to event type.

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 signed 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_CIMC_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 Reliable Time Source

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

This security function addresses the following SFR: FPT_STM.1

7.1.2 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.

- **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.

- **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 AdministrationCenter. 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 AdministrationCenter. Different set of privileges can be assigned to the Registrars from the AdministrationCenter.

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

Administrator, Registrar, Auditor creation,authorization, TOE secret keys management, Certificate, CRL profile management, Audit parameters management can be performed by the security functions.
Certain operations are only available to certain operators and the role restrictions are described in Table 24. 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 24Role 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 CIMC private keys is not provided.

Section/Function	Function/Authorized Role
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 CIMC boundary.
CIMC 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 revocation profile is restricted to Administrators.
Certificate Revocation List Profile Management	The capability to modify the certificate revocation list 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
Online Certificate Status Protocol (OCSP) Profile Management	The capability to modify the OCSP profile is restricted to Administrators.

7.1.3 Scope of Policy and Access Rules

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

Table 25 describes the operations and the related enforcing rules.

Table 25Access 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 isnot provided.

Section/Function	Event
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. At least two Registrars shall berequired to request the decryption of a certificatesubject private key.
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 wrapped with Administrators encryption certificates. The wrapped secret keys are stored in DB. The secret key renewal from the Administration Center is restricted to Administrators. 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.
Private and Secret Key Export	The capability to export a component private key is not provided. The capability to export certificate subject privatekeys shall be restricted to Registrars. The export of a certificate subject private key shallrequire the authorization of at least two Registrars. .
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.

Administrators need to enter their id and the smartcard password in the login screen. After successful login to the smartcard, the database password encrypted for the administrators which is stored in the ini file is decrypted with the administrator encryption certificate private key. Administrator id information and the smartcard serial number is checked from the database, so it is assured that the information in the smartcard is not copied. A random number is signed by the administrator, and it is checked against the signature certificate of the administrator in the database. Finally, the role attribute in the signature certificate is checked, and validated against the administrator object identifier.

Registrars need to enter their id and the smartcard password in the login screen. First of all, if the registration authority application is running, Registrars id is checked from the database and if found, smartcard library name, serial number and a random number is sent to the client. With the provided library name, registrar tries to login the smartcard. After login the smartcard serial number is checked, and the random number is signed with the signature certificate. This signature is validated in the registration authority application. Finally, the role attribute in the signature certificate is checked, and validated against the registrar object identifier.

Identification and authentication of auditors are like the administrators.

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 requires certificate based authentication for all defined roles which has a strength much greater than that required even when guessing at the maximum rate possible using the TOE interfaces . This security function addresses the following SFR: FIA_SOS.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 TLS 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_CIMC.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.

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 TLS protocol. To initate any key management or certificate management transactions a valid authentication code is required.
For security-relevant information, the TSF only accepts the information if it was signed using a digital signature algorithm.
This security function addresses the following SFRs: FPT_ITC.1 and FCO_NRO_CIMC.4

Protection of user data during transmission against unauthorized disclosure and modification is provided with encryption and digital signatures according to TOE Access Control Policy specified in section 9. This security function addresses the following SFR: 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. Proof of possession is always established before a certificate can be made available to an end-user. For X.509 v3 certificates, 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}).

Certificates are generated according to certificate profile choosen by the Registrars.

Before generating certificates, TOE verifies that public/private key pairs corresponds to each other.

This security function addresses the following SFR: FDP_CIMC_CER.1

7.1.6.2 Certificate Status Export

TOE exports certificate status information by two ways; CRLs and OCSP responses.

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

This security function addresses the following SFR: FDP_CIMC_CSE.1

TOE provides basic OCSP responsesin accordance with IETF RFC 2560. The administrator specifies ResponderId in the OCSP server configuration.

This security function addresses the following SFR: FMT_MOF_CIMC.6and FDP_CIMC_OCSP.1

7.1.6.3 Certificate Profile Management

Using TOEcertificate 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.

Administrators are required to specify the key owner's identifier, 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. They also need to specify keyUsage, basicConstraints and certificatePolicies.

This security function addresses the following SFRs: FMT_MOF_CIMC.3

If certificate profile is created accordingly, the user private keys are first encrypted with FIPS 140-2 validated cryptographic module and then stored in the database. This security function addresses the following SFR: FDP_ACF_CIMC.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. Administrators are required to specify issuer and nextUpdate(lifetime of a CRL) fields to create a CRL profile.

This security function addresses the following SFR: FMT_MOF_CIMC.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_CIMC_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 hardware cryptographic module. These keys are exported to end user with CMP protocol.This security function addresses the following SFRs: FDP_ACF_CIMC.2 and FDP_ETC_CIMC.5.

TOE secret keys are encrypted in FIPS 140-2 level 3 validated hardware cryptographic module and stored in the database in an encrypted form. This security function addresses the following SFRs: FMT_MTD_CIMC.4 and FMT_MTD_CIMC.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_CIMC.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_CIMC.3

7.1.8.3 Key Zeroization

TOE does not store plaintext keys. The zeroization of keys are provided by FIPS 140-2 validated Hardware and Software cryptographic modules which are invoked by the TOE.

This security function addresses the following SFR: FCS_CKM_CIMC.5

7.1.8.4 Strength of Functions and Cryptographic Operations

TOE uses FIPS validated software crytographic module for encryption, decryption, hashing, macing, signature verification. These operations are performed in accordance with the following standards

- Encryption/decryption: FIPS PUB 197 (AES);
- Signature generation/verification: FIPS PUB 186-2 (RSA, ECDSA), Draft FIPS PUB 186-3 (RSA-PSS);
- Hashing: FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA 224, SHA256, SHA384 and SHA512); and
- MACing: FIPS PUB 113

TOE uses FIPS validated hardware crytographic module for key generation, decryption and signature generation.

This security function addresses the following SFR:FCS_SOF_CIMC.1

8 STRENGTH OF FUNCTION (SoF) REQUIREMENTS

This section defines explicit metrics for various cryptographic functions addressing FCS_SOF_CIMC.1.

8.1 Cryptographic Modules

All cryptographic functions of CIMCs is performed within FIPS 140-2 validated cryptographic modules which are also required to generate cryptographic keys and secret keys.

8.1.1 Encryption and FIPS 140-2 Validated Modules

As noted earlier in the document, references to FIPS 140-2 refer to the most current version of the standard and themost current version can be found at http://csrc.nist.gov/cryptval.

8.1.1.1 Encryption Algorithms

The encryption specified for:

Table 26 Encryption Algorithms

Requirement Label	Requirement Name	
FAU_STG.1	Protected audit trail storage	Not applicable – access controlled

FCO_NRO_CIMC.4	Advanced verification of origin	CRL signing: default CA cert 2048-bit RSA;
		OCSP signing: default 2048-bit RSA;
		All configurable to RSA (1024-, 2048-, 4096-bits and others supported by the HSM).

FDP_ACF_CIMC.2	User private key confidentiality protection	Encryption Certificate for CA, default RSA-2048 and supports multiple key sizes (RSA 1024, 2048,4096 bits) Symmetric encryption key: AES (128-256)
FDP_ACF_CIMC.3	User secret key confidentiality protection	Not applicable – no user secret keys stored
FDP_ETC.CIMC.5	Extended user private and secret key export	Provided by Protocol Encryption Key, default RSA 2048 and supports RSA 1024,2048,4096 bits Symmetric encryption key:

		AES256
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action	Certificate signing: default CA cert 2048-bit RSA, configurable to RSA (1024-, 2048-, 3072-, 4096-bits and others supported by the HSM).
FMT_MTD_CIMC.4	TSF private key confidentiality protection	TSF private keys are stored and protected on the HSM.
FMT_MTD_CIMC.5	TSF secret key confidentiality protection	TSF secret keys are stored and protected on the HSM.
FMT_MTD_CIMC.7	Extended TSF private and secret key export	Not applicable – no TSF private or secret keys exported
FPT_CIMC_TSP.1	Audit log signing event	Keyed Hash, default HMAC SHA256

shall be performed using a FIPS-approved or recommended algorithm.

8.1.1.2 FIPS 140-2 Validated Cryptographic Modules

Cryptographic modules specified for:

FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_ETC_CIMC.5	Extended user private and secret key export
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.7	Extended TSF private and secret key export
FPT_CIMC_TSP.1	Audit log signing event

shall be validated against FIPS 140-2.

8.1.1.3 Split Knowledge Procedures

Split-knowledge procedures specified in:

FDP_ETC_CIMC.5	Extended user private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export

shall be implemented and validated as specified in FIPS 140-2.

8.1.1.4 Authentication Codes

The authentication code specified in:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verivication of origin
FPT_CIMC_TSP.1	Audit log signing event
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action

shall be a FIPS-approved or recommended authentication code.

8.1.2 Cryptographic module levels for cryptographic functions that involve private or secretkeys

All cryptographic operations performed (including key generation) at the request of the TOE shall be performed in aFIPS 140-2 validated cryptographic module operating in a FIPS-approved or recommended mode of operation.

Table 27 specifies for each category of use for a private or secret key, the required overall FIPS 140-2 level for thevalidated cryptographic module. If the CIMC generates certificate subject private keys, the required overall FIPS140-2 level for Long Term Private Key Protection keys shall apply.

Table 27 FIPS 140-2 Level for Validated Cryptographic Module

Required Overall FIPS 140-2 Level for CIMC Cryptographic Modules	
Category of Use	**FIPS 140-2 Level**
Certificate and Status Signing - single party signature - multiparty signature	 3 2
Integrity or Approval Authentication - single approval - dual approval	 2 2
General Authentication	2
Long Term Private Key Protection	3
Long Term Confidentiality	2
Short Term Private key Protection	2
Short Term Confidentiality	1

8.1.3 Cryptographic Functions That Do Not Involve Private or Secret Keys

There are two other cryptographic functions that may be performed in CIMCs that do not require private or secret keys. These include:

1. *Hash Generation*: One-way hash functions may be used in the process of signature generation andverification (a signature is typically generated by applying a private key to the hash of the message). Thegeneration of a hash does not require a key. Therefore, hash generation does not have the sameconfidentiality requirements of other cryptographic functions.
2. *Signature Verification*: Signatures are verified from a message text and a public key.

For a cryptographic module that only performs signature verification and/or keyless hash generation functions, theoverall required FIPS 140-2 level shall be Level 1.

9 CIMC TOE Access Control Policy

The TOE shall support the administration and enforcement of a CIMC 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.