Security Target

Entrust Authority Security Manager and Security Manager Administration

Version 5. 5

January 17, 2012

Prepared By:

Entrust Inc.

Document version control log

Version	Date	Author(s)	Description
1.0	May 8, 2009	Sharon Boeyen	Initial copy of Entrust Authority 8.0 Security Target
2.0	May 21, 2009	Mark Joynes	Modifying ST to reflect version number change for the product set – change to 8.1
3.0	July 14, 2010	Sharon Boeyen	Align ST with "Certificate Issuing and Management Components for Basic Robustness Environments Protection Profile Version 1.0 April 27, 2009".
4.0	August 10, 2010	Sharon Boeyen	Modify ST to resolve issues raised by evaluator Lachlan Turner in Domus Observation report dated August 9, 2010
4.1	August 12, 2010	Sharon Boeyen	Modify ST to resolve additional issues and concerns raised by evaluator Lachlan Turner in Domus Observation report dated August 12, 2010
4.2	September 17, 2010	Sharon Boeyen	Modify ST to resolve certifier comments
5.0	November 23, 2010	Sharon Boeyen	Modify to exclude EAAS from TOE
5.1	December 30, 2010	Sharon Boeyen	Align ST with revised PP
5.2	August 30, 2011	Sharon Boeyen	Corrected reference in section 7.1.1.1 for Operations Guide to point to Section E and added version number to Operations Guide in list of References in Section 10.
5.3	November 17, 2011	Sharon Boeyen	Updated EASM and EASMA versions to 8.1 SP1 and updated Security Kernel version to 8.1 SP1
5.4	December 16, 2011	Sharon Boeyen	Updated version numbers for database, directory, HSM and ESP and clarified which service/protocol made use of the GUTS cryptographic module that is turned off for purposes of the evaluation
5.5	January 17, 2012	Sharon Boeyen	Added EASM and EASMA specific build numbers, updated reference to CIMC PP to reference final CC approved version, updated reference to EASM Operations Guide, and updated version and date information for ST.

Table of Contents

1 Introduction 8

1.1 ST Reference 8
1.2 TOE Reference 8
1.3 TOE Overview 8
1.3.1 Components 8
1.3.2 Typical Deployment Scenarios 8
1.3.2.1 Traditional X.509 Environment 9
1.3.2.2 Electronic Passport Country Verifying Environment employing EAC 9
1.3.3 Non-TOE Requirements 9
1.3.3.1 TOE Component Platform Requirements 9
1.3.3.2 Additional Software Requirements 10
1.3.3.3 Additional Hardware Requirements 10
1.3.4 Evaluated Configuration 10
1.4 TOE Description 11
1.4.1 Product Type 11
1.4.2 Major Security Features 11
1.4.3 TOE Roles 12
1.4.4 High Level Architecture 13
1.4.4.1 Entrust Authority Security Manager 14
1.4.4.2 Entrust Authority Security Manager Administration 15
1.4.4.3 Database 15
1.4.4.4 Directory 16
1.4.4.5 Cryptographic Modules 16
1.4.5 TOE Boundary 17
1.4.5.1 Exclusion from the TOE Boundary 18

2 Conformance Claims 21

2.1 CC Conformance Claim 21
2.2 Protection Profile Claim 21

3 Security Problem Definition 22

3.1 Assumptions 22
3.1.1 Personnel Assumptions 22
3.1.2 Connectivity 23
3.1.3 Physical 23
3.2 Threats 23
3.2.1 Authorized Users 23
3.2.2 System 23
3.2.3 Cryptography 23
3.2.4 External Attacks 24
3.3 Organizational Security Policies 24

4 Security Objectives 25

4.1 Security Objectives for the TOE 25
4.1.1 Authorized Users 25
4.1.2 System 25
4.1.3 Cryptography 25
4.1.4 External Attacks 25
4.2 Security Objectives for the Environment 25
4.3 Security Objectives for both the TOE and the Environment 27

4.4 Security Objectives Rationale 28
4.4.1 Tracing Between Security Objectives and Security Problem Definition 28
4.4.2 Tracing Justification 31
4.4.2.1 Assumptions and Objectives Sufficiency 31
4.4.2.2 Threats and Objectives Sufficiency 33
4.4.2.3 Policies and Objectives Sufficiency 38

5 Extended Components Definition 40

5.1 Extended FCO Components 40
5.1.1 Enforced Proof of Origin and Verification of Origin 40
5.1.2 Advanced Verification of Origin 40
5.2 Extended FCS Components 41
5.2.1 CIMC Private and Secret Key Zeroization 41
5.2.2 CIMC Strength of Functions 41
5.2.2.1 Cryptographic Modules 41
5.3 Extended FDP Components 42
5.3.1 User Private Key Confidentiality Protection 42
5.3.2 User Secret Key Confidentiality Protection 43
5.3.3 Certificate Generation 43
5.3.4 Certificate Revocation List Validation 44
5.3.5 Certificate Status Export 44
5.3.6 Extended User Private and Secret Key Export 45
5.3.7 Stored Public Key Integrity Monitoring and Action 45
5.4 Extended FMT Components 46
5.4.1 Extended Certificate Profile Management 46
5.4.2 Extended Certificate Revocation List Profile Management 46
5.4.3 Private Key Confidentiality Protection 47
5.4.4 Secret Key Confidentiality Protection 47
5.4.5 Extended TSF Private and Secret Key Export 47
5.5 Extended FPT Components 47
5.5.1 Audit Log Signing Event 47

6 Security Requirements 49

6.1 Security Functional Requirements 49
6.1.1 Security Audit 50
6.1.2 Roles 52
6.1.3 Access Control 53
6.1.4 Identification and Authentication 55
6.1.5 Remote Data Entry and Export 56
6.1.5.1 Certificate Status Export 57
6.1.6 Key Management 57
6.1.6.1 Private Key Storage 57
6.1.6.2 Public Key Storage 58
6.1.6.3 Secret Key Storage 59
6.1.6.4 Private and Secret Key Destruction 59
6.1.6.5 Private and Secret Key Export 59
6.1.7 Certificate Profile Management 60
6.1.8 Certificate Revocation List Profile Management 60
6.1.9 Certificate Registration 60
6.1.10 Certificate Revocation 61
6.1.11 Strength of Function 61
6.1.12 Cryptographic Operations 62
6.2 Security Assurance Requirements 62
6.3 Security Requirements Rationale 63
6.3.1 Security Requirements Coverage 63
6.3.2 Security Requirements Dependencies 65

6.3.3 Security Requirements Sufficiency 65
6.3.3.1 Security Objectives for the TOE 65
6.3.3.2 Security Objectives for the TOE and Environment 67
6.3.4 Security Assurance Requirements Rationale 70

7 TOE Summary Specification 72

7.1 Security Audit 72
7.1.1 Specification of auditable events and recorded information 72
7.1.2 Accountability of users 73
7.1.3 Audit data selection 73
7.1.4 Audit Data Protection 73
7.1.5 Prevention of Audit Data Loss 74
7.1.6 Reliable Time Source 74
7.2 Roles 74
7.2.1 Role Definition 74
7.2.2 Management of security functions behavior 75
7.3 Access Control 76
7.4 Identification and Authentication 77
7.4.1 Authentication of users 77
7.4.2 Identification of users 77
7.4.3 User-Subject Binding 77
7.5 Remote Data Entry and Export 78
7.5.1 Enforced Proof of Origin and Verification of Origin 78
7.5.2 Protection of data communications between Security Manager and EASMA 78
7.5.3 Trusted channel 78
7.6 Certificate Management 78
7.6.1 Certificate Generation 78
7.6.2 Certificate Status Export 79
7.6.3 Certificate Profile Management 79
7.7 Certificate Revocation 79
7.7.1 CRL Profile Management 79
7.7.2 CRL Validation 79
7.8 Key Management 79
7.8.1 Key Generation 79
7.8.2 Private Key Protection 80
7.8.3 Public Key Protection 80
7.8.4 Key Zeroization 80
7.8.5 Strength of Functions and Cryptographic Operations 80

8 TOE Access Control Policy 82

9 Glossary 83

10 References 85

List of Figures

Figure 1: Entrust Authority Infrastructure Components 14
Figure 2: TOE Boundary 17

List of Tables

Table 1-1-1 Roles Description 12
Table 4-1 Relationship of Assumptions to Security Objectives 29
Table 4-2 Relationship of Security Objectives for the TOE to Threats 29
Table 4-3 Relationship of Security Objectives for the Environment to Threats 29
Table 4-4 Relationship of Security Objectives for Both the TOE and the Environment to Threats 30
Table 4-5 Relationship of Organizational Security Policies to Security Objectives 31
Table 6-1: TOE Functional Security Requirements 49
Table 6-2 Auditable Events and Audit Data 50
Table 6-3 Authorized Roles for Management of Security Functions Behavior 52
Table 6-4 Access Controls 54
Table 6-5 Assurance Requirements 62
Table 6-6 Security Functional Requirements Related to Security Objectives 63
Table 6-7 Security Assurance Requirements Related to Security Objectives 64
Table 6-8 FIPS 140-2 Level for Validated Cryptographic Module 67
Table 7-1 Audited events as specified by CIMC PP 72
Table 7-2 Role Restrictions 75
Table 7-3 Explicit Access Control Rules 76

1 Introduction

1.1 ST Reference

Entrust Authority Security Manager and Entrust Authority Security Manager Administration ST version 5.5 Entrust Inc, January 17, 2012.

1.2 TOE Reference

Entrust Inc., Entrust Authority Security Manager v8.1 SP1 (build number 8.1.350.240) and Entrust Authority Security Manager Administration v8.1 SP1 (build number 8.1.350.175).

1.3 TOE Overview

The Entrust Authority (EA) Target of Evaluation (TOE) is a comprehensive Public Key Infrastructure (PKI) security infrastructure that creates and manages public key certificates. This TOE supports traditional PKI, based on the [X.509] standard as well as PKI based on the [ISO 7816] standard for a specific application for Extended Access Control (EAC) for electronic passports.

1.3.1 Components

The Certification Authority (CA) PKI services are provided by the Entrust Authority Security Manager (EASM). As such, EASM issues certificates to users and other entities (including other CAs) and issues Certificate Revocation lists (CRL) containing status information for X.509 certificates. Access to EASM and its services is secured. Optionally, a 3rd party Hardware Security Module (HSM) can be used for the CA signing keys and the database protection keys.

The Registration Authority (RA) services for X.509 PKI infrastructures are provided by Entrust Authority Security Manager Administration (EASMA). RA services for the ISO 7816 PKI are provided by the command line interface to EASM. Access to RA functionality is secured and only authorized individuals are able to perform RA services. Administrative functions can be divided among a number of authorized administrators and additional roles can be defined, specific to a given operational environment's requirements.

A database system is used to store information relevant to the CA, the RA, administrators, users, security and security policy related information. EASM provides the security for the database.

A directory system is used to publish X.509 certificates and CRLs. All modifications to X.509 data in the directory are secured. Read access to certificates and CRLs is generally configured to allow anonymous read access.

Administrative user and end-user systems are used to perform local identification and authentication and perform local cryptographic operations such as digital signature generation and verification, encryption and decryption. Optionally administrative and end-users may use 3rd party smartcards.

1.3.2 Typical Deployment Scenarios

There are two primary types of environment where Entrust Authority PKI systems would typically be deployed. These include traditional X.509 single/multi-application environments, and ePassport Country Verifying environments employing Extended Access Control (EAC) with ISO 7816-based certificates. The CA requires a database in both scenarios. A directory is used in both scenarios to publish X.509 certificates and CRLs

1.3.2.1 Traditional X.509 Environment

These deployments support one to many PKI applications using X.509 certificates and Certificate Revocation Lists (CRL). Typical deployments include EASM and EASMA. They also make use of a CA database and typically use a directory to publish certificates and CRLs. Various certificate profiles can be used to issue certificates that are tailored to specific application requirements e.g. Document Signer certificate profile for use within ePassport Country Signing environments to support Basic Access Control (BAC). The base standards supported by this type of environment are [X.509] and [RFC 5280]. There are a number of additional standards supported as well, especially to facilitate application-specific requirements.

1.3.2.2 Electronic Passport Country Verifying Environment employing EAC

These deployments are typically single application deployments. They are usually separate from traditional X.509 application environments including ePassport Country Signing environments. These deployments include EASM. The CA functionality is provided by EASM and the RA functionality is also provided by EASM, with EAC administrators connecting to EASM through its command line interface.

The PKI trust model and certificate profiles for EAC are specified in [TR-03110] and [BIG CP]. The base certificate syntax is specified in [ISO 7816].

The EAC infrastructure includes two distinct types of CA. A Country Verifying CA (CVCA) is a single authoritative CA within a country for its EAC implementation. In that perspective, it is somewhat similar to an X.509 CA that is the Root of a strict hierarchy. A CVCA issues certificates to those DVs with which it has an established relationship both within its own country as well as to DVs in other countries. A DV is a distinct type of a CA that issues certificates to Inspection Systems (IS) within its own direct area of responsibility. There may be several DVs in a given country. ISs are systems that validate signatures on biometric data stored on ePassports, using a chain of certificates from the IS itself back to the CVCA of the country that issued the ePassport.

Each EAC deployment must be either a CVCA or a DV. It cannot be both, because of the nature of the entities and the trust model.

Certificates issued to CVCAs, DVs and ISs are ISO 7816 certificates that comply with the certificate profiles specified in [TR-03110] and [BIG CP]. These certificates are not published in the directory. They are short-lived certificates and by definition have no revocation scheme.

The database is used to store relevant data about both the X.509 and ISO 7816 infrastructures.

1.3.3 Non-TOE Requirements

In addition to the components within the TOE, a comprehensive infrastructure deployment requires the platforms for each of these components, as well as additional software and hardware components. These are outlined below. For each component (TOE and TOE environment, the evaluated configuration is indicated in italics.

1.3.3.1 TOE Component Platform Requirements

EASM 8.1 SP1 is supported on the following platforms. For more detail (e.g. versions) about other platforms, see the product documentation.

- *MS Windows 2008 R2 Server Enterprise*
- Solaris
- HP-UX
- Red Hat Linux

EASMA 8.1 SP1 is supported on the following platforms.

- *Microsoft Windows 7, 32 or 64 bit*
- Microsoft Windows Vista 32 or 64 bit
- MS Windows 2008 R2 Server Enterprise

1.3.3.2 Additional Software Requirements

The TOE environment also requires the following additional software components:

Database: The following databases are supported with the 8.1 SP1 TOE:

- *Postgresql 8.3.11*
- Oracle

Directory: The following directory systems are supported with the 8.1 SP1 TOE:

- CA Inc, CA Directory
- *Critical Path Inc., Directory Server (DS) 5.03*
- International Business Machines, Directory Server
- Microsoft Corporation, Active Directory
- Novell Inc, NDS eDirectory
- Siemens AG, DirX
-
- Java System Directory
- OpenLDAP
- Oracle Internet Directory
- RedHat Directory Server

End User Client Systems: X.509 end-users require client software components to communicate with the RA and CA functions to perform their life-cycle management functions. The evaluated configuration will use *Entrust Entelligence Security Provider (ESP) 9.1 on Microsoft Windows 7*.

1.3.3.3 Additional Hardware Requirements

No additional hardware components are required for a fully functioning X.509 and/or ISO 7816 PKI infrastructure. However to operate an infrastructure with the security assurance defined for this evaluation, the following additional hardware component is necessary for the TOE environment. In addition, optional smartcards could be added to the TOE environment for administrative users and end-users, if desired.

HSM: A 3rd party FIPS 140-2 level 3 HSM is used to protect CA signing keys and database protection keys. The following HSMs are supported with the TOE:

- SafeNet
- nCipher

The evaluated configuration will use *Luna CA4 with DOCK-2 USB reader, firmware 4.6.8 and client 2.5.*

1.3.4 Evaluated Configuration

The evaluated configuration for the TOE is as indicated in italics in section 1.3.3.1. The evaluated configuration for the environment is as indicated in italics in section 1.3.3.2. In general the default

settings for the TOE components will be used in the evaluated configuration. Specific configuration details will be provided in the Configuration Guide.

1.4 TOE Description

This section describes the Target of Evaluation (TOE) in terms of the class of product, the operational environment, and the provided security functionality.

1.4.1 Product Type

Entrust Authority is a comprehensive solution for PKI in a variety of environments supporting two distinct public-key certificate formats. This TOE constitutes a "Certificate Issuing and Management Component" (CIMC) and satisfies all SFRs and SARs specified in the [CIMC PP].

Entrust Authority provides privacy, access control, integrity, authentication, and support for the non-repudiation process to support information technology applications and electronic commerce transactions. Entrust Authority:

- Manages the generation and distribution of public key pairs;
- Issues X.509 certificates and associated status information;
- Issues ISO/IEC 7816 certificates for ePassport EAC; and
- Publishes X.509 certificates and associated status information in LDAP and X.500 directory systems and optionally in HTTP accessible files.

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

- CA Key management (managing CA signing key pair, master keys and enforcing infrastructure security policies);
- Operator management (providing capability to authorized operators to manage other operators including passwords, keys, roles and privileges etc.);
- End-entity management (managing end-users including creation, initializing, deleting, recovering, revoking key update etc.);
- Cross-certificate management (generation and maintenance of X.509 cross-certificates);
- CVCA management (management of CVCA signing keys and relationships with DVs); and
- DV management (management of DV signing keys, relationships with CVCAs and management of ISs).

The support services provided by EASM include:

- Self-management (initialize SM, start and stop Entrust services and validate operator passwords);
- Database management (operate and maintain the database);
- Audit trail management (maintain and analyze audit record of critical and non-critical events within infrastructure); and
- Directory management (operation and maintenance of Directory and directory entries).

1.4.2 Major Security Features

This ST couples certificate management functionality with assurances selected to provide a maximum amount of confidence consistent with existing best practices for COTS development.

Meeting the requirements established in this ST signifies that the Entrust Authority Security Manager and Entrust Authority Security Manager Administration, in conjunction with their environment, provide:

- Security audit that includes a chronological logging of events that acts as a deterrent against security violations;

- Protection of user private and public keys and CIMC secret keys against unauthorized modification and disclosure;
- Recognized cryptographic functionality, key management and operational use of cryptographic keys;
- Protection of user data including certificate issuance, revocation, backup and recovery, and profile management of certificates and Certificate Revocation List (CRL);
- Identification and Authentication that supports the administration and enforcement of access control policies to unambiguously identify the person and/or entity performing functions on the CIMC;
- Management of security functions including distinct roles to maintain the security of the CIMC;
- Functions that manage and protect the integrity of confidential data from disclosure and modification through the use of encryption, reliable time stamps, backup and recovery procedures, self-tests and audit logs; and
- Protection from modification and disclosure of transmitted data by means of a secure communications path between the CIMC and local and remote users.

1.4.3 TOE Roles

The CIMC PP defines four specific roles: Administrator, Operator, Officer and Auditor. This Security Target uses only three of those CIMP PP defined roles: Administrator, Officer and Auditor. In this context, the CIMC PP Operator role (which performs system backup and recovery) is included as part of the Administrator role.

The CIMC PP defined roles can be mapped to Entrust Authority roles as indicated in Table 1-1-1 below.

Table 1-1-1 Roles Description

Entrust Authority Role	Description	Corresponding CIMC PP Role
Master User	Master Users are responsible for the initial configuration of Entrust Authority, for its ongoing maintenance and database integrity. Other functions include performing database backups and starting and stopping services as needed.	Administrator
Security Officer	The main role of the Security Officer is to set and administer the organization's security policy as it applies to all Entrust users in the organization. Security Officers may also add, delete, and configure other administrative users The Security Officer may also define and configure new roles. Security Officers also have end-entity management privileges, and are Entrust end users (end-entities) themselves.	
Administrator	The main role of the Administrator is to manage X.509 end-entities. This includes the ability to add, enable, disable, change end user DNs, recover Entrust users, and to revoke certificates. Administrators may also view and modify Directory content and review audit logs. Administrators are also end-users	Officer
EAC Administrator	The main role of the EAC Administrator is to manage either a CVCA or a DV infrastructure. In the case of a CVCA EAC Administrator, this involves managing the CVCA itself and relationships with DVs. In the case of a DV EAC Administrator, this involves managing the DV itself, relationships with CVCAs and managing ISs under its control.	Officer
EAC Auditor	The main role of the EAC Auditor is to review EAC audit logs and	Auditor

	create reports	
Auditor	The main role of the Auditor is to review audit logs and create reports.	Auditor

There are additional roles supported by Entrust Authority that have no direct mapping to the CIMC PP roles and are outside the scope of this TOE. These include:

- **Directory Administrator:** Responsible for maintaining the Directory used as a repository for X.509 certificates, CRLs and ARLs.
- **Self-Administration Server Administrator:** Optional role used with Entrust Authority Self Administration Server product to facilitate automatic enrollment of X.509 users.
- **Custom-defined (flexible) Roles:** The configuration of roles provides the ability to grant or deny administrative access to various operations including: user administration operations (e.g., enable user, recover user, revoke certificate), types of certificates, security policy operations, audit log access, directory operations, and database operations.
- **End User:** End Users are the ultimate recipients of Entrust Authority services. An end user is a recipient of credentials, a creator of signed and/or encrypted information, or, in other terms, the ultimate consumer of the CIMC services provided by Entrust Authority. End user privileges are enforced by Entrust Authority, directly in the case of initialization and key recovery, and indirectly via certificates and revocation lists issued by Entrust Authority.

1.4.4 High Level Architecture

Figure 1 illustrates the high level of architecture of an Entrust Authority infrastructure. This infrastructure includes the components necessary to satisfy all requirements of a CIMC as well as the components that complete the infrastructure, such as end users. Additional optional components such as smartcards and HSMs, although frequently added to deployments, have been excluded for simplicity.

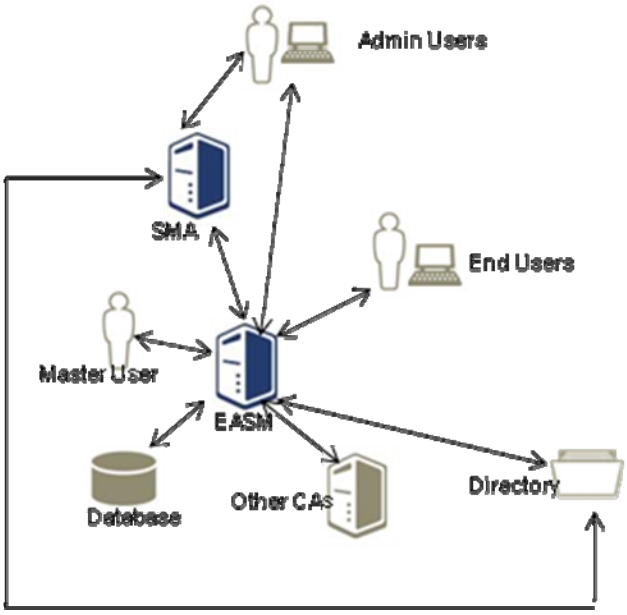

Figure 1: Entrust Authority Infrastructure Components

The following subsections outline the major components.

1.4.4.1 Entrust Authority Security Manager

EASM is the Certification Authority (CA) and core component of the Entrust Authority system. The main functions of EASM are to:

- Creation of encryption key pairs for users;
- Creation of certificates for all public keys;
- Management of a secure database that allows the recovery of users' encryption key pairs; and
- Enforcement of an organization's security policy.

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

- Ability to interoperate with other CAs or with other vendors' CA or PKI-enabled products;
- Ability to support and maintain a strict PKI hierarchy and peer-to-peer relationships with other CAs, and provide fine-grained control to limit relationships between CAs;
- Ability to specify and modify what administrators and users can do through the flexible configuration of roles, groups, user registration dialogs, and user settings;
- Use of flexible certificates (to include any extensions in the [X.509] standard or any properly formatted proprietary extension);
- Use of X.509 attribute certificates to support privilege management for end users;
- Use of ISO 7816 certificates to support EAC for ePassports;
- Ability to change the distribution of setup information to users and to specify the authorization code lifetime;
- Use of flexible password rules for Security Officers, Administrators and users;

- Ability to support N user key pairs;
- Ability to specify CA signing algorithm and CA signing key size;
- Ability to specify the CVCA signing algorithm and key size;
- Ability to specify DV signing algorithms and key sizes; and
- Ability to renew the CA signing key pair, CVCA signing key pair or DV signing key pairs before they expire and to recover from possible CA key compromise.

EASM is comprised of 3 primary modules:

SM Core is the module that contains all core services of the CA including software cryptographic modules, database protection and backup, communication with the database and directory, certificate and CRL signing etc.

SM Services is the module that monitors external interfaces and establishes communication with other components including EASMA, end-users etc. Several protocols are supported for this communication, including the IETF standard Certificate Management Protocol as defined in [CMP]. SM Services module is layered between the external entities and the SM Core module.

SM Control is the module that interfaces with Master User to facilitate management of EASM itself. This module is layered between Master User and SM Core to facilitate these services.

1.4.4.2 Entrust Authority Security Manager Administration

EASMA is a "thick" PKI Client application that is the graphical administrative interface to the Entrust Authority system. It is used by Security Officers, Administrators, Directory Administrators, Auditors, and custom-defined roles (with a customizable set of permissions). Primary uses for the EASMA includes:

- Renewal of the CA signing key pair before it expires and recover from possible CA key compromise;
- Addition and deletion of users;
- Revocation of X.509 certificates;
- Initiation of X.509 key recovery operations;
- Configuration of security policies; and
- Review of audit logs.

Security Officers, Administrators, and other administrative roles logging on to EASMA authenticate themselves using digital signatures. Once complete, all messages between EASMA and EASM are then secured for confidentiality, integrity, and authentication.

1.4.4.3 Database

EASM stores information about users and about the infrastructure itself in a database. This data is encrypted and protected by EASM. If an HSM is used, the database protection keys are managed by the HSM.

The Security Manager Database stores:

- X.509 CA signing key pair (unless an HSM is used);
- X.509 user status information, including the distinguished name (DN) of each user;
- Encryption key pair history for X.509 users, which includes all decryption private keys and encryption public key certificates for each user;

- Verification public key history for X.509 users, which includes all verification public key certificates for each user;
- Validity periods for user signing key pairs, user encryption key pairs, and system cross-certificates; and
- Security Officer and Administrator information.

In a CVCA deployment, the Database also stores

- CVCA signing key pair (unless an HSM is used) and any associated history of certificates; and
- Information about local and foreign DVs, including certificates and request status information.

In a DV deployment, the Database also stores

- DV signing key pairs (unless an HSM is used) and any associated history of certificates (DVs may have multiple valid signing keys at any one time – generally one per CVCA with which they have a relationship);
- Information about the local CVCA and foreign CVCAs with which they have a relationship, including certificates and request status information; and
- Information about local ISs they manage.

EASM enforces access control and maintains integrity of these resources.

1.4.4.4 Directory

The Directory is a repository of public information. It contains the name of each end entity in the X.509 CA domain. Public key certificates of each user, certificate revocation lists (lists of certificates that have been revoked for various reasons), and other information is written from EASM to the Directory.

The Directory Administrator is responsible for adding and removing people's names in the Directory. Entrust uses this entry to store the user's encryption public key certificate. The Directory Administrator can also add extra information to the Directory that shows the organization's geographical distribution or organizational hierarchy, and other user data such as email addresses etc. Security Manager provides mechanisms to maintain the authenticity and integrity of resources stored in the Directory.

The Directory is only used for X.509 certificates. In a CVCA or DV deployment, the Directory only holds information about entities that are issued X.509 certificates, such as administrators. CVCAs, DVs and ISs are issued ISO 7816 signature verification certificates, not encryption certificates. These are not stored in the Directory.

1.4.4.5 Cryptographic Modules

All cryptographic operations in the Entrust Authority TOE are performed in FIPS 140-2 validated cryptographic modules (CM).

The most sensitive operations, including key generation, management and use of CA signing keys and database protection keys can be performed either in a software CM in EASM or a 3rd party HSM. For this evaluation, these operations are performed in a 3rd party FIPS 140-2 Level 3 validated HSM that is outside the scope of this evaluation.

Other cryptographic operations are performed in Entrust Base Security Kernel CM version 8.0. which will be validated to FIPS 140-2 Level 2. (FIPS validation certificate number t.b.d.).

There are Entrust software CMs present in each of the components within the TOE.

1.4.5 TOE Boundary

The set of software of the TOE that must be relied upon for the correct enforcement of the TSP is included in the TOE boundary. The Entrust Authority TOE boundary is indicated in **Figure 2**.

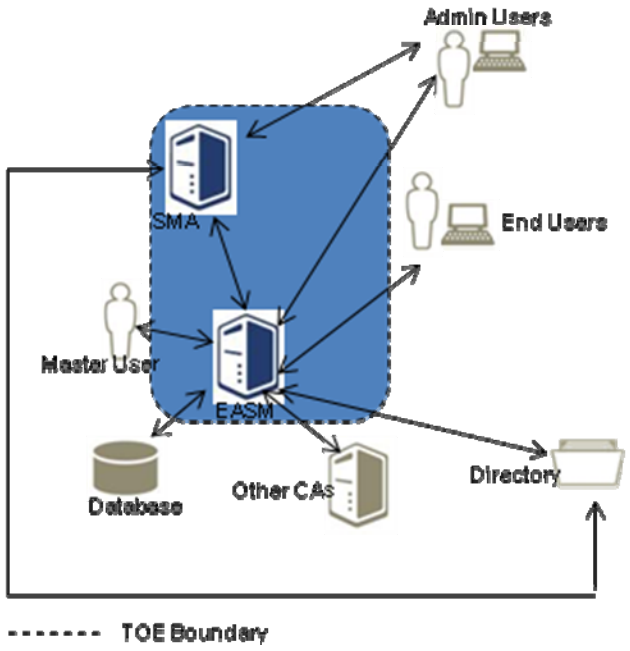

Figure 2: TOE Boundary

The components that are included within the Entrust Authority TOE boundary are:

Software Components:

- Entrust Authority Security Manager:
- Entrust Authority Security Manager Administration

Guidance Materials:

- Entrust Authority Security Manager 8.1 SP1 Documentation Suite (ZIP file containing all EASM 8.1 SP1 core documentation)
- Entrust Authority Security Manager 8.1 SP1 Release Notes
- Entrust Authority Security Manager 8.1 SP1 Deployment Guide
- Entrust Authority Security Manager 8.1 SP1 Directory Configuration Guide
- Entrust Authority Security Manager 8.1 SP1 Directory Configuration Files (ZIP file)
- Entrust Authority Security Manager 8.1 SP1 Installation Guide
- Entrust Authority Security Manager 8.1 SP1 Operations Guide
- Entrust Authority Security Manager Administration 8.1 SP1 Documentation Suite (ZIP file containing all EASMA 8.1 SP1 core documentation, except the online help)
- Entrust Authority Security Manager Administration 8.1 SP1 Release Notes
- Entrust Authority Security Manager Administration 8.1 SP1 User Guide

- Entrust Authority Security Manager Administration 8.1 SP1 Online Help (EXE file for installing the EASMA 8.1 SP1 Online Help)

1.4.5.1 Exclusion from the TOE Boundary

The components excluded from the Entrust Authority TOE boundary are given below. The justification for excluding these components is provided in the sections to follow.

- Security Manager Database
- Directory
- Hardware and operating system platform (Abstract Machine)
- Hardware Security Module
- Administrator and User desktop systems
- Optional EASM and EASMA features

1.4.5.1.1 Security Manager Database

The justification for excluding the database from the Entrust Authority TOE boundary is based on the following factors:

- **Database security provided by Entrust:** This Security Target makes no claims about inherent database security. All database security (i.e., confidentiality and integrity) is provided by Entrust (through the FIPS-validated cryptographic module), not the database. As such, all sensitive data items stored in the Security Manager database are encrypted to support the TOE Access Control SFP, and provided with integrity protection to generate MACs for each data item.
- **Database functionality not mapped to SFRs:** This Security Target makes no claims about database functionality (aside from the inherent, fundamental, and basic function of data storage). The Security Manager database operates only as a data warehouse for user and system data. Database functionality is not mapped to any of the SFRs in this Security Target.
- **Well-defined database interface:** The only interface to the database is through Security Manager and the ODBC-API. Any Security Manager database data items are in plaintext only while within the TOE boundary. Any Security Manager database data items transmitted across the TOE boundary are provided with confidentiality and integrity protection.

1.4.5.1.2 Directory

The justification for excluding the directory from the Entrust Authority TOE boundary is based on the following factors:

- **Directory functionality not mapped to SFRs:** This Security Target makes no claims about directory functionality (aside from the inherent, fundamental, and basic function of data storage). The directory operates only as a data warehouse for X.509 certificates. Directory functionality is not mapped to any of the SFRs in this Security Target.
- **Well-defined directory interface:** The only interface to the directory is through the LDAP interface. No directory items are considered sensitive since they are publicly available and all

certificates have inherent authenticity and integrity protection as they are digitally signed by the Security Manager CA.

1.4.5.1.3 Hardware and operating system platform (Abstract Machine)

The justification for excluding the abstract machine from the Entrust Authority TOE boundary is based on the following factors:

- **Operating system:** The TSP is enforced by the TOE and the SFRs are completely satisfied by TOE functions (aside from those with environmental dependencies). The operating system, with which the TOE interfaces, is assumed to be trusted, meaning that it can be relied upon to correctly execute the TOE functions. The Windows operating systems for each of the components within the TOE boundary used for this evaluation are all certified to the Common Criteria EAL4 level as illustrated on [NIAP site**]**.

- **Hardware independence:** The Entrust software is optimized to execute on any machine that satisfies the following Entrust system requirements.

  The following requirements are for EASM for a PKI of up to 2 million users. Stricter recommendations apply to larger deployments as are noted in EASM documentation:

  - 1 Gbyte of RAM
  - two CPUs, each running at 800 MHz (capacity approximately 500 transactions per minute)
  - Network: 100 kbits/s to 1 Mbit/s for communication between clients and the CA, full-duplex 10 Base-T for communication between the CA and the Directory
  - TCP/IP protocol stack installed
  - Striped mirrored disks (for example, RAID 1+0) for critical data

  The following requirements are for the EASMA system:

  - Pentium 300 Mhz or better
  - 256 Mbytes of RAM
  - 500 Mbytes of free disk space
  - a CD-ROM drive
  - TCP/IP protocol stack installed
  - minimum screen resolution of 800 x 600 pix

1.4.5.1.4 Hardware Security Module

The justification for excluding the hardware cryptographic device from the TOE boundary is that it is a 3rd party FIPS 140-2 validated crypto module.

1.4.5.1.5 Administrator and User Desktop Systems

PKI end-users are outside the scope of a CIMC as they have no CA or RA functionality. This ST makes no claims about administrator or end-user desktop systems or components.

1.4.5.1.6 Optional EASM and EASMA Features

EASM includes an optional service that enables EASM to communicate with Entrust client systems that pre-date the standard CMP protocol. This service supports two protocols (referred to in Entrust documentation as SEP and Proto-PKIX) that were based on early CMP drafts while that standard was evolving. There are no such legacy clients in this TOE. Therefore the SEP/ProtoPKIX and XAP services in SM Core are disabled for purposes of this evaluation, as well as the GUTS cryptographic module used by the XAP protocol. This ST makes no claims about these services, these protocols or the GUTS cryptographic module.

EASMA includes an optional service that enables EASMA to communicate with the Directory securely, using Secure LDAP and a separate cryptographic module. This service is disabled by default and disabled for purposes of this evaluation. This ST makes no claims about this service or the GUTS cryptographic module.

2 Conformance Claims

2.1 CC Conformance Claim

- Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July, 2009 [CC]
- CC Part 2 extended
- CC Part 3 conformant
- Security Assurance Level EAL 4 augmented with ALC_FLR.2

2.2 Protection Profile Claim

Certificate Issuing and Management Components Protection Profile, Version 1.1, December 27, 2010 [CIMP PP].

3 Security Problem Definition

This section includes the following:

- Assumptions;
- Threats; and
- Organizational security policies.

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

3.1 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).

3.1.1 Personnel Assumptions

A.Auditors Review Audit Logs
Audit logs are required for security-relevant events and must be reviewed by the Auditors.

A.Authentication Data Management
An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)

A.Competent Administrators, Officers and Auditors
Competent Administrators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

A.Cooperative Users
Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.

A.CPS
All Administrators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.

A.Disposal of Authentication Data
Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).

A.Malicious Code Not Signed
Malicious code destined for the TOE is not signed by a trusted entity.

A.Notify Authorities of Security Issues
Administrators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

A.Social Engineering Training
General users, Administrators, Officers and Auditors are trained in techniques to thwart social engineering attacks.

3.1.2 Connectivity

A.Operating System
The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the CIMC PP, as identified in this ST.

3.1.3 Physical

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.

3.2 Threats

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

3.2.1 Authorized Users

T.Administrative errors of omission
Administrators, Officers or Auditors fail to perform some function essential to security.

T.Administrators, Officers and Auditors commit errors or hostile actions
An Administrator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.

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.

3.2.2 System

T.Critical system component fails
Failure of one or more system components results in the loss of system critical functionality.

T.Flawed code
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

T.Malicious code exploitation
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.

T.Message content modification
A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.

3.2.3 Cryptography

T.Disclosure of private and secret keys
A private or secret key is improperly disclosed.

T.Modification of private/secret keys
A secret/private key is modified.

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

3.2.4 External Attacks

T.Hacker gains access
A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hacker physical access
A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

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

3.3 Organizational Security Policies

P.Authorized use of information
Information shall be used only for its authorized purpose(s).

P.Cryptography
FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

4 Security Objectives

This section includes the security objectives for 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 three categories: authorized users, cryptography, and external attacks.

4.1.1 Authorized Users

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

4.1.2 System

O.Preservation/trusted recovery of secure state
Preserve the secure state of the system in the event of a secure component failure and/or recover to a secure state.

4.1.3 Cryptography

O.Cryptographic functions
The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. (Validated is defined as FIPS 140-2 validated).

NOTE: This objective is included as an objective for the environment in the PP. It has been moved into the TOE in this ST, in accordance with extended components as defined in Section 5 of this ST.

O.Non-repudiation
Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.

4.1.4 External Attacks

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

4.2 Security Objectives for the Environment

This section specifies the security objectives for the environment.

O.Administrators, Officers and Auditors guidance documentation
Deter Administrator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.

O.Auditors Review Audit Logs
Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.

O.Authentication Data Management
Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)

O.Communications Protection
Protect the system against a physical attack on the communications capability by providing adequate physical security.

O.Competent Administrators, Officers and Auditors
Provide capable management of the TOE by assigning competent Administrators, Officers and Auditors to manage the TOE and the security of the information it contains.

O.Cooperative Users
Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE.

O.CPS
All Administrators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.

O.Disposal of Authentication Data
Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).

O.Installation
Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

O.Lifecycle security
Provide tools and techniques used during the development phase to ensure security is designed 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 entity prior to loading it into the system.

O.Notify Authorities of Security Issues
Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

O.Operating System
The operating system used is validated to provide adequate security, including domain separation and nonbypassability, in accordance with security requirements recommended 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 the TOE 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, Officers and Auditors in techniques to thwart social engineering attacks.

O. Sufficient backup storage and effective restoration
Provide sufficient backup storage and effective restoration to ensure that the system can be recreated.

O.Trusted Path
Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities.

O.Validation of security function
Ensure that security-relevant software, hardware, and firmware are correctly functioning through 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.

O.Configuration Management
Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.

O.Data import/export
Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

O.Detect modifications of firmware, software, and backup data
Provide integrity protection to detect modifications to firmware, software, and backup data.

O.Individual accountability and audit records
Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.

O.Integrity protection of user data and software
Provide appropriate integrity protection for user data and software.

O.Limitation of administrative access
Design administrative functions so that Administrators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Administrators who troubleshoot the system and perform system updates.

O.Maintain user attributes
Maintain a set of security attributes (which may include role membership. access privileges, etc.) associated with individual users. This is in addition to user identity.

O.Manage behavior of security functions
Provide management functions to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code

Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.

O.Procedures for preventing malicious code
Incorporate malicious code prevention procedures and mechanisms.

O.Protect stored audit records
Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

O.Protect user and TSF data during internal transfer
Ensure the integrity of user and TSF data transferred internally within the system.

O.React to detected attacks
Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.

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 by restricting auditable events.

O.Restrict actions before authentication
Restrict the actions a user may perform before the TOE authenticates the identity of the user.

O.Security-relevant configuration management
Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.

O.Time stamps
Provide time stamps to ensure that the sequencing of events can be verified.

O.User authorization management
Manage and update user authorization and privilege data to ensure they are consistent with 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.

4.4.1 Tracing Between Security Objectives and Security Problem Definition

The following five tables provide a mapping of security objectives to the environment defined by the assumptions, threats and policies, illustrating that each security objective covers at least one assumption, threat or policy and that each assumption, threat and policy is covered by at least one security objective. Table 4-1 maps assumptions to security objectives, listing which objectives each assumption helps to cover. Table 4-2 maps security objectives for the TOE to threats. Table 4-3 maps security objectives for the environment to threats. Table 4-4 maps security objectives for both the TOE and the environment to threats. Table 4-5 maps the organizational security policies to security objectives. The items in the tables are ordered alphabetically, sorted on the first column.

Table 4-1 Relationship of Assumptions to Security Objectives

Assumption	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, Officers and Auditors	O.Competent Administrators, Officers 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 Data	O.Disposal of Authentication 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

Table 4-2 Relationship of Security Objectives for the TOE to Threats

Security Objective	Threat
O.Certificates	T.Administrators, Officers and Auditors commit errors or hostile actions
O.Control unknown source communication traffic	T.Hacker gains access
O.Cryptographic functions	T.Disclosure of private and secret keys, T.Modification of secret/private keys
O.Non-repudiation	T.Sender denies sending information
O.Preservation/trusted recovery of secure state	T.Critical system component fails

Table 4-3 Relationship of Security Objectives for the Environment to Threats

Security Objective	Threat
O.Administrators, Officers and Auditors guidance documentation	T.Disclosure of private and secret keys, T.Administrators, Officers and Auditors commit errors or hostile actions T.Social engineering
O.Competent Administrators, Officers and Auditors	T.Administrators, Officers and Auditors commit errors or hostile actions
O.CPS	T.Administrative errors of omission
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 integrity	T.Malicious code exploitation
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, Officers and Auditors commit errors or hostile actions
O.Social Engineering Training	T.Social Engineering
O.Sufficient backup storage and effective restoration	T.Critical system component fails, T.User error makes data inaccessible
O.Trusted path	T.Hacker gains access, T.Message content modification
O.Validation of security function	T.Malicious code exploitation, T.Administrators, Officers and Auditors commit errors or hostile actions

Table 4-4 Relationship of Security Objectives for Both the TOE and the Environment to Threats

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, Officers and Auditors commit errors or hostile actions
O.Individual accountability and audit records	T.Administrative errors of omission, T.Hacker gains access, T.Administrators, Officers and 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, Officers and Auditors commit errors or hostile actions
O.Maintain user attributes	T.Administrators, Officers and Auditors commit errors or hostile actions
O.Manage behavior of security functions	T.Critical system component fails, T.Administrators, Officers and 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, Officers and 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, Officers and Auditors commit errors or hostile actions
O.Restrict actions before authentication	T.Hacker gains access, T.Administrators, Officers and Auditors commit

Security Objective	Threat
	errors or hostile actions
O.Security-relevant configuration management	T.Administrative errors of omission
O.Time stamps	T.Critical system component fails, T.Administrators, Officers and Auditors commit errors or hostile actions

Table 4-5 Relationship 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

4.4.2 Tracing Justification

The following discussions provide information regarding:

1) Why the identified security objectives uphold each assumption;
2) Why the identified security objectives provide for effective countermeasures to the threats; and
3) Why the identified security objectives provide complete coverage of each organizational security policy.

4.4.2.1 Assumptions and Objectives Sufficiency

Personnel

A.Auditors Review Audit Logs establishes that audit logs are necessary for security-relevant events and that they must be reviewed by auditors. This is addressed by

> **O.Auditors Review Audit Logs**, which ensures that security-relevant events recorded in audit logs are reviewed by auditors.

A.Authentication Data Management establishes that management of user authentication data is external to the TOE. This is addressed by

> **O.Authentication Data Management**, which ensures that users modify their authentication data in accordance with appropriate security policy.

A.Competent Administrators, Officers and Auditors establishes that security of the TOE is dependent upon those that manage it. This is addressed by

> **O.Competent Administrators, Officers and Auditors**, which ensures that the system managers will be competent in its administration.

A.Cooperative Users establishes that a secure IT environment is required to securely operate the TOE, and that users must work within the constraints of that environment. This is addressed by

> **O.Cooperative Users**, which ensures that users will cooperate with the constraints established.

A.CPS establishes that Administrators, Officers, and Auditors are familiar with the CP and CPS under which the TOE is operated. This is addressed by

> **O.CPS**, which ensures that Administrators, Officers, 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 their authorization has been removed. This is addressed by

> **O.Disposal of Authentication Data**, which ensures that access 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 it will not be loaded onto the system.

A.Notify Authorities of Security Issues establishes that users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss of compromise of data. This is addressed by

> **O.Notify Authorities of Security Issues** which ensures that user notify proper authorities of any security issues that impact their systems.

A.Social Engineering Training establishes that individuals will attempt to gain access to the system using social engineering practices. This is addressed by

> **O.Social Engineering Training**, which ensures that all users will be training to thwart social engineering attacks.

Connectivity

A.Operating System establishes that an insecure operating system will compromise system security. This is addressed by

> **O.Operating System**, which ensures that an operating system that meets security requirements recommended by the National Institute of Standards and Technology will be used.

Physical

A.Communications Protection establishes that the communications infrastructure is outside the TOE. This is addressed by

> **O.Communications Protection**, which ensures that adequate physical protections are afforded the necessary communications infrastructure.

A.Physical Protection establishes that physical modification of the TOE hardware, software, and firmware will compromise system security. This is addressed by

> **O.Physical Protection**, which ensures that adequate physical protection will be provided.

4.4.2.2 Threats and Objectives Sufficiency

Authorized users

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

> **O.CPS** provides Administrators, Officers, and Auditors with information regarding the policies and practices used by the system. Providing this information ensures that these authorized users of the system are aware of their responsibilities, thus reducing the likelihood that they will fail to perform a security-critical operation.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. These audit records will expose administrators that fail to perform security-critical operations so they can be held accountable.
>
> **O.Security-relevant configuration management** ensures that system security policy data and enforcement functions, and other security-relevant configuration data are managed and updated. This ensures that they are consistent with organizational security policies and that all changes are properly tracked and implemented.

T.Administrators, Officers and Auditors commit errors or hostile actions addresses:

- Errors committed by administrative personnel that directly compromise organizational security objectives, change the technical security policy enforced by the system or application, or
- Malicious obstruction by administrative personnel of organizational security objectives or modification of the system's configuration to allow security violations to occur.

It is countered by:

> **O.Competent Administrators, Officers and Auditors** ensures that users are capable of maintaining effective security practices. This reduces the likelihood that they will commit errors.
>
> **O.Administrators, Officers and Auditors guidance documentation** which deters administrative personnel errors by providing adequate guidance.
>
> **O.Certificates** ensures that certificates, certificate revocation lists, and certificate status information are valid. The validation of information provided by Officers that is to be included in certificates helps to prevent improperly entered information from appearing in certificates.
>
> **O.Detect modifications of firmware, software, and backup data** ensures that if the backup components have been modified, that it is detected.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. These audit records will expose administrators that perform inappropriate operations so they can be held accountable.
>
> **O.Limitation of administrative access**. The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for

necessary exceptions. In general, the exceptions tend to be role specific. Limiting the set of operations that a user may perform limits the damage that a user may cause.

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

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

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 Auditor shall be audited if the audit trail is full. This ensures that operations that are performed by users other than the Auditor are audited and so can be detected.

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

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

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

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

T.User abuses authorization to collect and/or send data addresses the situation where an authorized user abuses granted authorizations by browsing files in order to collect data and/or violates export control policy by sending data to 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 is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This audit records will expose users who abuse their authorized to collect and/or send data.

T.User error makes data inaccessible addresses a user accidentally deleting user data. Consequently, the user data is 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 automatic response.
- User does not understand the implications of the prompt at hand and inadvertently gives a response that deletes user data.
- 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 effective restoration to recreate the system, when required. This ensures that user data is available from backup, even if the current copy is accidentally deleted.

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

System

T.Critical system component fails addresses the failure of one or more system components that results in the loss of system-critical functionality. This threat is relevant when there are components that may fail due to hardware and/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. The configuration management program includes configuration identification and change control. This ensures that critical system components do not fail as a result of improper configuration.

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

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

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

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

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

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

O.Repair identified security flaws. The vendor repairs security flaws that have been identified by a user. Such security 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 accidental flaws are lack of engineering detail or bad design. An example of a deliberate flaw would be the inclusion of a trapdoor 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 and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of 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. The configuration management program includes configuration identification and change control. This ensures that malicious code is not introduced during the configuration process.

O.Integrity protection of user data and software ensures that appropriate integrity protection is provided for user data 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 after malicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removed as part of the process.

O.Periodically check integrity ensures that periodic integrity checks are performed on both system and software. If these 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 prevent incorporation of malicious code into the system.

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

O.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctly functioning 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 the likelihood that malicious code was included in the product by the developer. O.Lifecycle security also addresses the detection and resolution of flaws discovered during the operational phase, such as modifications of components by malicious code.

T.Message content modification addresses the situation where a hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient. Several kinds of modification are possible: modification of a single message, deletion or reordering of selected messages, insertion of bogus messages, replay of previous messages, and modification of accompanying message security attributes. It is countered by:

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

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

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

Cryptography

T.Disclosure of private and secret keys addresses the unauthorized disclosure of secret and/or private keys. It is countered by:

> **O.Administrators, Officers and Auditors guidance documentation** ensures that adequate documentation on securely configuring and operating the CIMC is available to Administrators, Officers and Auditors. This documentation will minimize errors committed by those users.
>
> **O.Cryptographic functions** ensures that TOE implements approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and uses validated cryptographic modules. Use of validated cryptographic modules ensures that cryptographic keys are adequately protected when they are stored within cryptographic modules.
>
> **O.Limitation of administrative access**. The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific. Limiting the number of users who have access to cryptographic keys reduces the likelihood of unauthorized disclosure.
>
> **O.Protect user and TSF data during internal transfer** protects private and secret keys from unauthorized disclosure during transmission between separated parts of the TOE.

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 for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and uses validated cryptographic modules. Use of validated cryptographic modules ensures that cryptographic keys are adequately protected when they are stored within cryptographic modules.
>
> **O.Integrity protection of user data and software** that ensures that appropriate integrity protection is provided for secret and private keys.
>
> **O.Object and data recovery free from malicious code** ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. If the malicious code cause private or secret keys to be revised in an unauthorized manner, this objective ensures that they are recovered to their correct values.
>
> **O.Protect stored audit records** ensures that audit records are protected against unauthorized access, modification, or deletion to provide for traceability of user actions. This objective ensures that modifications to private and secret keys can be detected through the audit trail.

T.Sender denies sending information addresses the situation where the sender of a message denies sending the message 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 the message to the recipient.

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 user is authenticated. This prevents a hacker who is unable to circumvent the access control mechanisms from performing security-relevant operations.

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

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

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

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

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

T.Hacker physical access addresses the threat where an individual exploits physical security weaknesses to gain physical control of system components. It is countered by:

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

T.Social Engineering addresses the situation where a hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation. It is countered by:

O.Administrators, Officers and Auditors guidance documentation which deters administrative personnel errors by providing adequate guidance.

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

O.Social Engineering Training which ensures that general users, Administrators, Officers, and Auditors are trained in techniques to thwart social engineering attacks.

4.4.2.3 Policies and Objectives Sufficiency

P.Authorized use of information establishes that information is used only for its authorized purpose(s). This is addressed by

O.Restrict actions before authentication ensures that the capability to perform security-relevant operations is limited to those who have been authorized to perform those operations.

O.Maintain user attributes, **O.Security roles**, and **O.User authorization management** ensure that users are only authorized to perform those operations that are necessary to perform their jobs.

O.Auditors review 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 the TOE. This is addressed by

O.Cryptographic functions which ensures that such standards are used.

5 Extended Components Definition

All extended components are defined in the [CIMC PP]. These components are included in this ST as they specify required functionality of a CIMC.

5.1 Extended FCO Components

5.1.1 Enforced Proof of Origin and Verification of Origin

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

Hierarchical to: FCO_NRO.2

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 [ST assignment: *other attributes*] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

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

Dependencies: FIA_UID.1 Timing of identification

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 and O.Control unknown source communication traffic.

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

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

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

The TSF may, for example, accept information whose origin can not be verified under in the following cases:

a) The received information is a request for public information (e.g., an Online Certificate Status Protocol (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 had originated from the authorized user who approved it.

5.1.2 Advanced Verification of Origin

FCO_NRO_CIMC.4 Advanced verification of origin

Hierarchical to: No other components.

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.

Dependencies: FCO_NRO_CIMC.3

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.

5.2 Extended FCS Components

5.2.1 CIMC Private and Secret Key Zeroization

FCS_CKM_CIMC.5 CIMC private and secret key zeroization

Hierarchical to: No other components.

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.

Dependencies: FCS_CKM.4 Cryptographic key destruction

5.2.2 CIMC Strength of Functions

FCS_SOF_CIMC.1 CIMC Strength of Functions

FCS_SOF_CIMC.1.1 The TSF shall provide cryptographic mechanisms that fulfill the specific Strength of Function requirements of section 5.2.2.1.

Dependencies: No dependencies

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

5.2.2.1 Cryptographic Modules

FIPS 140-2 validated cryptographic modules must perform all cryptographic functions performed by CIMCs. FIPS 140-2 validated cryptographic modules are also required to generate cryptographic keys and to store plaintext private and secret keys.

5.2.2.1.1 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 the most current version can be found at http://csrc.nist.gov/cryptval.

a) Encryption Algorithms

The encryption specified for:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification of origin
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 performed using a FIPS-approved or recommended algorithm.

b) 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.

c) 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.

d) Authentication Codes

The authentication code specified in:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification 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.

5.3 Extended FDP Components

5.3.1 User Private Key Confidentiality Protection

FDP_ACF_CIMC.2 User private key confidentiality protection

Hierarchical to: No other components

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.

Dependencies: No dependencies

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

5.3.2 User Secret Key Confidentiality Protection

FDP_ACF_CIMC.3 User secret key confidentiality protection

Hierarchical to: No other components

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.

Dependencies: No dependencies

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

5.3.3 Certificate Generation

FDP_CIMC_CER.1 Certificate Generation

Hierarchical to: No other components.

FDP_CIMC_CER.1.1 The TSF shall only generate certificates whose format complies with [ST assignment*: the X.509 standard for public key certificates, other standard (ST shall specify the standard and ST author shall ensure that a description of the format is available), or ST specified format (ST shall include a description of the format)*].

Application note: The ST should specify the format (or formats) used to generate certificates. If a standard format is not used, then the ST shall include a description of the format.

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

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

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

a) The version field shall contain the integer 0, 1, or 2.
b) If the certificate contains an issuerUniqueID or subjectUniqueID then the version field shall contain the integer 1 or 2.
c) If the certificate contains extensions then the version field shall contain the integer 2.
d) The serialNumber shall be unique with respect to the issuing Certification Authority.

e) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
f) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
g) If the subject field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical subjectAltName extension.
h) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a FIPS-approved or recommended algorithm.

Dependencies: No dependencies.

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

5.3.4 Certificate Revocation List Validation

FDP_CIMC_CRL.1 Certificate revocation list validation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies

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

5.3.5 Certificate Status Export

FDP_CIMC_CSE.1 Certificate status export

Hierarchical to: No other components

FDP_CIMC_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with [ST assignment*: the X.509 standard for CRLs, the OCSP standard as defined by RFC 2560, other standard (ST shall specify the standard and ST author shall ensure that a description of the format is available), or ST specified format (ST shall include a description of the format)*].

Application note: The ST should specify the format used to supply certificate status information. If a standard format is not used, then the ST shall include a description of the format.

Dependencies: No dependencies

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

NOTE: If certificate status information is exported using the X.509 CRL format, then the functional security requirements FDP_CIMC_CRL.1 and either FMT_MOF_CIMC.4 (Security Level 1) or FMT_MOF_CIMC.5 (Security Levels 2-4) apply. If certificate status information is exported using the X.509 CRL format, then the functional security requirements FDP_CIMC_OCSP.1 and FMT_MOF_CIMC.6 apply.

5.3.6 Extended User Private and Secret Key Export

FDP_ETC_CIMC.5 Extended user private and secret key export

Hierarchical to: FDP_ETC_CIMC.4

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.

Dependencies: No dependencies

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

5.3.7 Stored Public Key Integrity Monitoring and Action

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

Hierarchical to: No other components

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, 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 [ST assignment: *action to be taken if the verification fails, with the ST rationale showing why this completion is consistent with maintenance of security*].

Application Note: The ST should specify the actions to be taken in case the verification fails.

Dependencies: No dependencies

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

5.4 Extended FMT Components

5.4.1 Extended Certificate Profile Management

FMT_MOF_CIMC.3 Extended certificate profile management

Hierarchical to: FMT_MOF_CIMC.2

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.

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

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.

5.4.2 Extended Certificate Revocation List Profile Management

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: FMT_MOF_CIMC.4

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

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

- issuer;
- issuerAltName (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.)
- nextUpdate (i.e., lifetime of a CRL).

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

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

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.

5.4.3 Private Key Confidentiality Protection

FMT_MTD_CIMC.4 TSF private key confidentiality protection

Hierarchical to: No other components

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.

Dependencies: No dependencies

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

5.4.4 Secret Key Confidentiality Protection

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

Hierarchical to: No other components

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.

Dependencies: No dependencies

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

5.4.5 Extended TSF Private and Secret Key Export

FMT_MTD_CIMC.7 Extended TSF private and secret key export

Hierarchical to: FMT_MTD_CIMC.6

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.

Dependencies: No dependencies

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

5.5 Extended FPT Components

5.5.1 Audit Log Signing Event

FPT_CIMC_TSP.1 Audit log signing event

Hierarchical to: No other components.

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.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MOF.1 Management of security functions behavior

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 at Security Levels 2 and 3.

6 Security Requirements

6.1 Security Functional Requirements

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

Table 6-1: TOE Functional Security Requirements

Security Requirement		Component
Security Audit (FAU)	Audit data generation	FAU_GEN.1
	User identity association	FAU_GEN.2
	Selective audit	FAU_SEL.1
	Protected audit trail storage	FAU_STG.1
	Prevention of audit data loss	FAU_STG.4
Communication (FCO)	Enforced proof of origin and verification of Remote Data Entry and Export	FCO_NRO_CIMC.3
	Advanced verification of origin Remote Data Entry and Export	FCO_NRO_CIMC.4
Cryptographic Support (FCS)	Cryptographic key generation	FCS_CKM.1
	Cryptographic key destruction	FCS_CKM.4
	CIMC private and secret key zeroization	FCS_CKM_CIMC.5
	Cryptographic operation	FCS_COP.1
	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
	Extended user private and secret key export	FDP_ETC_CIMC.5
	Basic internal transfer protection (iterations 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 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
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 (iterations 1 and 2)	FPT_ITT.1
	Reliable time stamps	FPT_STM.1

6.1.1 Security Audit

FAU_GEN.1 Audit data generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimum level of audit; and
c) The events listed in Table 6-2 below.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, the information specified in the Additional Details column in Table 6-2 below.

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

Table 6-2 Auditable 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.
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	FCS_CKM.1 Cryptographic 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	

Section/Function	Component	Event	Additional Details
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 Officer, etc.).
Certificate Status Change Approval		All requests to change the status of a certificate.	Whether the request was accepted or rejected.
CIMC Configuration		Any security-relevant changes to the configuration of the TSF	
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

FAU_GEN.2 User identity association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SEL.1 Selective audit
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

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

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

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to detect unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the Auditor, if the audit trail is full.

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies.

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

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.

6.1.2 Roles

FMT_MOF.1 Management of security functions behavior
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in Table 6-3. to the authorized roles as specified in Table 6-3.

Table 6-3 Authorized Roles for Management of Security Functions Behavior

Section/Function	Component	Function/Authorized Role

Section/Function	Component	Function/Authorized Role
Security Audit		The capability to configure the audit parameters shall be restricted to Administrators. The capability to change the frequency of the audit log signing event shall be restricted to Administrators.
Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers. If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Officers.
Data Export and Output		The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer or Auditor.
Certificate Status Change Approval		Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.
CIMC Configuration		The capability to configure any TSF functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)
Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administrators.
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.

6.1.3 Access Control

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in 8 on *[subjects: all users and their associated roles to execute the following objects: certificate requests, certificate revocation requests, data export and output, key generation, private key load, private key storage, trusted public key entry deletion and storage, secret key storage, private and secret key destruction, private and secret key export, and certificate status change].*

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 8 to objects based on the identity of the subject and the set of roles that the subject is authorized to assume.

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

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

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

Table 6-4 Access Controls

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

Section/Function	Event
	private keys shall be restricted to Officers. The export of a certificate subject private key shall require the authorization of at least two Officers or one Officer and an Administrator or Auditor.
Certificate Status Change Approval	Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold. Only Officers shall be capable of removing a certificate from on hold status. Only Officers shall be capable of approving the placing of a certificate on hold. Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate. Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

6.1.4 Identification and Authentication

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components

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].

Dependencies: No dependencies

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

FIA_UAU.1.1 The TSF shall allow *[access to the login screen and help menu from the EASMA user interface]* on behalf of the user to be performed before the user is authenticated.

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

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

FIA_UID.1.1 The TSF shall allow *[access to the login screen and help menu from the EASMA user interface]* on behalf of the user to be performed before the user is identified.

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

FIA_USB.1 User-subject binding
Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users: [*only Administrators and Security Officers are authorized to associate user security attributes*]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users: [*only Administrators and Security Officers are authorized to associate user security attributes*]

6.1.5 Remote Data Entry and Export

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin
Hierarchical to: FCO_NRO.2
Dependencies: FIA_UID.1 Timing of identification

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.

FDP_ITT.1 Basic internal transfer protection (iteration 1)
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 8 to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1 Basic internal transfer protection (iteration 2)
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 8 to prevent the disclosure of confidential user data when it is transmitted between physically separated parts of the TOE.

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.
Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 8 to transmit confidential objects in a manner protected from unauthorized disclosure.

FPT_ITC.1 Inter-TSF confidentiality during transmission
Hierarchical to: No other components.
Dependencies: No dependencies

FPT_ITC.1.1 The TSF shall protect all confidential TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1)
Hierarchical to: No other components.
Dependencies: No dependencies

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

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 2)
Hierarchical to: No other components.
Dependencies: No dependencies

FPT_ITT.1.1 The TSF shall protect all confidential TSF data from disclosure when it is transmitted between separate parts of the TOE.

FCO_NRO_CIMC.4 Advanced verification of origin
Hierarchical to: No other components.
Dependencies: FCO_NRO_CIMC.3

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.

6.1.5.1 Certificate Status Export

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].*

6.1.6 Key Management

6.1.6.1 Private Key Storage

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The FIPS 140-2 validated cryptographic modules shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[RSA,RSA-PSS, DSA, ECDSA, CAST5, 3DES and AES]* and specified cryptographic key sizes

- *[1024, 1280, 1536, 2048, 3072, 4096 and 6144 (RSA and RSA-PSS),*
- *512 and 1024 (DSA),*
- *160, 163, 191, 192, 193, 224, 233, 239, 256, 283, 320, 359, 384, 409, 431, 512, 521 and 571 (ECDSA), 80 to 128 bit (CAST5),*
- *192 bit (3DES), and*
- *256 bit (AES)]*

that meet the following: *[FIPS PUB 186-2 (RSA and DSA),Draft FIPS PUB 186-3 (RSA-PSS), ANSI X9.62-2005 Annexes E.7, B, L.3, L.4, L.5, L.6, FIPS PUB 186-2 Appendix 6 (ECDSA), FIPS 186-2 APPENDIX 3 (CAST5, 3DES and AES) and PUB 197 (AES)]*.

FIPS validation certificate numbers t.b.d.

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

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.

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.

6.1.6.2 Public Key Storage

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

6.1.6.3 Secret Key Storage

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 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.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.

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

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

6.1.6.4 Private and Secret Key Destruction

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.

6.1.6.5 Private and Secret Key Export

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

FMT_MTD_CIMC.7 Extended TSF private and secret key export
Hierarchical to: FMT_MTD_CIMC.6
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.

6.1.7 Certificate Profile 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 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.

6.1.8 Certificate Revocation List Profile Management

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.

6.1.9 Certificate Registration

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 or with the ePassport Extended Access Control TR-03110]*.

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

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

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

a) The version field shall contain the integer 0, 1, or 2.
b) If the certificate contains an issuerUniqueID or subjectUniqueID then the version field shall contain the integer 1 or 2.
c) If the certificate contains extensions then the version field shall contain the integer 2.
d) The serialNumber shall be unique with respect to the issuing Certification Authority.
e) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
f) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
g) If the subject field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical subjectAltName extension.
h) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a FIPS-approved or recommended algorithm.

6.1.10 Certificate Revocation

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. At a minimum, the following items shall be validated:

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

6.1.11 Strength of Function

FCS_SOF_CIMC.1 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 6.1.11.1.

6.1.12 Cryptographic Operations

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The FIPS 140-2 validated cryptographic modules shall perform *[encryption and decryption, digital signature generation and verification, hashing, Message Authentication Code (MAC) generation and verification]* in accordance with a specified cryptographic algorithm *[RSA,RSA-PSS, DSA, ECDSA, CAST5, 3DES and AES]* and cryptographic key sizes

- *[1024, 1280, 1536, 2048, 3072, 4096 and 6144 (RSA and RSA-PSS),*
- *512 and 1024 (DSA),*
- *160, 163, 191, 192, 193, 224, 233, 239, 256, 283, 320, 359, 384, 409, 431, 512, 521 and 571 (ECDSA), 80 to 128 bit (CAST5),*
- *192 bit (3DES), and*
- *256 bit (AES)]*

that meet the following: *[FIPS PUB 186-2 (RSA and DSA),Draft FIPS PUB 186-3 (RSA-PSS), ANSI X9.62-2005 Annexes E.7, B, L.3, L.4, L.5, L.6, FIPS PUB 186-2 Appendix 6 (ECDSA), FIPS 186-2 APPENDIX 3 (CAST5, 3DES and AES) and PUB 197 (AES)]*.

(FIPS validation certificate numbers t.b.d.)

6.2 Security Assurance Requirements

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

Table 6-5 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.2: Flaw reporting procedures.

Table 6-5 Assurance Requirements

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

AVA: Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

6.3 Security Requirements Rationale

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

6.3.1 Security Requirements Coverage

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

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 6-6, addresses the mapping of security functional requirements to security objectives for the TOE. The second table, Table 6-7, addresses the mapping of security assurance requirements to security objectives for the TOE.

Table 6-6 Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
FAU_GEN.1 Audit data generation	O.Individual accountability and audit records
FAU_GEN.2 User identity 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 and verification of origin	O.Non-repudiation, O.Control unknown source communication traffic
FCO_NRO_CIMC.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM.1 Cryptographic key generation	O.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_COP.1 Cryptographic operation	O.Cryptographic functions
FCS_SOF_CIMC.1 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 malicious code
FDP_ACF_CIMC.3 User secret key confidentiality protection.	O.Certificates, O.Procedures for preventing malicious code.
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_ETC_CIMC.5 Extended user private and secret key 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

Functional Requirement	Objective
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 integrity monitoring 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 actions before authentication
FIA_UID.1 Timing of identification	O.Individual accountability and audit records, O.Limitation of administrative access
FIA_USB.1 User-subject binding	O.Maintain user attributes
FMT_MOF.1 Management of security functions behavior	O.Configuration management, O.Manage behavior of security functions, O.Security-relevant configuration management
FMT_MOF_CIMC.3 Extended certificate profile management	O.Configuration management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	O.Configuration management
FMT_MTD_CIMC.4 TSF private key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.7 Extended TSF private and secret key export	O.Data import/export
FPT_CIMC_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_ITC.1 Inter-TSF confidentiality during transmission	O.Data import/export
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 1and 2)	O.Protect user and TSF data during internal transfer
FPT_STM.1 Reliable time stamps	O.Time stamps

Table 6-7 Security 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, Officers and Auditors guidance documentation, O.Auditors Review Audit Logs, O.Competent Administrators, Officers and Auditors, O.Configuration Management, O.Installation, O.Malicious Code Not Signed, O.Procedures for preventing malicious code,

Assurance Requirement	Objective
	O.Require inspection for downloads, O.Security-relevant configuration management, O.User authorization management,
AGD_PRE.1 Preparative procedures	Selection of EAL 4, O.Installation
ALC_CMC.4 Production support, acceptance procedures 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 tools	Selection of EAL 4
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 Dependencies

There are some dependencies specified in section 6.1 of this ST that are not met directly by this ST.

The following SFRs have dependencies on FMT_SMR.1:

FMT_MOF.1
FMT_MOF_CIMC.3
FMT_MOF_CIMC.5

The following SFR has a dependency on FIA_ATD.1:

FIA_USB.1

In compliance with the PP, FMT_SMR.1 and FIA_ATD.1 are functional requirements associated with the environment, not with the TOE. Therefore these dependencies are met by the environment, in compliance with the PP.

6.3.3 Security Requirements Sufficiency

6.3.3.1 Security Objectives for the TOE

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),** and **FDP_CIMC_CSE.1 (Certificate status export)** ensure that certificate revocation lists and certificate status information are valid.
>
> **FDP_ACF_CIMC.2 (User private key confidentiality protection)** ensures that the certificate is not invalidated by the disclosure of the private key by the TOE.

FDP_ACF_CIMC.3 (User secret key confidentiality protection) ensures that an attacker cannot obtain a bad certificate by obtaining a user's authenticator from the TOE and then using that authenticator to obtain a bad certificate.

System

O.Preservation/trusted recovery of secure state, in compliance with the PP, there are no security requirements mapped to this objective.

Cryptography

O.Cryptographic functions is provided by

FCS_CKM.1 (Cryptographic key generation), **FCS_COP.1 (Cryptographic operations)** and cover the requirement that approved algorithms be used for encryption/decryption, authentication, and signature generation/verification and that approved key generation techniques be used.

FCS_SOF_CIMC.1 (Strength of functions) covers the requirement that FIPS 140-2 validated cryptographic modules perform all cryptographic functions, generate cryptographic keys and store plaintext private and secret keys. Specifically, this functional requirement ensures that:

- For encryption and FIPS 140-2 validated modules:
  The encryption specified for:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification of origin
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

  Is performed using a FIPS-approved or recommended algorithm

  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

  Are validated against FIPS 140-2

  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

  are implemented and validated as specified in FIPS 140-2

  The authentication codes specified in:

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

are FIPS-approved or recommended authentication codes

- For cryptographic functions that involve private or secret keys
  All cryptographic operations performed (including key generation) at the request of the TOE are performed in a FIPS 140-2 validated cryptographic module operating in a FIPS-approved or recommended mode of operation.

  Table 6-8 specifies for each category of use for a private or secret key, the overall FIPS 140-2 level for the validated cryptographic module. For CIMCs that generate certificate subject private keys, the required overall FIPS 140-2 level for *Long Term Private Key Protection* keys applies.

Table 6-8 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

- For cryptographic functions that do not involve private or secret keys (i.e. cryptographic modules that only perform signature verification and/or keyless hash generation), the overall required FIPS 140-2 level is 1.

O.Non-repudiation is provided by

FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin) covers the requirement that messages containing security-relevant data are not accepted by the TOE unless they contain evidence of origin and

FCO_NRO_CIMC.4 (Advanced verification of origin) covers the requirement that digital signatures be used so that the evidence of origin for a message may be verified by a third-party.

External Attacks

O.Control unknown source communication traffic is provided by

FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin) which covers the requirement that the TOE discard messages from an unknown source that contain security-relevant information.

6.3.3.2 Security Objectives for the TOE and Environment

O.Configuration Management is provided by

FMT_MOF.1 (Management of security functions behavior) 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 able to control the types of information that are included in generated certificates.

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

A.Competent Administrators, Officers and Auditors and **A.CPS** ensure that Administrators are competent and are familiar with the CPS under which the TOE is to be operated.

ALC_CMC.4 (Production support, acceptance procedures and automation) and ALC CMS.4 (Problem tracking CM coverage) ensure that a configuration management system is implemented and used.

This objective is also supported by the assumption **AGD_OPE.1 (Operational user guidance)** that covers the requirement that Administrators be provided with documentation describing the configuration management features of the TOE.

O.Data import/export is provided by

FDP_UCT.1 (Basic data exchange confidentiality) and **FPT_ITC.1 (Inter-TSF confidentiality during transmission)** cover the requirement that data other than private and secret keys be protected when they are transmitted

FDP_ETC_CIMC.5 (Extended user private and secret key export), and **FMT_MTD_CIMC.7 (Extended TSF private and secret key export)** cover the requirement that private and secret keys be protected when they are transmitted to and from the TOE.

O.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

FIA_UID.1 (Timing of identification) covers the requirement that users be identified before performing any security-relevant operations.

FAU_GEN.1 (Audit data generation) and **FAU_SEL.1 (Selective audit)** cover the requirement that security-relevant events be audited

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 records along with the identities of the entities responsible for the actions.

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)** cover the requirement that user data be protected

FMT_MTD_CIMC.4 (TSF private key confidentiality protection) and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are required to protect the confidentiality of the private and secret keys used to protect the data and software since data and software are protected using cryptography.

O.Limitation of administrative access is provided by

FIA_SOS.1 (Verification of secrets), FIA_UAU.1 (Timing of authentication) and FIA_UID.1 (Timing of identification) ensure that Administrators, Officers, and Auditors cannot perform any security-relevant operations until they have been identified and authenticated

FDP_ACC.1 (Subset access control) and **FDP_ACF.1 (Security attribute based access control)** ensure that Administrators, Officers, and Auditors can only perform those operations necessary to perform their jobs.

O.Maintain user attributes 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 functions behavior) covers the requirement that authorized users be able to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code, in compliance with the PP, there are no security requirements mapped to this objective.

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)**, **FCS_CKM.4 (Cryptographic key destruction)** 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) covers the requirement that audit records be protected against modification or unauthorized deletion.

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 1and 2) covers the requirement that user data be protected during internal transfer

FPT_ITT.1 (Basic internal TSF data transfer protection) (iterations 1 and 2) covers the requirement that TSF data be protected during internal transfer.

O.React to detected attacks is provided by

> **FCS_CKM.4 (Cryptographic key destruction)** and **FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** 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)** covers the requirement that no auditable events, except those taken by the Auditor, can be performed when audit trail storage is full.

O.Restrict actions before authentication is provided by

> **FIA_UAU.1 (Timing of authentication)** covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.

O.Security-relevant configuration management is provided and supported by

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

6.3.4 Security Assurance Requirements Rationale

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

The assurance that satisfies these requirements is EAL 3/EAL 4 augmented.

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

7 TOE Summary Specification

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

7.1 Security Audit.

7.1.1 Specification of auditable events and recorded information

Entrust Authority does not provide the capability to start and stop the audit functions independently of the authority service, but the audit function starts-up and shuts down whenever the authority service starts-up and shuts down, and these are auditable events. Entrust Authority also audits all of the events specified in Section E of [EASM Operations Guide], including all applicable events specified in the CIMC PP, as listed below in Table 7-1.

Table 7-1 Audited events as specified by CIMC PP

Event	TOE Functional Specification
Any changes to the audit parameters, e.g., audit frequency, type of event audited.	Not applicable. Entrust Authority does not provide the ability to modify audit parameters; therefore changes to audit parameters cannot be auditable events.
Any attempt to delete the audit log.	Each audit file consists of an audit header which contains information about the audits in the file and a list of audit events. A MAC is created for each of the audit event and the audit header. All audit events have a unique audit number. Audit numbers for a new installation will start from one (1) and increment sequentially throughout the lifetime of the system. The last used audit number and the file name of the current audit trail is recorded. The sequence number and MAC prevent any earlier records from being deleted, modified or added without the auditor to detect that fact. Also, audit files can be archived on a non-modifiable media.
Audit log signing event	A MAC is created for each of the audit event and the audit header of the file that contain the audit events.
All security-relevant data that is entered in the system	Entrust Authority generates an audit event for each entry of security-relevant data. The subject identity is included in each entry.
All security-relevant messages that are received by the system	Entrust Authority 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.)	Entrust Authority generates an audit event whenever cryptographic key generation is requested, except for session and one-time use symmetric keys. The serial number of the certificate that holds a public key is included in the audit event.
The loading of Component private keys	Not applicable. Private keys cannot be loaded in Entrust Authority.
All access to certificate subject private keys retained within the TOE for key recovery purposes	Entrust Authority generates an audit event for any key recovery.
All changes to the trusted public keys,	Entrust Authority generates an audit event whenever public

Event	TOE Functional Specification
including additions and deletions	keys are generated, updated or deleted. The serial number of the certificate that holds a public key is included in the audit event.
The manual entry of secret keys used for authentication (Security Levels 3 and 4)	Not applicable. Entrust Authority does not support manual entry of secret keys for authentication.
The export of private and secret keys (keys used for a single session or message are excluded)	Entrust Authority exports private keys during user recovery which is audited.
All certificate requests	Entrust Authority generates an audit event for all certificate requests. If accepted, serial number of the certificate is included in the audit event; if rejected, the reason for rejection is included.
All requests to change the status of a certificate.	Entrust Authority generates an audit event for all requests to revoke certificates.
Any security-relevant changes to the configuration of the TSF	Entrust Authority generates an audit event for any security-relevant changes to the configuration of the TSF
All changes to the certificate profile	Entrust Authority generates an audit event for any changes to the certificate profile. The certificate specification is maintained separately in protected storage.
All changes to the revocation profile	Not applicable Revocation profile is hard coded in Entrust Authority and cannot be modified. Changes in CRL setting configuration that affect CRL extension value are audited (e.g. nextUpdate).
All changes to the certificate revocation list profile	Not applicable Entrust Authority does not provide the capability to change the CRL profile.

Each audit event includes the following information: data and time of event, type of event, subject identity, outcome, log number, event description, severity level, user type, state, extra text, and MAC.

This security function addresses the following SFR: FAU_GEN.1

7.1.2 Accountability of users

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

This security function addresses the following SFR: FAU_GEN.2

7.1.3 Audit data selection

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

This security function addresses the following SFR: FAU_SEL.1

7.1.4 Audit Data Protection

Entrust Authority stores all audit entries in audit files. Each audit file consists of an audit header which contains information about the audits in the file and a list of audits. A MAC is created for each of the audit

events and the audit header. The audit file MAC (in the audit header) is updated each time a new audit event is logged.

All audit events have a unique audit number. Audit numbers for a new installation will start from one (1) and increment sequentially throughout the lifetime of the system. The last used audit number and the file name of the current audit trail is recorded. Also, audit files can be archived on a nonmodifiable media.

The sequence number and MAC prevent any earlier records from being deleted, modified or added without the Auditor (or Administrator) to detect that fact.

This security function addresses the following SFRs: FAU_STG.1, FPT_CIMC_TSP.1

7.1.5 Prevention of Audit Data Loss

The audit trail never gets full since a new audit log file is created when the current audit log reaches a specific size. Old audit trails can be automatically archived to prevent the local hard disk from getting full. In any case, should an error be generated while writing an audit entry to the file, the service that provides the auditable event will shut down which prevents any auditable events from occurring.

This security function addresses the following SFR: FAU_STG.4

7.1.6 Reliable Time Source

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

This security function addresses the following SFR: FPT_STM.1

7.2 Roles

7.2.1 Role Definition

Entrust Authority maintains the roles Master User, Security Officer, Administrator, Directory Administrator, Auditor, Self-Administration Server Administrator, and End User. Entrust Authority also allows for authorized operators to define new roles. These roles are described below:

- **Master User** As the only Entrust operators who can access the SMC interface, Master Users are responsible for the initial configuration of Entrust Authority, for its ongoing maintenance and database integrity. Other functions include changing performing database backups and starting and stopping services as needed.

- **Security Officer** The main role of the Security Officer is to set and administer an organization's security policy as it applies to all Entrust users in the organization. Security Officers may also add, delete, and configure other administrative users, including defining and configuring new roles. Security Officers also have end-entity management privileges, and are Entrust end users (end-entities) themselves.

- **Administrator** The main role of the Administrator is to add, enable, disable, change end user DNs, recover Entrust users, and to revoke X.509 certificates. Administrators may also view and modify Directory content and review audit logs. Administrators are also end-users.

- **EAC Administrator** The main role of the EAC Administrator is to manage EAC entities and certificates. For an EAC administrator in a CVCA deployment this includes managing local and foreign DVs. It also includes countersigning initial certificate requests that local DVs will send to foreign CVCAs. For an EAC administrator in a DV environment this includes managing local ISs and managing relationships with local and foreign CVCAs. EAC Administrators may also review audit logs. EAC Administrators are also end-users.

- **Directory Administrator** Directory Administrators are responsible for maintaining the Directory used as a repository for certificates, CRLs and ARLs. As such, their main role is to add and delete Entrust users entries to and from the Directory, either in bulk or one at a time. Directory Administrators are also end users.

- **Auditor** The main role of the Auditor is to review audit logs and create reports.

- **Self-Administration Server Administrator** The Self-Administration Server Administrator role is intended to restrict the administrative functions that Self-Administration Server, an optional Entrust product, can perform. The Self-Administration Server automates the process of adding users to the Entrust Authority PKI. This role, which can only administer End-Users, has a similar, yet reduced set of permissions from that of the Administrator role.

- **Custom-defined (flexible) Roles** The configuration of roles provides the ability to grant or deny administrative access to various operations including: user administration operations (e.g., enable user, recover user, revoke certificate), types of certificates, security policy operations, audit log access, directory operations, and database operations.

- **End User** End Users are the ultimate recipients of Entrust Authority services. An end user is a recipient of credentials, a creator of signed and/or encrypted information, or, in other terms, the ultimate consumer of the PKI services provided by Entrust Authority. End user privileges are enforced by Entrust Authority, directly in the case of initialization and key recovery, and indirectly via certificates and revocation lists issued by Entrust Authority.

When a new user is created (with the exception of Master Users), an operator with sufficient privileges has the option of associating the new user with the roles of Security Officer, Administrator, Directory Administrator, EAC Administrator, Auditor, End User, or any custom roles that may exist. The End User role actually has no privileges to access Entrust Authority via the EASMA or SMC (i.e., an End User cannot log in to the EASMA or SMC except for key management operations which are transparent to the End User).

Some conditions must hold in order for the role to be assigned to the user. A user can be associated with the Security Officer, Administrator, EAC Administrator, Directory Administrator, Auditor, or other custom-defined role only as explicitly assigned by a Security Officer or operator with sufficient privileges. The Security Officer and End User roles are assigned a fixed set of privileges that can be assigned or revoked. Master User (CIMC Administrator role) can never be deleted. No Master Users past the original three may be added. A user cannot be disassociated from the Master User role.

A mapping of the Entrust roles to the roles specified by the CIMC PP and used in this ST is provided in Table 1-1-1.

This security function, in conjunction with the security function Management of security functions behavior described below in Section 7.2.2, addresses the following SFR: FMT_MOF.1

7.2.2 Management of security functions behavior

Each Entrust role provides access to a specific set of operations, including the ability to modify the behavior of the Entrust system. Certain operations are only available to certain operators. Some role restrictions are described in Table 7-2 below:

Table 7-2 Role Restrictions

Section/Function	Function/Authorized Role
Security Audit	Except for controlling which audit logs are published externally which can be

Section/Function	Function/Authorized Role
	configured by Administrators, the audit parameters, including the MAC generation behavior, are hard coded and cannot be modified by any of the roles.
Backup and Recovery .	The capability to configure the backup parameters is restricted to Administrators. The capability to initiate the backup or recovery function is also restricted to Administrator.
Certificate Registration	The capability to approve fields or extensions to be included in a certificate is restricted to Officers. The capability to configure that process is also restricted to Officers.
Data Export and Output	The export of CIMC private keys requires the authorization of at least two Administrators.
Certificate Status Change Approval	Only Officers are allowed to configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate.
CIMC Configuration	The capability to configure any TSF functionality is restricted to Administrators, except as stated elsewhere in this document.
Certificate Profile Management	The capability to modify the X.509 certificate profiles shall be restricted to Administrators.
Revocation Profile Management	Entrust Authority does not provide the capability to modify the revocation profile.
Certificate Revocation List Profile Management	Entrust Authority does not provide the capability to modify the certificate revocation list profile.

This security function, in conjunction with the security function Role Definition described above in Section 7.2.1, addresses the following SFR: FMT_MOF.1

7.3 Access Control

The TOE controls access to all Entrust system data associated with operations initiated by any Entrust operator: Master User, Security Officer, Administrator, EAC Administrator, Auditor, Directory Administrator, or any custom-defined role.

The TOE controls access to all Entrust system data on the basis of the following security attributes: Identity; Role; Privileges (i.e., permissions); and State (Entrust state: e.g., enabled, disabled, set for key recovery, etc.).

Entrust Authority enforces the rules specified below in Table 7-3 to determine if an operation among controlled subjects and controlled objects is allowed.

Table 7-3 Explicit Access Control Rules

Section/Function	Event
Certificate Request Remote and Local Data Entry	The entry of certificate request data is restricted to Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry	The entry of certificate revocation request data is restricted to Officers and the subject of the certificate to be revoked.
Data Export and Output	The export or output of confidential and security-relevant data is only at the request of authorized users, i.e. Administrators, Officers or End-users for recovery purposes.
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 Administrators.
Private Key Load	The capability to request the loading of Component private keys into cryptographic modules is not provided.
Private Key Storage	The capability to request the decryption of certificate subject private

Section/Function	Event
	keys is restricted to Officers. The TSF does not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. The end users decryption private keys are stored in the database in an encrypted form and are not accessible to any administrators. These keys can only be requested during a user recovery process initiated by the owner of the keys. No capability is provided to decrypt private keys.
Trusted Public Key Entry, Deletion, and Storage	The capability to change (add, revise, delete) the trusted public keys is restricted to Administrators. Any key management function can only by initiated by Administrators.
Secret Key Storage	The capability to request the loading of CIMC secret keys into cryptographic modules is not provided.
Private and Secret Key Destruction	Plain text private and secret keys never leave the cryptographic module and no user interface is provided to zeroize them.
Private and Secret Key Export	The capability to export a component private key is not provided. The capability to allow export of certificate subject private keys is restricted to Officers. The setting of user for key recovery, which involves the export of subject private key, can be configured to require the authorization of more than one Officer.
Certificate Status Change Approval	Only Officers have the capability of putting certificates on hold and taking certificates off hold. As well, only Officers and the subject of a certificate are capable of requesting the revocation of a certificate, and only Officers are allowed to approve 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

7.4 Identification and Authentication

7.4.1 Authentication of users

Entrust Authority does not allow the selection of any Entrust Authority-mediated function before the operator is successfully authenticated with a password. All functions require the operator to be authenticated before allowing any Entrust Authority-mediated action.

This security function addresses the following SFR: FIA_UAU.1

7.4.2 Identification of users

Entrust Authority does not allow selection of any Entrust Authority-mediated function before the operator is successfully identified. All functions require the operator to be identified before allowing any Entrust Authority-mediated action.

This security function addresses the following SFR: FIA_UID.1

7.4.3 User-Subject Binding

Entrust Authority 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

7.5 Remote Data Entry and Export

7.5.1 Enforced Proof of Origin and Verification of Origin

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

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

All communications between EASM and EASMA are conducted through secure protocols which extend the enforcement of the access control policy to the physically separated components while providing confidentiality and integrity of transmitted data.

This security function addresses the following SFR: FCO_NRO_CIMC.3

7.5.2 Protection of data communications between Security Manager and EASMA

Entrust Authority internal communications between EASM and EASMA are protected from disclosure and modification as all data is always encrypted and integrity-protected using digital signatures or MACs. Any services available to EASMA operators including administrative functions, user initialization, automatic key updates, key recovery services, and cross-certification establishment services require use of protected communications.

This security function addresses the following SFRs: FDP_ITT.1 and FPT_ITT.1

7.5.3 Trusted channel

EASM provides a trusted channel between itself and remote Entrust entities via CMP. A trusted channel is required for any key management and certificate management transactions (including certificate requests, key recovery and automatic key update of end user encryption key and signing key pairs) between Entrust entities and EASM. These transactions are initiated by the remote Entrust entities. Entrust Authority requires a valid authentication code to initiate any certificate request transaction from end users. Any sensitive data transmitted through this trusted channel is always protected against unauthorized disclosure and modification using encryption and digital signatures.

This security function addresses the following SFRs: FDP_UCT.1, FPT_ITC.1 and FCO_NRO_CIMC.4

7.6 Certificate Management

7.6.1 Certificate Generation

EASM generates certificates whose format complies with X.509 version 3 certificates. In EAC environments, EASM also issues certificates whose format complies with ISO 7816. All generated certificates must be consistent with the defined certificate specification. For X.509 certificates, EASM ensures that:

- *SerialNumber* is unique;
- *notBefore* is set to current date and the *notAfter* value is set current date + cross-certificate lifetime;
- *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 for FIPS-approved algorithms .

Proof of possession is always established before a certificate can be made available to an end-user. Proof of possession is established either when the end-user includes the private key in the certificate request or when Entrust Authority encrypts the certificate using the public key that was included in the certificate request.

This security function addresses the following SFR: FDP_CIMC_CER.1

7.6.2 Certificate Status Export

EASM issues Certificate Revocation Lists (CRLs) in a format that complies with X.509 version 2 CRLs.

This security function addresses the following SFR: FDP_CIMC_CSE.1

7.6.3 Certificate Profile Management

EASM implements flexible certificate definitions for X.509 certificates and ensures that issued certificates are consistent with that specification. It requires an Administrator to specify the set of acceptable values for:

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

This security function addresses the following SFR: FMT_MOF_CIMC.3

7.7 Certificate Revocation

7.7.1 CRL Profile Management

EASM generates CRLs according to an X.509 compliant CRL specification, implemented directly in code, and ensure CRLs are always consistent with that profile. Authority specifies its own DN for issuer and does not use issuerAltName. Some values, such as nextUpdate, can be modified by Administrators only.

This security function addresses the following SFR: FMT_MOF_CIMC.5

7.7.2 CRL Validation

EASM only generates CRLs whose format complies with X.509 version 2 CRLs. It ensures that the *Issuer* attribute is set to the CA's DN and never contains a null name. The *Signature* and *signatureAlgorithm* attributes can be set to contain the OID for FIPS-approved algorithms. Also, *thisUpdate* is set to the CRL issue time (UCT time),
nextUpdate is set to next CRL issue time (UCT time) and never precede the time specified for the *thisUpdate* atribute.

This security function addresses the following SFR: FDP_CIMC_CRL.1

7.8 Key Management

7.8.1 Key Generation

All key material used within Entrust Authority is generated and used within the FIPS 140-2 validated software-based cryptographic modules specified listed in Section 1.4.4.5. These CMs generate keys in

accordance with *[RSA,RSA-PSS, DSA, ECDSA, CAST5, 3DES and AES]* and specified cryptographic key sizes

- *[1024, 1280, 1536, 2048, 3072, 4096 and 6144 (RSA and RSA-PSS),*
- *512 and 1024 (DSA),*
- *160, 163, 191, 192, 193, 224, 233, 239, 256, 283, 320, 359, 384, 409, 431, 512, 521 and 571 (ECDSA), 80 to 128 bit (CAST5),*
- *192 bit (3DES), and*
- *256 bit (AES)]*

that meet the following: *[FIPS PUB 186-2 (RSA and DSA),Draft FIPS PUB 186-3 (RSA-PSS), ANSI X9.62-2005 Annexes E.7, B, L.3, L.4, L.5, L.6, FIPS PUB 186-2 Appendix 6 (ECDSA), FIPS 186-2 APPENDIX 3 (CAST5, 3DES and AES) and PUB 197 (AES)]*.

The keys used by the IT environment for user certificate signing and database protection are generated by a FIPS 140-2 level 3 validated hardware cryptographic device.

This security function addresses the following SFR: FCS_CKM.1

7.8.2 Private Key Protection

All key material used within Entrust Authority is generated and used within the FIPS 140-2 validated Entrust software. Keys are exported only when suitably protected, such as when encrypted under a public key, using FIPS 140-2 approved techniques.

User private or secret keys are stored in the database in a FIPS-approved encrypted form and only exported to end-users over PKIX-CMP in encrypted form. For enhanced protection, EASM can store the key used to encrypt the database on a FIPS 140-2 level 3 validated hardware cryptographic device.

Subject private keys that are used to generate digital signatures are not generated by EASM but by the subjects themselves.

This security function addresses the following SFRs: FDP_ACF_CIMC.2, FDP_ACF_CIMC.3, FMT_MTD_CIMC.4, FMT_MTD_CIMC.5, FMT_MTD_CIMC.7 and FDP_ETC_CIMC.5

7.8.3 Public Key Protection

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

EASM exports End-user public keys embedded in X.500 certificates. All certificates are digitally signed, which protects the exported public keys against unauthorized modifications.

This security function addresses the following SFR: FDP_SDI_CIMC.3

7.8.4 Key Zeroization

The FIPS 140-2 validated Entrust Cryptographic modules which are implemented as part of Entrust Authority provides the capability to zeroize plaintext secret and private keys. The hardware cryptographic module supported by EASM also provides capability to zeroize plaintext secret and private keys.

This security function addresses the following SFRs: FCS_CKM.4 and FCS_CKM_CIMC.5

7.8.5 Strength of Functions and Cryptographic Operations

All cryptographic operations are performed within the FIPS 140-2 validated software-based CMs identified in Section 1.4.4.5. The supported cryptographic operations include encryption and decryption, digital signature generation and verification, hashing, and Message Authentication Code (MAC) generation and verification. These operations are performed in accordance with the following standards:

- Encryption/decryption: RFC 2144 (CAST5), FIPS PUB 46-3 (3DES) and FIPS PUB 197 (AES);
- Signature generation/verification: FIPS PUB 186-2 (DSA, 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

As mentioned above, Entrust Authority also supports the use of hardware cryptographic devices for CA signing key storage and signing of user certificates and CRLs. For the purpose of this evaluation, the 3rd party FIPS 140-2 level 3 hardware device is part of the IT environment.

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

8 TOE Access Control Policy

As per the [CIMC PP], this TOE Access Control Policy is referenced from a number of SFRs including FDP_ACF.1.1, FDP_ITT.1.1 and FDP_UCT.1.1 and is required to complete the specification of those SFRs..

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:

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

Subject identification includes:

- 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.

9 Glossary

ADM-API	Administration API
AES	Advanced Encryption Standard
API	Application Programming Interface
ARL	Authority Revocation List
BAC	Basic Access Control
CA	Certification Authority
CAST	Carlisle Adams, Stafford Tavares [Entrust symmetric key algorithm]
CC	Common Criteria
CIMC	Certificate Issuing and Management Component
CM	Cryptographic Module
CMP	IETF PKIX Certificate Management Protocol
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certification Authority
DES	Data Encryption Standard
DN	Distinguished Name
DS	Document Signer
DSA	Digital Signature Algorithm
DV	Document Verifier
EA	Entrust Authority
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EASM	Entrust Authority Security Manager
EASMA	Entrust Authority Security Manager Administration
FIPS PUB	Federal Information Processing Standard Publication
GUI	Graphical User Interface
HSM	Hardware Security Module
I&A	Identification and Authentication
ICAO	International Civil Aviation Authority
IP	Internet Protocol
IS	Inspection System
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
ODBC	Open Database Connectivity

PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman [public key algorithm]
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm 1
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

10 References

[BIG CP] Common Certificate Policy for the Extended Access Control Infrastructure for passports and travel documents issued by EU Member States, Version 1.0, April 2008

[CC] Common Criteria for Information Security Evaluation. Version 3.1 Revision 3, July, 2009

[CIMC PP] Certificate Issuing and Management Components Protection Profile, Version 1.5, August 11, 2011

[CMP] RFC 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocol, September 2005

[Draft FIPS 186-3] U.S. National Institute of Standards and Technology – Digital Signature Standard, November 2008

[EASM Operations Guide] Entrust Authority Security Manager 8.1 SP1 Operations Guide for Windows, Entrust Inc., version 1.0, January 2012

[FIPS 113] U.S. National Institute of Standards and Technology – Computer Data Authentication Standard, May 1985

[FIPS 180-1] U.S. National Institute of Standards and Technology - Secure Hash Standard, April 1995

[FIPS 180-2] U.S. National Institute of Standards and Technology - Secure Hash Standard, August 2002

FIPS 186-2] U.S. National Institute of Standards and Technology – Digital Signature Standard, January 2000

[FIPS 197] U.S. National Institute of Standards and Technology – Advanced Encryption Standard, November 2001

[ISO 7816] ISO/IEC 7816: Identification Cards – Integrated Circuit Cards (Parts 10, 11 & 12)

[RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

[TR-03110] European Union – Article 6 Committee - Brussels Interoperability Group – Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control, Version 1.11 RC 2, 2007

[X.509] ITU-T Recommendation X.509 (2005 | ISO/IEC 9594-8: 2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks