Security Target

Entrust Authority Security Manager 7.0

Version 1.7

August 6, 2004

Prepared By:

SMI Consulting
www.smiconsulting.ca

Document version control log

Version	Date	Author(s)	Description
1.0 (Draft)	October 2003	Marc Laroche	Initial copy of Entrust Authority 7.0 Security Target.
1.1	November 16 2003	Marc Laroche	Updates made to address OR1, OR2, OR3 and OR4.
1.2	November 17 2003	Marc Laroche	Minor updates. New ST version and changed FIPS 140-2 to 140-1.
1.3	December 9 2003	Marc Laroche	Updates in response to OR5.
1.4	February 21, 2004	Marc Laroche	Updates in response to OR 6, OR7 (addition of FIA_SOS.1) and OR8.
1.5	April 26, 2004	Marc Laroche	Updates to Table 8-11 in response to OR 8, OR 10 and OR 11. Minor updates in response to OR 16.
1.6	May 19, 2004	Marc Laroche	Updates to Table 8-11.
1.7	August 6, 2004	Marc Laroche	Updates to Table 8-11 in response to OR 21 and 24.

Table of contents

List of figures

List of tables

1 Introduction

1.1 ST and TOE Identification

ST Title: Security Target for Entrust Authority Security Manager 7.0, v1.7, August 6, 2004.

TOE Identification: Entrust Authority Security Manager 7.0

CC Conformance:

- Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 2, August 1999 (ISO 15408-2)
- CC Version 2.1 Part 2 extended
- Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 3 August 1999 (ISO 15408-3
- CC Version 2.1 Part 3 augmented

Protection Profile (PP) Conformance: Certificate Issuing and Management Component (CIMC) Security Level 3 PP, Version 1.0, October 31 2001.

Assurance level: EAL4 augmented with ALC_FLR.2

Keywords: Commercial-off-the-shelf (COTS), certification authority, key management, cryptographic services, digital certificate management, public-key infrastructure, digital signature, encryption, confidentiality, integrity, networked information systems, baseline information protection.

1.2 ST Overview

This Security Target (ST) couples certificate issuing 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 Manager, in conjunction with its environment, provides:

- 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.

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

1.3 Entrust Authority System Overview

A CIMC is a cryptographic key and certificate delivery and management system that makes possible secure financial electronic transactions and exchanges of sensitive information between relative strangers. The Entrust Authority Security Manager system (referred later in this document as **Entrust Authority**) enables the use of digital signature, digital receipt, encryption and permissions management services across a wide variety of applications. This enables organizations to establish and maintain enhanced secure networking environments for internal and external relationships. By adding this level of security, organizations are poised to:

- Ensure confidential communication with employees, customers, partners, etc.
- Enhance revenue growth
- Expand customer and business opportunities
- Offer trust-based services (i.e. automated purchase orders using digital signatures to track accountability)
- Work across multiple operating systems
- Scale to size as the organization grows

There are five main components in an Entrust Authority system, namely:

- Security Manager
- Database
- Security Manager Administration
- Directory
- Cryptographic Module

2 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.

2.1 Product Type

Entrust Authority Security Manager (Entrust Authority) is a cryptographic key and certificate delivery and management system which makes possible secure financial electronic transactions and exchanges of sensitive information between relative strangers. 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; and
- Publishes the public keys with the user's identification as certificates in open bulletin boards (e.g., X.500 directory services).

2.1.1 Entrust Authority System Components

2.1.1.1 Security Manager

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

- Create encryption key pairs for users.
- Create certificates for all public keys.
- Manage a secure database of Entrust Authority information that allows the recovery of users' encryption key pairs.
- Enforce an organization's security policy.

Security Manager 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.509v3 standard or any properly formatted proprietary extension).
- Use of attribute certificates to support privilege management for end users.

- 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 either RSA 1024-bit, RSA 2048-bit, RSA 4096, DSA 1024-bit, or ECDSA (128 to 768)-bit as the CA signing algorithm and CA signing key size.
- Ability to renew the CA signing key pair before it expires and to recover from possible CA key compromise.

2.1.1.2 Security Manager Administration (SMA)

The SMA is the graphical administrative interface to the Entrust Authority system. It is used by Security Officers, Administrators, Directory Administrators, Auditors, and custom-defined roles[1] (with a customizable set of permissions) either remotely across a network or on the workstation that hosts Security Manager. Primary uses for the SMA include:

- Ability to renew the CA signing key pair before it expires and to recover from possible CA key compromise
- Adding and deleting users
- Revoking certificates
- Initiating key recovery operations
- Setting security policies
- Reviewing audit logs
- Security Officers, Administrators, and other administrative roles connecting to Security Manager authenticate themselves using digital signatures. Once complete, all messages between the SMA and Security Manager are then secured for confidentiality, integrity, and authentication.

2.1.1.3 Database

Security Manager stores information about Entrust users and the infrastructure itself in a database. This data is encrypted and protected by Security Manager.

The Security Manager Database stores:

- the CA signing key pair
- user status information, including the distinguished name (DN) of each user
- the encryption key pair history for all Entrust users, which includes all decryption private keys and encryption public key certificates for each user

[1] The roles supported by Entrust Authority and corresponding CIMC PP roles are defined in Section 2.2.2.

- the verification public key history for all Entrust users, which includes all verification public key certificates for each user
- the validity periods for user signing key pairs, user encryption key pairs, and system cross-certificates
- Security Officer and Administrator information

Security Manager enforces access control and maintains integrity of these resources.

For additional protection, a FIPS-140-1 level 3 hardware cryptographic device can be used to store the CA signing key and the database encryption key.

2.1.1.4 Directory

The Directory is a repository of public information. It contains the name of each end entity in the CA domain. Public certificates of each user, certificate revocation lists (lists of certificates that have been revoked for various reasons), and other information is written from Security Manager 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. Security Manager provides mechanisms to maintain the authenticity and integrity of resources stored in the Directory.

2.1.1.5 Cryptographic Module

All cryptographic operations for Entrust Authority are performed on a FIPS 140-1 level 2 validated Entrust Security Kernel cryptographic module (FIPS 140-1 certificate #308) or optional hardware cryptographic module. The Entrust Security Kernel 7.0 cryptographic module is embedded in the SMA and Security Manager and provides a PKCS#11 interface for using an optional hardware cryptographic module.

2.2 Entrust Authority Roles and Services

2.2.1 Delivered Services

The main role of an Entrust Authority PKI is to manage end-entity public-key certificates, including creating and issuing certificates, Certification Revocation Lists (CRLs), and Authorization Revocation Lists (ARLs) and publishing them in a X.500 public directory. In addition, Entrust Authority provides the infrastructure functions that are necessary for maintaining end-entity encryption key-pair history and end-entity verification certificate history, providing automatic public key and certificate updates, auditing security-related events, and maintaining CA data confidentiality and integrity.

The functionality provided by Entrust Authority can be categorized into the following set of services:

1) **Core Services:** The Core Services are the basis for all PKI management functionality.

2) **Support Services:** The Support Services comprise a set of services relating to management of Entrust Authority-related components. These services include CA Self-Management, Security Manager Database Management, Audit Trail Management, and Directory Management.

2.2.1.1 Core Services

Core Services are provided mainly by Security Manager. They are required to provide encryption and authentication services to end-entities. They consist of:

3) **CA Key Management Service:** This service is, among other things, responsible for managing the CA signing key pair, master keys, and enforcing infrastructure security policies.

4) **End-entity Management Service:** Similar to Operator Management, the End-entity Management Service allows authorized operators to manage End users associated with a CA domain or group. This service allows, for example, for creating, initializing, and deleting users, recovering, revoking, and updating keys, and other functions.

5) **Operator Management Service:** This service is responsible for providing the capability to authorized operators to manage other operators. Passwords, keys, roles and privileges, and other operator attributes are managed through this service.

6) **Cross-Certificate Management Service:** This service manages the generation and maintenance of cross-certificates.

2.2.1.2 Support Services

Support Services are also provided mainly by Security Manager. They provide support capabilities to the CA Core Services. The Support Services consist of:

7) **Self Management Service:** Service to initialize Security Manager, start and stop Entrust services, and validate operator passwords.

8) **Database Management Service:** Service to operate and maintain the repository that stores security critical data Entrust Authority needs for proper operation (e.g., security policy data, end user encryption key pairs).

9) **Audit Trail Management Service:** Service to maintain and analyze an audit record of critical and non-critical events that have occurred within the Entrust Authority infrastructure.

10) **Directory Management Service:** Service to operate and maintain the Directory and Directory entries (e.g., search the directory, create new entries, modify attributes).

2.2.2 Entrust Operator Roles

There are two human interfaces into Entrust Authority: Security Manager Control or SMC (which is part of the Security Manager) and the SMA.

The SMC is used to manage Entrust Authority itself. It is comprised of a GUI and a command line shell. The functions available through the SMC include, but are not limited to: perform initial configuration of Entrust Authority, enable/disable services, verification of the Security Manager database, schedule database backups, and performing exceptional management

events such as database re-encryption and Security Officer key recovery. The SMC can only be accessed by Master User.

The SMA is a remote administrative user interface for day-to-day management of Entrust end users and administrative users. The SMA can be accessed by the defined Entrust roles listed below:

- Security Officer
- Administrator
- Directory Administrator
- Auditor
- Self-Administration Server Administrator
- Custom-defined (flexible) roles

It should be noted that there is an additional role in Entrust, that of End User [2]. This type of user has no administrative access to Entrust Authority via the SMA or SMC.

2.2.2.1 TOE Roles

The CIMC PP defines four specific roles: Administrator, Operator, Officer and Auditor. This Security Target (in accordance with CIMP level 3) 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 and part of the Administrator role.

The CIMC PP defined roles can be mapped to Entrust Authority roles as indicated in Table 2-1 below.

Table 2-1 Roles Description

Entrust Authority Role	Description	Corresponding CIMC PP Role
Master User	Master Users, as the only Entrust operators who can access the SMC, 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.	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, 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 certificates. Administrators may also view and modify Directory content and review audit logs. Administrators are also end-users	Officer

[2] Also referred to as an Entrust user or end-entity.

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

2.2.2.2 Other supported roles

- **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.

- **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 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.

2.3 TOE High-Level Architecture

Entrust Authority is comprised of several related and inter-dependent software and hardware modules that cooperate to provide all Entrust Authority services. A high-level view of Entrust Authority is represented at Figure 1.

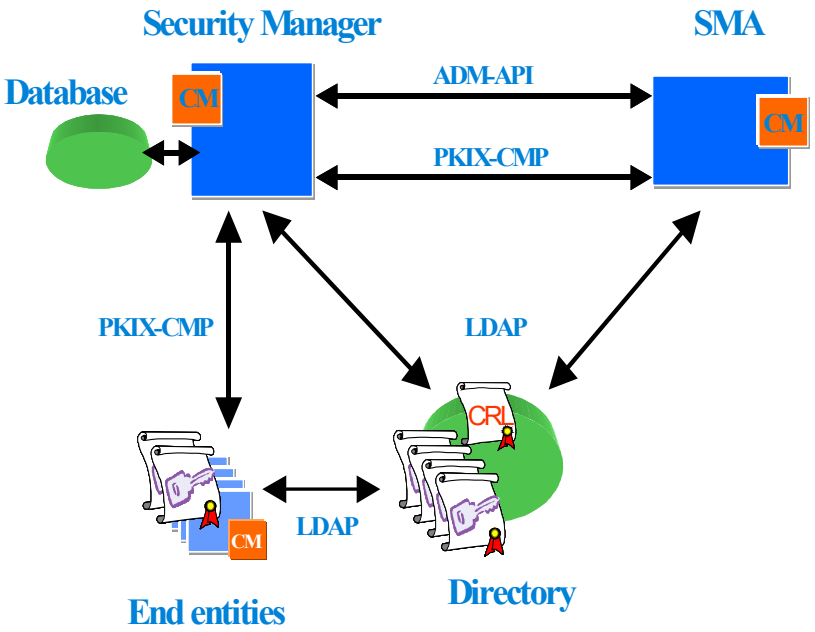


Figure 1: Entrust Authority

The Entrust Authority architecture is shown in Figure 2. As can be seen from this diagram, Entrust Authority is comprised of several related and inter-dependent modules that cooperate to provide all Entrust Authority services. These services and the components used to provide them are described below. Entrust Authority is installed as a single package normally on multiple nodes. Entrust Authority normally executes on multiple nodes.

2.3.1 Security Manager Control (SMC)

The SMC (comprised of a GUI and command line shell), is used to manage Entrust Authority itself. That is, to perform initial configuration of Entrust Authority based on data provided during software setup, to verify the integrity of the Security Manager database, to schedule backups of the database, and to perform exceptional PKI-management events such as PKI operator recovery. In other words, the SMC provides the interface into initialization and maintenance services, as well as certain support and operator management services.

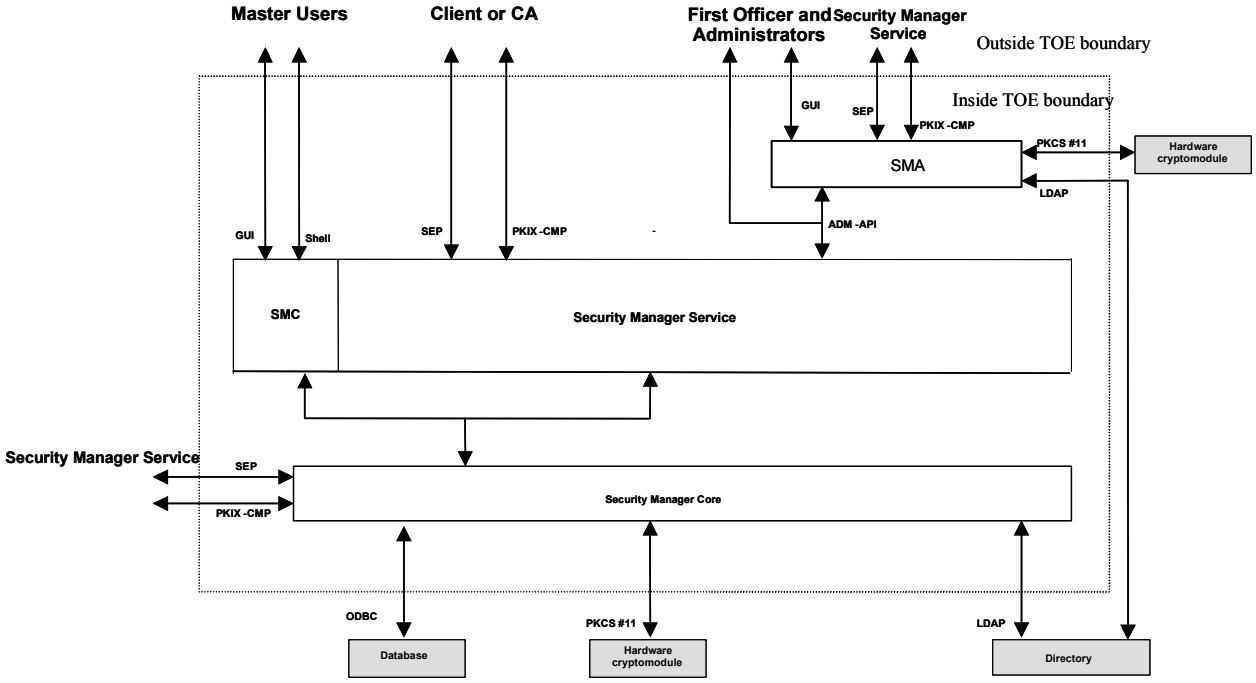


Figure 2: Security Manager Architecture

2.3.2 Monitor (Security Manager Service)

The Monitor (Security Manager Service) executable will be used to launch and monitor the following subsystem processes:

- PKIX-CMP (Certificate Management Protocol): CMP is a module that handles all PKIX-CMP requests for client initialization, key update, or key recovery from end users. For each CMP request that arrives, a new CMP process is spawned. CMP allows the older and new PKIX messages to co-exist and not break backwards compatibility and provide consistency for SEP and PKIX-CMP.

- Administration Service (AS): The Administration Service (AS) is a subsystem that listens for and processes requests from SMA or from other administrative applications via ADM-API. All connections between AS and SMA clients are secured for confidentiality and integrity.

- Database Backup: The database backup module is a process that performs all database backup activities. This subsystem runs transparently in the background

- Database Integrity: The database integrity module is a process that performs all database integrity validation activities. This subsystem runs transparently in the background

- CRL/ARL Writing: The CRL writing module is a process that performs all revocation list writing to the directory and CRL checking activities at Secure Manager. This process runs transparently in the background.

- Key generation (Keygen): The key generation module (Keygen) is a process that performs all pre-generation of public key pairs. This process runs transparently in the background.

Monitor performs the following activities:

- acts as the initial startup process
- starts all the other processes
- monitors the progress of each of the other subsystem modules and detects the death of any of its subsystem modules
- signals a subsystem module process to shutdown

2.3.3 Security Manager Core

The Security Manager Core performs all CA functions. It is the component that implements database access, and that makes use of the Entrust FIPS 140-1 validated cryptomodule to perform all cryptography-related CA functions, such as CA signing key pair generation, certificate signing[3], and end-entity encryption key pair generation.

Security Manager Core manages access to all data stored in the database. Access to protected data is a matter of retrieving and decrypting/verifying the data objects using the cryptomodule. All data to be protected in the database, is protected by the cryptomodule, and is exported from the cryptomodule only in protected form, then written to the database.

Security Manager Core validates the database every time a record in the database is used. That is, entries are checked for integrity when the entries are accessed. With this approach, Security Manager Core can detect unauthorized modification of any datum and report any errors to the audit trail.

2.3.4 Security Manager Administration (SMA)

The SMA is the primary operator interface for day-to-day management of Entrust users and other Entrust operators. Hence, management of the Entrust configuration and Entrust users via the SMA is assigned to the defined Entrust roles listed above.

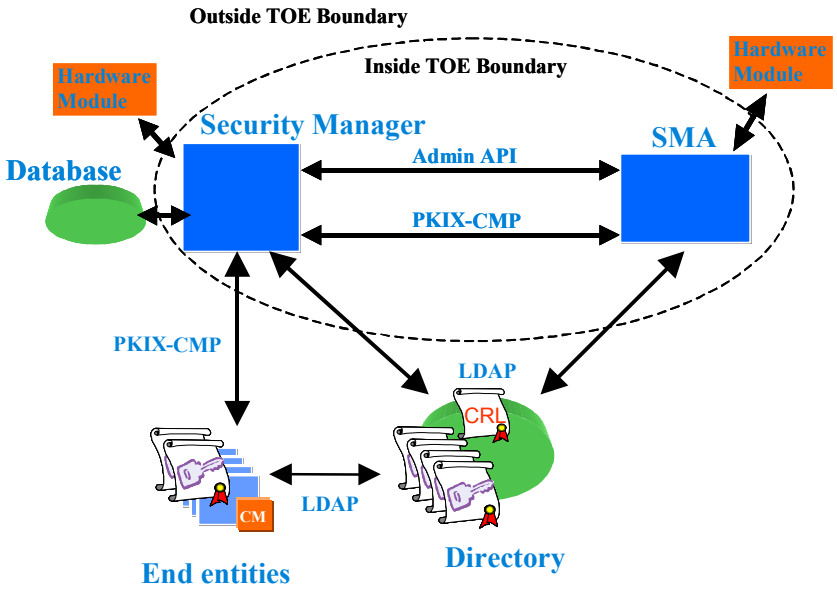
The GUI is the primary interface to the SMA services. For every service offered by the SMA, there is at least one corresponding GUI element that enables operators to invoke that service. The other interface to the SMA services are the bulk input files. These files are used for batch processing of the SMA services; they are used to perform either directory management services, such as adding new user entries, or end-entity or operator management services, such as enabling end-entities. Bulk-input file (BIF) processing is initiated via the GUI.

[3] An optional FIPS 140-1/140-2 level 3 validated cryptographic module can also be used for CA signing key pair generation and certificate signing.

2.4 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 3.

Figure 3: TOE Boundary



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

1) Security Manager including:

- SMC (GUI and Command Shell)
- Security Manager Service
- Security Manager Core

2) Security Manager Administration

2.4.1 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) [4]
- Hardware cryptographic device

2.4.1.1 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. That is, database access is only available through a well-defined interface (ODBC-API) **Reference 4**. 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.

2.4.1.2 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 **Reference 6** and **Reference 7**. 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.

2.4.1.3 Hardware and operating system platform (Abstract Machine)

The TOE abstract machine consists of the Windows 2000 operating system (evaluated against the US NCSC CAPP Protection Profile Reference 5) and any hardware for which the operating system and TOE configurations are valid.

[4] Not illustrated in Figure 3.

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. As well, Windows 2000 is certified to the Common Criteria EAL4 level (See **Reference 5)**.

- **Hardware independence:** The Entrust software is optimized to execute any x86 (i.e., Intel or equivalent processor)-based machines, regardless of the hardware vendor. That is, any hardware platform that meets the following minimum Entrust system requirements:

  1) Security Manager

  - Windows 2000 Server operating system and Service Pack 1 or 2
  - 256 Mbytes of RAM
  - Pentium 300 MHz or better
  - one 2X or faster CD-ROM drive
  - TCP/IP protocol stack installed
  - 2 Gbyte hard disk with a minimum of 1 Gbyte of free space (more if you're installing over a network)

  2) SMA

  - Windows 2000 Professional, Windows 2000 Server, or Windows 2000 Advanced Server
  - Pentium 300 MHz or better
  - an additional 32 Mbytes of RAM if the SMA runs on the server that will host Security Manager
  - 5 Mbytes of free disk space
  - one 2X or faster CD-ROM drive
  - TCP/IP protocol stack installed

2.4.1.4 Hardware Cryptographic Device

The justification for excluding the hardware cryptographic device from the TOE boundary is assumed to be validated to Level 3 under the FIPS 140-1/140-2 evaluation process, and thus trusted.

2.4.2 Cryptography-related IT Assets

The cryptographic aspect of the TOE requires that cryptography-related security critical items be protected. Entrust Authority's functions and services ensure that the following security critical assets are protected against unauthorized disclosure and modification:

- Cryptographic variables (including private keys, public keys, public parameters, initialization vectors, etc.)
- Input and output data from the cryptographic function (e.g., plaintext input and cipher text output)
- The implementation of the cryptographic services
- Other critical security parameters (e.g., authentication data)

3 TOE Security Environment

This section includes the following:

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

This information provides the basis for the Security Objectives specified in Section 4, the security functional requirements for the TOE and environment specified in Sections 5.1 and 5.2, and the TOE Security Assurance Requirements specified in Section 5.3.

3.1 Secure Usage 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.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.

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.

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 level 3 PPs, 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 to security

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.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.

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.

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.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.

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

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 Organization 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 four categories: authorized users, system, 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.

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

4.1.3 Cryptography

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.

4.2.1 Non-IT 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.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.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.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.Social Engineering Training
Provide training for general users, Administrators, Officers and Auditors in techniques to thwart social engineering attacks.

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.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.Repair identified security flaws
The vendor repairs security flaws that have been identified by a user.

4.2.2 IT security objectives for the environment

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.Security roles
Maintain security-relevant roles and the association of users with those roles.

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

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.

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.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.

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.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 140-1 validated.)

5 IT Security Requirements

5.1 Security Requirements for the IT Environment

This section specifies the security functional requirements that are applicable to the IT environment. Operations that are completed on the SFR components are indicated throughout this section through the use of Bold Italic text.

Table 5-1: IT Environment Functional Security Requirements

Security Requirement		Component
Security Audit (FAU)	Audit data generation (iteration 1)	FAU_GEN.1
	User identity association (iteration 1)	FAU_GEN.2
	Audit Review	FAU_SAR.1
	Selectable audit review	FAU_SAR.3
	Selective audit (iteration 1)	FAU_SEL.1
	Protected audit trail storage (iteration 1)	FAU_STG.1
	Prevention of audit data loss (iteration 1)	FAU_STG.4
Cryptographic Support (FCS)	Cryptographic key generation (iteration 1)	FCS_CKM.1
	Cryptographic key destruction (iteration 1)	FCS_CKM.4
	Cryptographic operation (iteration 1)	FCS_COP.1
User Data Protection (FDP)	Subset access control (iteration 1)	FDP_ACC.1
	Security attribute based access control (iteration 1)	FDP_ACF.1
	Basic internal transfer protection (iterations 1 and 2)	FDP_ITT.1
	Basic data exchange confidentiality (iteration 1)	FDP_UCT.1
Identification and Authentication (FIA)	Authentication failure handling	FIA_AFL.1
	User attribute definition	FIA_ATD.1
	Timing of authentication (iteration 1)	FIA_UAU.1
	Timing of identification (iteration 1)	FIA_UID.1
	User-subject binding (iteration 1)	FIA_USB.1
Security Management (FMT)	Management of security functions behavior (iteration 1)	FMT_MOF.1
	Management of security attributes	FMT_MSA.1
	Secure security attributes	FMT_MSA.2
	Static attribute initialization	FMT_MSA.3
	Management of TSF data	FMT_MTD.1
	Restrictions on security roles	FMT_SMR.2
Protection of the TSF (FPT)	Abstract machine testing	FPT_AMT.1
	Inter-TSF confidentiality during transmission (iteration 1)	FPT_ITC.1
	Basic internal TSF data transfer protection (iterations 1 and 2)	FPT_ITT.1
	Non-bypassability of the TSP (iteration 1)	FPT_RVM.1
	TSF domain separation	FPT_SEP.1
	Reliable time stamps (iteration 1)	FPT_STM.1
	Software/firmware integrity test	FPT_TST_CIMC.2
	Software/firmware load test	FPT_TST_CIMC.3
Trusted Path/Channel (FTP)	Trusted path	FTP_TRP.1

5.1.1 Security Audit

FAU_GEN.1 Audit data generation (iteration 1)
Hierarchical to: No other components.

FAU_GEN.1.1 The IT environment 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 5-2 below.

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, the information specified in the Additional Details column in Table 5-2 below.

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

Dependencies: FPT_STM.1 Reliable time stamps

Table 5-2 Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
Security Audit	FAU_GEN.1 Audit data generation (iteration 1)	Any changes to the audit parameters, e.g., audit frequency, type of event audited	
		Any attempt to delete the audit log	
Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a role	
	FIA_AFL.1 Authentication failure handling	The value of maximum authentication attempts is changed.	
	FIA_AFL.1 Authentication failure handling	Maximum authentication attempts unsuccessful authentication attempts occur during user login.	
	FIA_AFL.1 Authentication failure handling	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	
		An Administrator changes the type of authenticator, e.g., from password to biometrics	
Account Administration		Roles and users are added or deleted	
		The access control privileges of a user account or a role are modified	

FAU_GEN.2 User identity association (iteration 1)
Hierarchical to: No other components.

FAU_GEN.2.1 The IT environment shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review
Hierarchical to: No other components.

FAU_SAR.1.1 The IT environment shall provide Auditors with the capability to read all information from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation.

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.

FAU_SAR.3.1 The IT environment shall provide the ability to perform searches of audit data based on the type of event, the user responsible for causing the event, and as specified in Table 5-3 below.

Dependencies: FAU_SAR.1 Audit review

Table 5-3 Audit Search Criteria

Section/Function	Search Criteria
Certificate Request Remote and Local Data Entry	Identity of the subject of the certificate being requested
Certificate Revocation Request Remote and Local Data Entry	Identity of the subject of the certificate to be revoked

FAU_SEL.1 Selective audit (iteration 1)
Hierarchical to: No other components.

FAU_SEL.1.1 The IT environment shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) *[event type]*
b) *[no additional attributes]*.

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

FAU_STG.1 Protected audit trail storage (iteration 1)
Hierarchical to: No other components.

FAU_STG.1.1 The IT environment shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The IT environment shall be able to detect modifications to the audit records.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss (iteration 1)
Hierarchical to: FAU_STG.3

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

Dependencies: FAU_STG.1 Protected audit trail storage

FPT_STM.1 Reliable time stamps (iteration 1)
Hierarchical to: No other components.

FPT_STM.1.1 The IT environment shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.1.2 Roles

FMT_SMR.2 Restrictions on security roles
Hierarchical to: FMT_SMR.1

FMT_SMR.2.1 The IT environment shall maintain the roles: Administrator, Auditor, and Officer[5].

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

FMT_SMR.2.3 The IT environment shall ensure that:
a) no identity is authorized to assume both an Administrator and an Officer role;
b) no identity is authorized to assume both an Auditor and an Officer role; and
c) no identity is authorized to assume both an Administrator and an Auditor role.

Dependencies: FIA_UID.1 Timing of identification.

FMT_MOF.1 Management of security functions behavior (iteration 1)
Hierarchical to: No other components.

FMT_MOF.1.1 The IT environment shall restrict the ability to modify the behavior of the functions listed in Table 5-4 to the authorized roles as specified in Table 5-4.

Dependencies: FMT_SMR.1 Security roles.

Table 5-4 Authorized Roles for Management of Security Functions Behavior

Section/Function	Function/Authorized Role
Security Audit	The capability to configure the audit parameters shall be restricted to Administrators.
Identification and Authentication	The capability to specify or change *maximum authentication attempts* shall be restricted to Administrators. The capability to change authentication mechanisms shall be restricted to Administrators.
Account Administration	The capability to create user accounts and roles shall be restricted to Administrators. The capability to assign privileges to those accounts and roles shall be restricted to Administrators.

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.

FMT_MSA.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1 to restrict the ability to modify the security attributes *[Role assignment for users and access control privileges for objects]* to Administrators.

[5] The role definitions are listed below:
1. Administrator – role authorized to install, configure, and maintain the CIMC; establish and maintain user accounts; configure profiles and audit parameters; and generate Component keys.
2. Officer – role authorized to request or approve certificates or certificate revocations.
3. Auditor – role authorized to view and maintain audit logs.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components.

FMT_MSA.3.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1 to provide *[permissive]* default values for security attributes that are used to enforce the SFP.

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

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

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.

FMT_MTD.1.1 The IT environment shall restrict the ability to view (read) or delete the audit logs to Auditors.

Dependencies: FMT_SMR.1 Security roles

FMT_MSA.2 Secure security attributes
Hierarchical to: No other components.

FMT_MSA.2.1 The IT environment shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security Roles

5.1.3 Access Control

FDP_ACC.1 Subset access control (iteration 1)
Hierarchical to: No other components.

FDP_ACC.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1on [*all users, files and access files*].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control (iteration 1)
Hierarchical to: No other components.

FDP_ACF.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1 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 IT environment shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: The capability to zeroize plaintext private and secret keys shall be restricted to Administrators, Auditors and Officers.

FDP_ACF.1.3 The IT environment shall explicitly authorize access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The IT environment shall explicitly deny access of subjects to objects based on the [*no additional rules*].

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

FPT_SEP.1 TSF domain separation
Hierarchical to: No other components.

FPT_SEP.1.1 Each operating system in the IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 Each operating system in the IT environment shall enforce separation between the security domains of subjects in its scope of control.

Dependencies: No dependencies

FPT_RVM.1 Non-bypassability of the TSP (iteration 1)
Hierarchical to: No other components.

FPT_RVM.1.1 Each operating system in the IT environment shall ensure that its policy enforcement functions are invoked and succeed before each function within its scope of control is allowed to proceed.

Dependencies: No dependencies

5.1.4 Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.

FIA_ATD.1.1 The IT environment shall maintain the following list of security attributes belonging to individual users: the set of roles that the user is authorized to assume, *[no other security attributes*].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication (iteration 1)
Hierarchical to: No other components.

FIA_UAU.1.1 The IT environment shall allow *[access to the IT Environment login window]* on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification (iteration 1)
Hierarchical to: No other components.

FIA_UID.1.1 The IT environment shall allow *[access to the IT Environment login window]* on behalf of the user to be performed before the user is identified.

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

Dependencies: No dependencies.

FIA_USB.1 User-subject binding (iteration 1)
Hierarchical to: No other components.

FIA_USB.1.1 The IT environment shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User attribute definition

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.

FIA_AFL.1.1 If authentication is not performed in a cryptographic module that has been FIPS 140-1 validated to an overall Level of 2 or higher with Level 3 or higher for Roles and Services, the IT environment shall detect when an Administrator configurable maximum authentication attempts unsuccessful authentication attempts have occurred since the last successful authentication for the indicated user identity.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the IT environment shall *[disable the related user account for 15 minutes]*.

Dependencies: FIA_UAU.1 Timing of authentication

FTP_TRP.1 Trusted path
Hierarchical to: No other components.

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

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

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

Dependencies: No dependencies

5.1.5 Remote Data Entry and Export

FDP_ITT.1 Basic internal transfer protection (iteration 1)
Hierarchical to: No other components.

FDP_ITT.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1 to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the IT environment.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.1 Basic internal transfer protection (iteration 2)
Hierarchical to: No other components.

FDP_ITT.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1 to prevent the disclosure of confidential user data when it is transmitted between physically-separated parts of the IT environment.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1 Basic data exchange confidentiality (iteration 1)
Hierarchical to: No other components.

FDP_UCT.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section 9.1 to be able to transmit objects in a manner protected from unauthorized disclosure.

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]

FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 1)
Hierarchical to: No other components.

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

Dependencies: No dependencies

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

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

Dependencies: No dependencies

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

FPT_ITT.1.1 The IT environment shall protect confidential IT environment data from disclosure when it is transmitted between separate parts of the IT environment.

Dependencies: No dependencies

5.1.6 Key Management

FCS_CKM.1 Cryptographic key generation (iteration 1)
Hierarchical to: No other components.

FCS_CKM.1.1 The FIPS 140-1 validated cryptographic module shall generate cryptographic keys in accordance with *[RSA, DSA, ECDSA, CAST5, DES, Triple-DES and AES]* that meet the following: *[FIPS PUB 186-2 (RSA and DSA), ANSI X9.62 (ECDSA), FIPS 186-2 APPENDIX 3 (CAST5, DES, 3DE and AES) and PUB 197 (AES)]*.

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

FCS_CKM.4 Cryptographic key destruction (iteration 1)
Hierarchical to: No other components.

FCS_CKM.4.1 The IT environment shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[zeroization]* that meets the following: *[FIPS 140-1]*.

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

5.1.7 Self-tests

FPT_AMT.1 Abstract machine testing
Hierarchical to: No other components

FPT_AMT.1.1 The IT environment shall run a suite of tests *[during initial start-up and at the request of an authorized user]* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the IT environment.

Dependencies: No dependencies.

FPT_TST_CIMC.2 Software/firmware integrity test
Hierarchical to: No other components.

FPT_TST_CIMC.2.1 An error detection code (EDC) or FIPS-approved or recommended authentication technique (e.g., the computation and verification of an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware residing within the CIMC (e.g., within EEPROM and RAM). The EDC shall be at least 16 bits in length.

FPT_TST_CIMC.2.2 The error detection code, authentication code, keyed hash, or digital signature shall be verified at power-up and on-demand. If verification fails, the IT environment shall *[report an error].*

Dependencies: FPT_AMT.1 Abstract machine testing.

FPT_TST_CIMC.3 Software/firmware load test
Hierarchical to: No other components

FPT_TST_CIMC.3.1 A cryptographic mechanism using a FIPS-approved or recommended authentication technique (e.g., an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware that can be externally loaded into the CIMC.

FPT_TST_CIMC.3.2 The IT environment shall verify the authentication code, keyed hash, or digital signature whenever the software or firmware is externally loaded into the CIMC. If verification fails, the IT environment shall *[report an error].*

Dependencies: FPT_AMT.1 Abstract Machine Testing

5.1.8 Cryptographic Modules

FCS_COP.1 Cryptographic operation (iteration 1)
Hierarchical to: No other components.

FCS_COP.1.1 The FIPS 140-1 validated cryptographic module shall perform *[encryption and decryption, digital signature generation and verification, hashing, Message Authentication Code (MAC) generation and verification]* in accordance with *[RFC 2144 (CAST5), FIPS PUB 46-3 (DES/3DES), FIPS PUB 186-2 (DSA, RSA, ECDSA), FIPS PUB 180-1 (SHA-1), FIPS PUB 113 (MAC) and FIPS PUB 197 (AES)]*.

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

5.2 TOE Security Functional Requirements

This section specifies the security functional requirements that are applicable to the TOE. Operations that are completed on the SFR components are indicated throughout this section through the use of Bold Italic text.

Table 5-5: TOE Functional Security Requirements

Security Requirement		Component
Security Audit (FAU)	Audit data generation (iteration 2)	FAU_GEN.1
	User identity association (iteration 2)	FAU_GEN.2
	Selective audit (iteration 2)	FAU_SEL.1
	Protected audit trail storage (iteration 2)	FAU_STG.1
	Prevention of audit data loss (iteration 2)	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)	CIMC private and secret key zeroization	FCS_CKM_CIMC.5
	Cryptographic key generation (iteration 2)	FCS_CKM.1
	Cryptographic key destruction (iteration 2)	FCS_CKM.4
	Cryptographic operation (iteration 2)	FCS_COP.1
User Data Protection (FDP)	Subset access control (iteration 2)	FDP_ACC.1
	Security attribute based access control (iteration 2)	FDP_ACF.1
	User private key confidentiality protection	FDP_ACF_CIMC.2
	User secret key confidentiality protection	FDP_ACF_CIMC.3
	CIMC backup and recovery	FDP_CIMC_BKP.1
	Extended CIMC backup and recovery	FDP_CIMC_BKP.2
	Certificate Generation	FDP_CIMC_CER.1
	Certificate Revocation	FDP_CIMC_CRL.1
	Certificate status export	FDP_CIMC_CSE.1

Security Requirement		Component
	Extended user private and secret key export	FDP_ETC_CIMC.5
	Basic internal transfer protection (iterations 3 and 4)	FDP_ITT.1
	Stored public key integrity monitoring and action	FDP_SDI_CIMC.3
	Basic data exchange confidentiality (iteration 2)	FDP_UCT.1
Identification and Authentication (FIA)	Timing of authentication (iteration 2)	FIA_UAU.1
	Timing of identification (iteration 2)	FIA_UID.1
	Verification of secrets	FIA_SOS.1
	User-subject binding (iteration 2)	FIA_USB.1
Security Management (FMT)	Management of security functions behavior (iteration 2)	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 (iteration 2)	FPT_ITC.1
	Basic internal TSF data transfer protection (iterations 3 and 4)	FPT_ITT.1
	Non-bypassability of the TSP (iteration 2)	FPT_RVM.1
	Reliable time stamps (iteration 2)	FPT_STM.1

5.2.1 Security Audit

FAU_GEN.1 Audit data generation (iteration 2)
Hierarchical to: No other components.

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 5-6 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, and the outcome (success or failure) of the event; and
b) For each audit event type, the information specified in the Additional Details column in Table 5-6 below.

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

Dependencies: FPT_STM.1 Reliable time stamps

Table 5-6 Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
Security Audit	FAU_GEN.1 Audit data generation (iteration 2)	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	
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.4 User private and secret key export FMT_MTD_CIMC.6 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.

Section/Function	Component	Event	Additional Details
CIMC Configuration		Any security-relevant changes to the configuration of the TSF	
Certificate Profile Management	FMT_MOF_CIMC.2 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.4 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 (iteration 2)
Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

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

FAU_SEL.1 Selective audit (iteration 2)
Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) *[event type (severity)]*
b) *[event number, range of event numbers]*.

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

FAU_STG.1 Protected audit trail storage (iteration 2)
Hierarchical to: No other components.

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

FAU_STG.1.2 The TSF shall be able to detect modifications to the audit records.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss (iteration 2)
Hierarchical to: FAU_STG.3

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

Dependencies: AU_STG.1 sheltered audit trail storage

FPT_STM.1 Reliable time stamps (iteration 2)
Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.
Dependencies: No dependencies.

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 function behavior

5.2.2 Roles

FMT_MOF.1 Management of security functions behavior (iteration 2)
Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in Table 5-7 to the authorized roles as specified in Table 5-7.

Dependencies: FMT_SMR.1 Security roles

Table 5-7 Authorized Roles for Management of Security Functions Behavior

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.
Backup and Recovery .		The capability to configure the backup parameters shall be restricted to Administrators. The capability to initiate the backup or recovery function shall be restricted to *[Administrator*].
Certificate		The capability to approve fields or extensions to be

Section/Function	Component	Function/Authorized Role
Registration		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.2 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.4 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.

5.2.3 Backup and Recovery

FDP_CIMC_BKP.1 CIMC backup and recovery
Hierarchical to: No other components.

FDP_CIMC_BKP.1.1 The TSF shall include a backup function.

FDP_CIMC_BKP.1.2 The TSF shall provide the capability to invoke the backup function on demand.

FDP_CIMC_BKP.1.3 The data stored in the system backup shall be sufficient to recreate the state of the system at the time the backup was created using only:

a) a copy of the same version of the CIMC as was used to create the backup data;
b) a stored copy of the backup data;
c) the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and

d) the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.

FDP_CIMC_BKP.1.4 The TSF shall include a recovery function that is able to restore the state of the system from a backup. In restoring the state of the system, the recovery function is only required to create an "equivalent" system state in which information about all relevant CIMC transactions has been maintained.

Dependencies: FMT_MOF.1 Management of security functions behavior

FDP_CIMC_BKP.2 Extended CIMC backup and recovery
Hierarchical to: No other components.

FDP_CIMC_BKP.2.1 The backup data shall be protected against modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_CIMC_BKP.2.2 Critical security parameters and other confidential information shall be stored in encrypted form only.

Dependencies: FDP_CIMC_BKP.1 CIMC backup and recovery

5.2.4 Access Control

FDP_ACC.1 Subset access control (iteration 2)
Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 on *[all Entrust Authority data objects and services associated with operations performed by Entrust users, including Administrators, Officers and Auditors].*

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control (iteration 2)
Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 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 rules specified in Table 5-8 to determine if an operation among controlled subjects and controlled objects is allowed.

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 *[none].*

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

Table 5-8 Access Controls

Section/Function	Component	Event
Certificate Request Remote and		The entry of certificate request data shall be

Section/Function	Component	Event
Local Data Entry		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	FCS_CKM.1 Cryptographic 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 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

Section/Function	Component	Event
		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.

FPT_RVM.1 Non-bypassability of the TSP (iteration 2)
Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Dependencies: No dependencies

5.2.5 Identification and Authentication

FIA_UAU.1 Timing of authentication (iteration 2)
Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow *[access to the login screen and help menu from the SMA 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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification (iteration 2)
Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow *[access to the login screen and help menu from the SMA 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.

Dependencies: No dependencies.

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 the following criteria:

1) **Specified Master User password rules applicable to**:

- ***minimum number of upper case letters (default: 1)***
- ***minimum number of digits (default: 1)***
- ***minimum number of lower case letters (default: 1)***
- ***minimum number of characters (default: 10)***

- ***character restriction (default: must not be part of home directory path)***
- ***valid characters (default: 0-9, a-z, A-Z, ~!@#$%^&*_+-=|:;<>?,./)***
- ***word restriction (default: must not include the words "Entrust")***
- ***character restriction (default: must not be a keyboard sequence)***
- ***word restriction (default: must not contain names, words or combination of words specified in dictionary files)***

2) ***Specified Security Officer, Administrator, Directory Administrator, Auditor, Self-Administration Server Administrator, End-User, and custom-defined roles password rules applicable to:***

- ***time to password expiry (default: 0)***
- ***password history (default: 8)***
- ***password length (default: 8)***
- ***at least one non-alphanumeric character (default: OFF)***
- ***at least one upper case letter (default: ON)***
- ***at least one lower case letter (default: ON)***
- ***at least one digit (default: OFF)***
- ***must not contain many occurrences of the same character (i.e., the most occurrences of the same character allowed in the password is half the length of the password) (always ON)***
- ***must not be the same as the Entrust profile username (always ON)***
- ***must not contain a long substring of the Entrust profile name (i.e., the longest allowable profile (.epf) username substring is equal to half the length of the password) (always ON).***

Dependencies: No dependencies.

FIA_USB.1 User-subject binding (iteration 2)
Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User attribute definition

5.2.6 Remote Data Entry and Export

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 *[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.

Dependencies: FIA_UID.1 Timing of identification

FDP_ITT.1 Basic internal transfer protection (iteration 3)
Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the TOE.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ITT.1 Basic internal transfer protection (iteration 4)
Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 to prevent the disclosure of confidential user data when it is transmitted between physically separated parts of the TOE.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_UCT.1 Basic data exchange confidentiality (iteration 2)
Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 to be able to transmit objects in a manner protected from unauthorized disclosure.

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]

FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 2)
Hierarchical to: No other components.

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

Dependencies: No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 3)
Hierarchical to: No other components.

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

Dependencies: No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 4)
Hierarchical to: No other components.

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

Dependencies: No dependencies

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

5.2.7 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 *[the X.509 standard for CRLs].*

Dependencies: No dependencies

5.2.8 Key Management

FCS_CKM.1 Cryptographic key generation (iteration 2)
Hierarchical to: No other components.

FCS_CKM.1.1 The FIPS 140-1 validated cryptographic module shall generate cryptographic keys in accordance with *[RSA, DSA, ECDSA, CAST5, DES, Triple-DES and AES]* that meet the following: *[FIPS PUB 186-2 (RSA and DSA), ANSI X9.62 (ECDSA), FIPS 186-2 APPENDIX 3 (CAST5, DES, 3DES and AES) and PUB 197 (AES)]*.

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

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 140-1 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 140-1 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 140-1 validated cryptographic module.

Dependencies: No dependencies

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 140-1 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 140-1 validated cryptographic module.

Dependencies: No dependencies

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 140-1 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]*.

ST Rational: It shall not be possible for a CIMC to use or distribute corrupted public keys. Failure in the verification of a public key shall report an error and generate an audit entry, which is consistent with maintenance of security.

Dependencies: No dependencies

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 140-1 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-1 validated cryptographic module.

Dependencies: No dependencies

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 140-1 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-1 validated cryptographic module.
Dependencies: No dependencies

FCS_CKM.4 Cryptographic key destruction (iteration 2)
Hierarchical to: No other components.

FCS_CKM.4.1 The FIPS 140-1 validated cryptographic module shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[zeroization]* that meets the following: *[FIPS 140-1]*.

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

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 140-1 validated cryptographic module.

Dependencies: FCS_CKM.4 Cryptographic key destruction
FDP_ACF.1 Security attribute based access control

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

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

5.2.9 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

5.2.10 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;
- 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

5.2.11 Certificate Registration

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 *[the X.509 standard for public key certificates]*.

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

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

FDP_CIMC_CER.1.4 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.

5.2.12 Certificate Revocation

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:

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.

Dependencies: No dependencies

5.2.13 Cryptographic module

FCS_COP.1 Cryptographic operation (iteration 2)
Hierarchical to: No other components.

FCS_COP.1.1 The FIPS 140-1 validated cryptographic module shall perform *[encryption and decryption, digital signature generation and verification, hashing, Message Authentication Code (MAC) generation and verification]* in accordance with *[RFC 2144 (CAST5), FIPS PUB 46-3 (DES/3DES), FIPS PUB 186-2 (DSA, RSA, ECDSA), FIPS PUB 180-1 (SHA-1), FIPS PUB 113 (MAC) and FIPS PUB 197 (AES)]*.

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

5.3 TOE 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 5-9 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 5-9 Assurance Requirements

Assurance Class	Component ID	Component Title

Assurance Class	Component ID	Component Title
Configuration Management	ACM_AUT.1	Partial CM Automation
	ACM_CAP.4	Authorization controls
	ACM_SCP.2	Problem tracking CM coverage
Delivery and Operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.2	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.4 Strength of Function Requirements

The minimum strength of function level for the TOE and IT environment functional security requirements is SOF-basic. The SOF-basic level shall apply except where specific strength of function requirements is specified later in this section.

5.4.1 Authentication Mechanisms

The authentication mechanisms specified in FIA_UAU.1 iterations 1 and 2 and supported by the password rules specified in FIA_SOS.1 shall meet the following strength of function requirements:

a) 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.)
b) 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.

5.4.2 Cryptographic Modules

FIPS 140-1 validated cryptographic modules must perform all cryptographic functions performed by CIMCs. FIPS 140-1 validated cryptographic modules are also required to generate cryptographic keys and to store plaintext private and secret keys.

5.4.2.1 Encryption and FIPS 140-1 Validated Modules

As noted earlier in the document, references to FIPS 140-1 refer to the most current version of the standard and the most current version can be found at http://csrc.nist.gov/cryptval.

5.4.2.1.1 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_CIMC_BKP.2 Extended CIMC backup and recovery
FDP_ETC_CIMC.4 User private and secret key export
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.6 TSF private and secret key export
FMT_MTD_CIMC.7 Extended TSF private and secret key export
FPT_CIMC_TSP.1 Audit log signing event
FPT_CIMC_TSP.2 Audit log time stamp event
FPT_TST_CIMC.2 Software/firmware integrity test
FPT_TST_CIMC.3 Software/firmware load test

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

5.4.2.1.2 FIPS 140-1 Validated Cryptographic Modules

Cryptographic modules specified for:

FCS_CKM.1 Cryptographic key generation
FDP_ACF_CIMC.2 User private key confidentiality protection
FDP_ACF_CIMC.3 User secret key confidentiality protection
FDP_ETC_CIMC.4 User private and secret key export
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.6 TSF private and secret key export
FMT_MTD_CIMC.7 Extended TSF private and secret key export
FPT_CIMC_TSP.1 Audit log signing event

shall be validated against FIPS 140-1.

5.4.2.1.3 Split Knowledge Procedures

Split-knowledge procedures specified in:

FDP_ETC_CIMC.4 User private and secret key export
FDP_ETC_CIMC.5 Extended user private and secret key export
FMT_MTD_CIMC.6 TSF 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 140-1.

5.4.2.1.4 Authentication Codes

The authentication code specified in:

FAU_STG.1 Protected audit trail storage
FCO_NRO_CIMC.4 Advanced verification of origin
FDP_CIMC_BKP.2 Extended CIMC backup and recovery
FPT_CIMC_TSP.1 Audit log signing event
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
FPT_TST_CIMC.2 Software/firmware integrity test
FPT_TST_CIMC.3 Software/firmware load test

shall be a FIPS-approved or recommended authentication code.

5.4.2.2 Cryptographic module levels for cryptographic functions that involve private or secret keys

All cryptographic operations performed (including key generation) at the request of the TOE shall be performed in a FIPS 140-1 validated cryptographic module operating in a FIPS-approved or recommended mode of operation.

Table 5-10 specifies for each category of use for a private or secret key, the required overall FIPS 140-1 level for the validated cryptographic module. If the CIMC generates certificate subject private keys, the required overall FIPS 140-1 level for Long Term Private Key Protection keys shall apply.

Table 5-10 FIPS 140-1 Level for Validated Cryptographic Module

Required Overall FIPS 140-1 Level for CIMC Cryptographic Modules	
Category of Use	**FIPS 140-1 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

The level of the validated cryptographic module is selected from the above table using the category of use (row). For example, if a key is used for general authentication, the cryptographic module must be validated to FIPS 140-1 Level 2, with level Roles and Services.

5.4.2.3 Cryptographic Functions That Do Not Involve Private or Secret Keys

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

1. **Hash Generation**: One-way hash functions may be used in the process of signature generation and verification (a signature is typically generated by applying a private key to the hash of the message). The generation of a hash does not require a key. Therefore, hash generation does not have the same confidentiality requirements of other cryptographic functions.

2. **Signature Verification**: Signatures are verified from a message text and a public key.

For a cryptographic module that only performs signature verification and/or keyless hash generation functions, the overall required FIPS 140-1 level shall be Level 1 for CIMC Security Levels 1 through 3 and Level 2 for CIMC Security Level 4.

6 TOE Summary Specification

6.1 IT Security Functions

This section describes the IT security functions provided by Entrust Authority to meet the SFRs specified for the TOE in Section 5.2. Each security function described in this section contributes to meeting one or several SFRs. A complete mapping of security functions and SFRs is provided in Table 8-10.

6.1.1 Security Audit

6.1.1.1 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 Appendix B of Reference 1, including all applicable events specified in the CIMC PP for level 3, as listed below in Table 6-1.

Table 6-1 Audited events as specified by CIMC PP for Level 3

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.

Event	TOE Functional Specification
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, including additions and deletions	Entrust Authority generates an audit event whenever public 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

6.1.1.2 Accountability of users

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

This security function addresses the following SFR: FAU_GEN.2

6.1.1.3 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

6.1.1.4 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

6.1.1.5 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

6.1.1.6 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

6.1.2 Roles

6.1.2.1 Role Definition

Entrust Authority maintains the roles[6] 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.

[6] The Entrust Master User role combined with the Entrust Security Officer role together consist of the CIMP Administrator role. The Entrust Administrator role consists of the CIMC Officer role. The Entrust Auditor role consists of the CIMC Auditor role. See Section 2.2.2.1 for details.

- **Administrator** The main role of the Administrator is 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.

- **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, Auditor, Self-Administration Server Administrator, End User, or any custom roles that may exist. The End User role actually has no privileges to access Entrust Authority via the SMA or SMC (i.e., an End User cannot log in to the SMA 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, Directory Administrator, Auditor, Self-Administration Server Administrator, 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 2-1.

This security function, in conjunction with the security function Management of security functions behavior described below in Section 6.1.2.2, addresses the following SFR: FMT_MOF.1

6.1.2.2 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 6-2 below:

Table 6-2 Role Restrictions

Section/Function	Function/Authorized Role
Security Audit	Except for controlling which audit logs are published externally which can be 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 certificate profile 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 6.1.2.1, addresses the following SFR: FMT_MOF.1

6.1.3 Backup and Recovery

Entrust Authority can perform two types of backups: full backups and incremental backups. Using a combination of both types of backups, Entrust Authority minimizes the risk of data loss in the event of a hardware or software failure.

During an incremental or full backup, Entrust Authority writes information to backup files. These files are located in subfolders of the backup directory. When the Entrust Authority database or its content changes (e.g., when a user is added), Entrust Authority creates a transaction log. The information a transaction log provides is a record of one change. As part of a backup (either full or incremental), Entrust Authority backs up the information in the transaction logs and then deletes the transaction logs. Entrust Authority creates new transaction logs to save changes that occur after completing the backup. Because transaction logs exist only until their information has been backed up, the transaction logs that exist at any particular time provide a record of changes that have occurred since the previous backup.

A full backup creates a set of files from which the entire database can be restored. During a full backup, Entrust Authority also backs up the Directory because it stores some of the same information as the database (e.g., users' public encryption and verification certificates). Backing up both the database and the Directory at the same point in time ensures that their contents are synchronized.

When running a full backup, Entrust Authority:

- may optionally validate the database beforehand to verify its integrity and records verification information in the audit logs;
- writes the database and Directory information to backup files; and

- moves the backup files to the backup folder and names the files using the current date and time.

The Entrust Authority database and its contents can be restored using a full backup or an incremental backup. After the restore is complete, the content of the Entrust Authority database is exactly the same as it existed when the backup was performed. It may also be possible to restore changes to the database that occurred after the backup and before the failure.

Since all security critical information in the database is encrypted and/or MACed, unauthorized disclosure and/or modification of backed up data is not a concern.

This security function addresses the following SFRs: FDP_CIMC_BKP.1 and FDP_CIMC_BKP.2

6.1.4 Access Control

6.1.4.1 Scope of Policy and Access Rules

The TOE controls access to all Entrust system data associated with operations initiated by any Entrust operator: Master User, Security Officer, Administrator, Auditor, Self-Administration Server Administrator, 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 6-3 to determine if an operation among controlled subjects and controlled objects is allowed.

Table 6-3 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 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.

Section/Function	Event
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

6.1.4.2 Non-bypassability of security functions

To maintain the security domain for Entrust Authority, all security-policy enforcing functions are invoked and succeed before each function is allowed to proceed.

This security function addresses the following SFR: FPT_RVM.1

6.1.5 Identification and Authentication

6.1.5.1 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

6.1.5.2 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

6.1.5.3 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

6.1.5.4 Password Rules (SoF - Basic)

Entrust Authority enforces that user-generated passwords (for Master User, Security Officer, Administrator, Directory Administrator, Auditor, Self-Administration Server Administrator, End-User, and custom-defined roles) meet the password criteria specified for the role, as described below:

1) For Master User:

   - minimum number of upper case letters (default: 1)
   - minimum number of digits (default: 1)
   - minimum number of lower case letters (default: 1)
   - minimum number of characters (default: 10)
   - character restriction (default: must not be part of home directory path)
   - valid characters (default: 0-9, a-z, A-Z, ~!@#$%^&*_+-=|:;<>?,./)
   - word restriction (default: must not include the words “Entrust”)
   - character restriction (default: must not be a keyboard sequence)
   - word restriction (default: must not contain names, words or combination of words specified in dictionary files)

2) For Security Officer, Administrator, Directory Administrator, Auditor, Self-Administration Server Administrator, End-User, and custom-defined roles:

   - time to password expiry (default: 0)
   - password history (default: 8)
   - password length (default: 8)
   - at least one non-alphanumeric character (default: OFF)
   - at least one upper case letter (default: ON)
   - at least one lower case letter (default: ON)
   - at least one digit (default: OFF)
   - must not contain many occurrences of the same character (i.e., the most occurrences of the same character allowed in the password is half the length of the password) (always ON)
   - must not be the same as the Entrust profile username (always ON)
   - must not contain a long substring of the Entrust profile name (i.e., the longest allowable profile (.epf) username substring is equal to half the length of the password) (always ON).

This security function addresses the following SFR: FIA_SOS.1.

6.1.6 Remote Data Entry and Export

6.1.6.1 Enforced Proof of Origin and Verification of Origin

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

Authority 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 Security Manager and SMA are conducted through Admin-API and EntrustSession which extends the enforcement of the access control policy to the physically separated while providing confidentiality and integrity of transmitted data.

This security function addresses the following SFR: FCO_NRO_CIMC.3

6.1.6.2 Protection of data communications between Security Manager and SMA

Entrust Authority internal communications between Security Manager and the SMA (which could be physically separated) are protected from disclosure and modification in EntrustSession or PKIX-CMP messages as all data is always encrypted and integrity-protected using digital signatures or MACs. Any services available to SMA 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

6.1.6.3 Trusted channel

Entrust Authority provides a trusted channel between itself and remote Entrust entities via PKIX-CMP (and SEP to support older versions of Entrust products). 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 Entrust Authority. 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

6.1.7 Certificate Management

6.1.7.1 Certificate Generation

Entrust Authority only generates certificates whose format complies with X.509 version 3. All generated certificates must be consistent with the defined certificate specification. Entrust Authority 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 (RSA/SHA-1 or DSA/SHA-1).

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

6.1.7.2 Certificate Status Export

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

This security function addresses the following SFR: FDP_CIMC_CSE.1

6.1.7.3 Certificate Profile Management

Entrust Authority implements certificate specifications 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

6.1.8 Certificate Revocation

6.1.8.1 CRL Profile Management

Entrust Authority 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 X.500 name 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

6.1.8.2 CRL Validation

Entrust Authority only generates CRLs whose format complies with X.509 version 2. 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 (RSA/SHA-1 or DSA/SHA-1). 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

6.1.9 Key Management

6.1.9.1 Key Generation

All key material used within Entrust Authority is generated and used within the FIPS 140-1 validated software-based Entrust Security Kernel v7.0 cryptographic module. The Security Kernel generates keys in accordance with RSA, DSA, ECDSA, CAST5, DES, Triple-DES and AES as specified in FIPS PUB 186-2 (RSA and DSA), ANSI X9.62 (ECDSA), FIPS 186-2 APPENDIX 3 (CAST5, DES, 3DES and AES) and PUB 197 (AES) respectively.

The keys used by the IT environment for user certificate signing and database protection are generated by a FIPS 140-1 level 3 validated hardware cryptographic device.

This security function addresses the following SFR: FCS_CKM.1

6.1.9.2 Private Key Protection

All key material used within Entrust Authority is generated and used within the FIPS 140-1 validated Entrust software. Keys are exported only when suitably protected, such as when encrypted under a public key, using FIPS 140-1 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, Entrust Authority can store the key used to encrypt the database (and all user private and secret keys) on a FIPS 140-1 level 3 validated hardware cryptographic device.

Subject private keys that are used to generate digital signatures are not generated by Authority 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

6.1.9.3 Public Key Protection

End-user public keys stored in the database by Entrust Authority are protected against unauthorized modification using a MAC. Entrust Authority 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.

Entrust Authority 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

6.1.9.4 Key Zeroization

The FIPS 140-1 validated Entrust Cryptographic module which is implemented as part of Entrust Authority provides the capability to zeroize plaintext secret and private keys. The hardware cryptographic module supported by Entrust Authority 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

6.1.10 Cryptographic Operations

All cryptographic operations are performed within the FIPS 140-1 validated software-based Entrust Security Kernel v7.0 cryptographic module. 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 (DES/3DES) and FIPS PUB 197 (AES);
- Signature generation/verification: FIPS PUB 186-2 (DSA, RSA, ECDSA);
- Hashing: FIPS PUB 180-1 (SHA-1); 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 FIPS 140-1 level 3 Chrysalis Luna CA3 hardware device is part of the IT environment.

This security function addresses the following SFR: FCS_COP.1

6.2 Assurance Measures

The assurance requirements for this TOE are met by EAL4-augmented, which stresses assurance through Entrust actions that are within or exceed the bounds of current best-commercial-practice. These assurance requirements provide, primarily via review of Entrust-supplied evidence, independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

1) Confirmation of effective configuration management, life-cycle model, problem tracking and remediation, and acceptance procedures

2) Confirmation of secure site development security measures

3) Confirmation of secure product delivery and installation procedures

4) Confirmation that the guidance documentation is adequate

5) Verification that the system security state is not misrepresented

6) Verification of a sample of the vendor functional testing

7) Verification of samples of the product implementation

8) Searching for vulnerabilities and verification of resistance against obvious penetration attacks

9) Independent functional testing

To define the assurance measures claimed to satisfy the security assurance requirements specified in Section 5.3, a mapping is provided between the Assurance Requirements and the Assurance Measures, which are intended to satisfy the Assurance Requirements. As shown in Table 8-11, the Assurance Measures are provided in the form of references to the relevant and appropriate document associated with each requirement.

6.3 Strength of Function Claims

Entrust Authority is designed to operate in a range of environments, from benign to hostile. Entrust Authority includes a software based FIPS 140-1 Level 2 validated cryptographic module (FIPS 140-1 validation certificate #308) that performs all cryptographic functions. For higher assurance or to operate in more hostile environments, Entrust Authority can also make use of a

FIPS 140-1 level 3 validated hardware cryptographic device also known as hardware security module (HSM). A HSM is typically used for either, or both, of these reasons:

- to store the CA signing key pair that Entrust Authority uses to sign certificates and CRL;
- to store a key that is used to protect the database.

Through the cryptographic functions provided by either the software based cryptographic module, the HSM or both, Entrust Authority provides integrity, confidentiality, nondisclosure, and authentication services.

Entrust Authority contains only one security function (i.e., authentication) that is realized by a probabilistic or permutational mechanism[7]. The minimum strength level specified in the CIMC PP is SOF-Basic. Thus, the global minimum strength level claimed for the TOE is also SOF-Basic. In addition to the SOF-Basic requirement, the CIMC PP also specifies several explicit SOF claims. Entrust Authority addresses these SOF claims as described in the following sections:

6.3.1 Authentication Mechanisms

Entrust Authority implements password policies and rules that allow the authentication mechanisms to meet and exceed the explicit SOF requirements specified by the CIMC PP (see above Section 5.4.1).

6.3.2 Cryptographic Modules

Entrust Authority performs all cryptographic functions, including key generation, key wrapping, encryption, digital signature, hashing, MACing and random number generation, within a FIPS 140-1 validated cryptographic module, as specified below under FIPS 140-1 Validated Cryptographic Modules**.**

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_CIMC_BKP.2 Extended CIMC backup and recovery
FDP_ETC_CIMC.4 User private and secret key export
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.6 TSF private and secret key export
FMT_MTD_CIMC.7 Extended TSF private and secret key export
FPT_CIMC_TSP.1 Audit log signing event
FPT_CIMC_TSP.2 Audit log time stamp event
FPT_TST_CIMC.2 Software/firmware integrity test
FPT_TST_CIMC.3 Software/firmware load test

are all performed using a FIPS-approved or recommended algorithm.

FIPS 140-1 Validated Cryptographic Modules
Cryptographic modules specified for:

[7] The strength of cryptographic algorithms is outside the scope of the CC. Strength of function only applies to probabilistic or permutational mechanisms that are non-cryptographic. Therefore, the SOF claim contained in this ST (i.e. SOF-Basic) does not apply to any cryptographic mechanisms.

FCS_CKM.1 Cryptographic key generation
FDP_ACF_CIMC.2 User private key confidentiality protection
FDP_ACF_CIMC.3 User secret key confidentiality protection
FDP_ETC_CIMC.4 User private and secret key export
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.6 TSF private and secret key export
FMT_MTD_CIMC.7 Extended TSF private and secret key export
FPT_CIMC_TSP.1 Audit log signing event

are validated against FIPS 140-1. All cryptographic operations are performed within the FIPS 140-1 level 2 Entrust Security Kernel 7.0 cryptographic module (validation certificate #308). The evaluated environment also includes the Chrysalis Luna CA3 hardware-based FIPS 140-1 level 3 validated cryptographic module (validation certificate #214). This Luna CA3 HSM is used to store the CA signing key pair and to generate signatures for certificates and CRLs; it also stores a key that is used to protect the database (and all Entrust Authority security sensitive data, including end-user key history).

Split Knowledge Procedures
Entrust Authority always export private or secret keys in encrypted form and does not employ any split key procedures.

Authentication Code
The authentication code specified in:

FAU_STG.1 Protected audit trail storage
FCO_NRO_CIMC.4 Advanced verification of origin
FDP_CIMC_BKP.2 Extended CIMC backup and recovery
FPT_CIMC_TSP.1 Audit log signing event
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
FPT_TST_CIMC.2 Software/firmware integrity test
FPT_TST_CIMC.3 Software/firmware load test

are FIPS-approved.

7 Protection Profile Claims

As previously mentioned in this ST, Entrust Authority Security Manager 7.0 conforms to the following Protection Profile (PP):

- Certificate Issuing and Management Components (CIMC) Security Level 3 PP, version 1.0, October 31, 2001.

All of the assumptions, threats, policies, objectives and security requirements defined for CIMC PP Security Level 3 (which includes also the ones defines for all levels) have been reproduced in this ST. No additional assumption, threat, policy, objective or security requirement has been used.

All operations performed on the IT security requirements are within the bounds set by the CIMC PP for Security Level 3. Assignment and selection operations on security requirements (Section 5) are indicated in *italic*.

8 Rationale

This section includes the rationale for the functional and assurance requirements specified for the TOE. The rationale is based on specified objectives, threats, assumptions, and policies.

8.1 Security Objectives Rationale

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

The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy or assumption is covered by at least one security objective. Table 8-1 maps security objectives for the TOE to threats, Table 8-2 maps security objectives for the environment to threats, and Table 8-3 maps security objectives for both the TOE and the environment to threats. Table 8-4 maps the organizational security policies to security objectives. Table 8-5maps assumptions to IT security objectives, listing which objectives each assumption helps to cover. The items in the tables are ordered alphabetically, sorted on the first column.

Table 8-1 Relationship of Security Objectives for the TOE to Threats

IT 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.Non-repudiation	T.Sender denies sending information
O.Preservation/trusted recovery of secure state	T.Critical system component fails
O.Sufficient backup storage and effective restoration	T.Critical system component fails, T.User error makes data inaccessible

Table 8-2 Relationship of Security Objectives for the Environment to Threats

Non-IT 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.Physical Protection	T.Hacker physical access
O.Repair identified security flaws	T.Flawed code T.Critical system component fails
O.Social Engineering Training	T.Social Engineering
IT security objective	**Threat**
O.Cryptographic functions	T.Disclosure of private and secret keys,

	T.Modification of secret/private keys
O.Periodically check integrity	T.Malicious code exploitation
O.Security roles	T.Administrators, Officers and Auditors commit errors or hostile actions
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 8-3 Relationship of Security Objectives for Both the TOE and the Environment to Threats

Non-IT Security Objective	Threat
O.Configuration management	T.Critical system component fails, T.Malicious code exploitation
O.Data import/export	T.Message content modification
O.Detect modifications of firmware, software, and backup data	T.User error makes data inaccessible, T.Administrators, 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 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 8-4 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

Table 8-5 Relationship of Assumptions to IT Security Objectives

Assumption IT Security	Objective
A.Auditors Review Audit Logs	O.Auditors Review Audit Logs
A.Authentication Data Management	O.Authentication Data Management
A.Communications Protection	O.Communications Protection
A.Competent Administrators, 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

8.1.1 Security Objectives Sufficiency

The following discussions provide information regarding:

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

8.1.1.1 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.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.

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.

Authorized Users

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.

Cryptography

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.

8.1.1.2 Policies and Objectives Sufficiency

P.Authorized use of information establishes that information is used only for its authorized purpose(s). This is addressed by the following objectives: **O.Maintain user attributes**, **O.Restrict actions before authentication**, **O.Security roles**, and **O.User authorization management**. **O.Restrict actions before authentication** ensures 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. Finally, **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.

8.1.1.3 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.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.

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.

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.

8.2 Security Requirements Rationale

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

8.2.1 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 is covered by at least one security requirement. The first table in this section, Table 8-6, addresses the mapping of security functional requirements to security objectives. The second table, Table 8-7, addresses the mapping of security assurance requirements to security objectives.

Table 8-6 Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
FAU_GEN.1 Audit data generation (iterations 1 and 2)	O.Individual accountability and audit records
FAU_GEN.2 User identity association (iterations 1 and 2)	O.Individual accountability and audit records
FAU_SAR.1 Audit review	O.Individual accountability and audit records O.Auditors Review Audit Logs
FAU_SAR.3 Selectable audit review	O.Individual accountability and audit records O.Auditors review audit logs
FAU_SEL.1 Selective audit (iterations 1 and 2)	O.Individual accountability and audit records O.Auditors review audit logs
FAU_STG.1 Protected audit trail storage (iterations 1 and 2)	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss (iterations 1 and 2)	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 (iterations 1 and 2)	O.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction (iterations 1 and 2)	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 (iterations 1 and 2)	O.Cryptographic functions
FDP_ACC.1 Subset access control (iterations 1 and 2)	O.Limitation of administrative access
FDP_ACF.1 Security attribute based access control (iterations 1 and 2)	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_BKP.1 CIMC backup and recovery	O.Object and data recovery free from malicious code, O.Preservation/trusted recovery of secure state, O.Sufficient backup storage and effective restoration
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	O.Detect modifications of firmware, software, and backup data, O.Object and data recovery free from 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 (iterations	O.Integrity protection of user data and software,

Functional Requirement	Objective
1 and 3)	O.Protect user and TSF data during internal transfer
FDP_ITT.1 Basic internal transfer protection (iterations 2 and 4)	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 (iterations 1 and 2)	O.Data import/export
FIA_AFL.1 Authentication failure handling	O.React to detected attacks
FIA_ATD.1 User attribute definition	O.Maintain user attributes
FIA_UAU.1 Timing of authentication (iterations 1 and 2)	O.Limitation of administrative access, O.Restrict actions before authentication
FIA_UID.1 Timing of identification (iterations 1 and 2)	O.Individual accountability and audit records, O.Limitation of administrative access
FIA_SOS.1 Selection of secrets	O.Limitation of administrative access
FIA_USB.1 User-subject binding (iterations 1 and 2)	O.Maintain user attributes
FMT_MOF.1 Management of security functions behavior (iterations 1 and 2)	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_MSA.1 Management of security attributes	O.Maintain user attributes, O.User authorization management
FMT_MSA.2 Secure security attributes	O.Security-relevant configuration management
FMT_MSA.3 Static attribute initialisation	O.Security-relevant configuration management
FMT_MTD.1 Management of TSF data	O.Individual accountability and audit records, O.Protect stored audit records
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
FMT_SMR.2 Restrictions on security roles	O.Security roles
FPT_AMT.1 Abstract machine testing	O.Periodically check integrity, O.Validation of security function
FPT_CIMC_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_ITC.1 Inter-TSF confidentiality during transmission (iterations 1 and 2)	O.Data import/export
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 1-4)	O.Protect user and TSF data during internal transfer
FPT_RVM.1 Non-bypassability of the TSP (iteration 1)	O.Operating System
FPT_RVM.1 Non-bypassability of the TSP (iteration 2)	O.Limitation of administrative access
FPT_SEP.1 TSF domain separation	O.Operating System
FPT_STM.1 Reliable time stamps (iterations 1 and 2)	O.Individual accountability and audit records, O.Time stamps
FPT_TST_CIMC.2 Software/firmware integrity test	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software, O.Object and data recovery free from malicious code, O.Periodically check integrity, O.Procedures for preventing malicious code, O.Validation of security function
FPT_TST_CIMC.3 Software/firmware load test	O.Integrity protection of user data and software, O.Object and data recovery free from malicious

Functional Requirement	Objective
	code, O.Periodically check integrity, O.Require inspection for downloads
FTP_TRP.1 Trusted path	O.Trusted path

Table 8-7 Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
ACM_AUT.1 Partial CM automation	selection of EAL 3, EAL 4, O.Configuration management
ACM_CAP.4 Generation support and acceptance procedures	selection of EAL 4, O.Configuration management
ACM_SCP.2 Problem tracking CM Coverage	selection of EAL-CSPP, EAL 4, O.Configuration management
ADO_DEL.2 Detection of modification	selection of EAL 4
ADO_IGS.1 Installation, Generation, and Start-up Procedures	selection of EAL 1, EAL-CSPP, EAL 3,EAL 4, O.Installation
ADV_FSP.2 Fully defined external interfaces	selection of EAL 4, O.Lifecycle security
ADV_HLD.2 Security enforcing high-level design	selection of EAL 3, EAL 4, O.Lifecycle security
ADV_IMP.1 Subset of the implementation of the TSF	selection of EAL 4, O.Lifecycle security
ADV_LLD.1 Descriptive low-level design	selection of EAL 4, O.Lifecycle security
ADV_RCR.1 Informal Correspondence Demonstration	O.Lifecycle security, selection of EAL 1, EAL-CSPP, EAL 3, EAL 4
ADV_SPM.1 Informal TOE security policy model	selection of EAL-CSPP, EAL 4, O.Lifecycle security
AGD_ADM.1 Administrator Guidance	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, O.Require inspection for downloads, O.Security-relevant configuration management, O.User authorization management, selection of EAL 1, EAL-CSPP, EAL 3, EAL 4
AGD_USR.1 User Guidance	O.Administrators, Officers and Auditors guidance documentation, O.Malicious Code Not Signed, O.Procedures for preventing malicious code, O.Require inspection for downloads, selection of EAL 1, EAL-CSPP, EAL 3, EAL 4
ALC_DVS.1 Identification of security measures	selection of EAL-CSPP, EAL 3, EAL 4
ALC_FLR.2 Flaw reporting procedures	O.Lifecycle security (Security Levels 2-4), O.Repair identified security flaws, selection of EAL-CSPP
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-CSPP, EAL 3, EAL 4
ATE_DPT.1 Testing - High-Level Design	selection of EAL-CSPP, EAL 3
ATE_FUN.1 Functional testing	selection of EAL-CSPP, EAL 3, EAL 4

Assurance Requirement	Objective
ATE_IND.2 Independent Testing - Sample	selection of EAL-CSPP, EAL 3, EAL 4
AVA_MSU.2 Validation of analysis	selection of EAL-CSPP, EAL 4
AVA_SOF.1 Strength of TOE Security Function Evaluation	selection of EAL-CSPP, EAL 3, EAL 4
AVA_VLA.2 Independent vulnerability analysis	selection of EAL 4

8.2.1.1 Security Requirements Sufficiency

8.2.1.1.1 Security Objectives for the TOE

Authorized Users

O.Certificates is provided by **FDP_CIMC_CER.1 (Certificate Generation)** which ensures that certificates are valid, and **FDP_CIMC_CRL.1 (Certificate revocation list validation), FDP_CIMC_CSE.1 (Certificate status export)** which ensures 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 can not 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 is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)** which covers the requirement that the state of the system be preserved so that it can be recovered in the event of a secure component failure.

O.Sufficient backup storage and effective restoration is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)** which covers the requirement that sufficient backup data is created and stored and that an effective restoration procedure is provided.

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.

Cryptography

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

8.2.1.1.2 Non-IT Security Objectives for the Environment

O.Administrators, Officers and Auditors guidance documentation is provided by **AGD_ADM.1 (Administrator Guidance)** and **AGD_USR.1 (User Guidance)** which ensure that adequate guidance on the secure operation of the TOE is provided to Administrators, Officers, and Auditors.

O.Auditors Review Audit Logs is provided by **A.Auditors Review Audit Logs** which ensures that auditors review the audit logs. It is supported by **AGD_ADM.1 (Administrator Guidance)** which ensures that Auditors are provided with the information they need to understand the contents of the audit logs. In addition, it is also supported by **FAU_SAR.1 (Audit review)** and **FAU_SAR.3 (Selectable audit review)** which cover the requirement that the audit records are made available for review, and **FAU_SEL.1 (Selective audit) (iterations 1 and 2)** which cover the requirement that security-relevant events are audited.

O.Authentication Data Management is provided by **A.Authentication Data Management** which covers the requirement that an authentication data management policy be enforced.

O.Communications Protection is provided by **A.Communications Protection** which covers the requirement that the system be adequately physically protected against loss of communications.

O.Competent Administrators, Officers and Auditors is provided by **A.Competent Administrators, Officers and Auditors** which covers the requirement that Administrators, Officers, and Auditors be capable of managing the TOE and the security of the information it contains. It is also supported by **AGD_ADM.1 (Administrator Guidance)** which ensures that Administrators, Officers, and Auditors are provided with the information they need to properly manage the TOE and its security functionality.

O.CPS is provided by **A.CPS** which covers the requirement that Administrators, Officers, and Auditors be familiar with the CP and CPS under which the TOE is operated.

O.Disposal of Authentication Data is provided by **A.Disposal of Authentication Data**, which covers the requirement that authentication data be disposed of properly after access has been removed.

O.Installation is provided by **ADO_IGS.1 (Installation, Generation, and Start-up Procedures)** and **AGD_ADM.1 (Administrator Guidance)** which cover the requirement that Administrators, Officers, and Auditors be provided with documentation describing the procedures necessary to securely install and operate the TOE. **A.Competent Administrators, Officers and Auditors** covers the requirement that competent Administrators, Officers, and Auditors, who are capable of securely managing the TOE, are used.

O.Malicious Code Not Signed is provided by **A.Malicious Code Not Signed** which covers the requirement that malicious code destined for the TOE is not signed by a trusted entity. It is also supported by **AGD_ADM.1 (Administrator Guidance)** and **AGD_USR.1 (User Guidance)** which ensure that entities that are trusted to sign code are aware of their responsibilities.

O.Notify Authorities of Security Issues is provided **by A.Notify Authorities of Security Issues** which covers the requirement that proper authorities be notified of any security issues that impact their systems.

O.Physical Protection is provided by **A.Physical Protection** which covers the requirement that TOE hardware, software, and firmware critical to security policy enforcement be protected from unauthorized physical modification.

O.Social Engineering Training is provided by **A.Social Engineering Training** which covers the requirement that general users, administrators, officers, and auditors are trained in techniques to thwart social engineering attacks.

O.Cooperative Users is provided by **A.Cooperative Users** which covers the requirement that users act in a cooperative manner.

O.Lifecycle security is provided by **ADV_FSP.2 (Fully defined external interfaces)**, **ADV_HLD.2 (Security enforcing high-level design)**, **ADV_IMP.1 (Subset of the implementation of the TSF)**, **ADV_LLD.1 (Descriptive low-level design), ADV_RCR.1 (Informal correspondence demonstration)**, and **ADV_SPM.1 (Information TOE security policy model)** which cover the requirement that security is designed into the CIMC. **ALC_FLR.2 (Flaw reporting procedures)** covers the requirement that flaws are detected and resolved during the operational phase.

O.Repair identified security flaws is provided by **ALC_FLR.2 (Flaw reporting procedures)** which covers the requirement that vendor repair security flaws that have been identified by a user.

8.2.1.1.3 IT Security Objectives for the Environment

O.Operating System is provided by **A.Operating System** which covers the requirement that the operating system(s) on which the TSF operates provides security functions required by the CIMC to counter the perceived threats for the appropriate Security Level. It is also supported by **FPT_RVM.1 (Non-bypassability of the TSP) (iteration 1**) and **FPT_SEP.1 (TSF domain separation)** which ensure that the operating system(s) on which the TSF operates provides domain separation and non-bypassability.

O.Periodically check integrity is provided by **FPT_AMT.1 (Abstract machine testing)** which covers the requirement provide periodic integrity checks on the system and **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** cover the requirement to periodically check the integrity of software.

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

O.Validation of security function is provided by **FPT_AMT.1 (Abstract machine testing)** which covers the requirement to ensure that security-relevant hardware and firmware are functioning correctly and **FPT_TST_CIMC.2 (Software/firmware integrity test)** which covers the requirement to ensure that security-relevant software is functioning correctly.

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

8.2.1.1.4 Security Objectives for the TOE and Environment

O.Configuration Management is provided by **FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2)** which covers the requirement that only authorized users can change the configuration of the system. **FMT_MOF_CIMC.3 (Extended certificate profile management)** covers the requirement that Administrators be 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.

O.Configuration Management is supported by **AGD_ADM.1 (Administrator Guidance)** which covers the requirement that Administrators be provided with documentation describing the configuration management features of the TOE and by **A.Competent Administrators, Officers and Auditors** and **A.CPS** which ensure that Administrators are competent and are familiar with the CPS under which the TOE is to be operated. O.Configuration

Management is also supported by **ACM_AUT.1 (Partial CM automation**), **ACM_CAP.4 (Generation support and acceptance procedures)**, and **ACM_SCP.2 (Problem tracking CM coverage)** which ensure that a configuration management system is implemented and used.

O.Data import/export is provided by **FDP_UCT.1 (Basic data exchange confidentiality) (iterations 1 and 2)** and **FPT_ITC.1 (Inter-TSF confidentiality during transmission) (iterations 1 and 2)** which cover the requirement that data other than private and secret keys be protected when they are transmitted and from the **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 **FPT_TST_CIMC.2 (Software/firmware integrity test)** which covers the requirement that modifications to software or firmware be detected and **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery)** which covers the requirement that modifications to backup data be detected. Since **FPT_TST_CIMC.2** and **FDP_CIMC_BKP.2** make use of digital signatures, keyed hashes, or authentication codes to detect modifications, **FMT_MTD_CIMC.4 (TSF private key confidentiality protection)** and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are necessary to ensure that an attacker who has modified firmware, software, or backup data can not prevent detection of the modification by computing a new digital signature, keyed hash, or authentication code.

O.Individual accountability and audit records is provided by a combination of requirements. **FIA_UID.1 (Timing of identification) (iterations 1 and 2)** covers the requirement that users be identified before performing any security-relevant operations. **FAU_GEN.1 (Audit data generation) (iterations 1 and 2)** and **FAU_SEL.1 (Selective audit) (iterations 1 and 2)** cover the requirement that security-relevant events be audited while **FAU_GEN.2 (User identity association) (iterations 1 and 2)** and **FPT_STM.1 (Reliable time stamps) (iterations 1 and 2)** 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. **FMT_MTD.1 (Management of TSF data)** covers the requirement that audit data be available for review by ensuring that users, other than Auditors, cannot delete audit logs. Finally, **FAU_SAR.1 (Audit review)** and **FAU_SAR.3 (Selectable audit review)** cover the requirement that the audit records are made available for review so that individuals can be held accountable for their actions.

O.Integrity protection of user data and software is provided by **FDP_ITT.1 (Basic internal transfer protection) (iterations 1 and 3)** and **FDP_SDI_CIMC.3 (Stored public key integrity monitoring and action)** which cover the requirement that user data be protected and **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** which cover the requirement that software and firmware be protected. Since data and software are protected using cryptography, **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.

O.Limitation of administrative access is provided by **FDP_ACC.1 (Subset access control) (iterations 1 and 2**), **FDP_ACF.1 (Security attribute based access control) (iterations 1 and 2)**, **FIA_UAU.1 (Timing of authentication) (iterations 1 and 2),** and **FIA_UID.1 (Timing of identification) (iterations 1 and 2)**. **FIA_UAU.1 (Timing of authentication) (iterations 1 and 2) and FIA_UID.1 (Timing of identification) (iterations 1 and 2)** ensure that Administrators, Officers, and Auditors can not perform any security-relevant operations until they have been identified and authenticated and **FDP_ACC.1 (Subset access control) (iterations 1 and 2)** and **FDP_ACF.1 (Security attribute based access control) (iterations 1 and 2)** ensure that Administrators, Officers, and Auditors can only perform those operations necessary to perform

their jobs. **FPT_RVM.1 Non-bypassability of the TSP (iteration 2)** ensure that Administrators, Officers, and Auditors can not perform operations that they are not authorized to perform by bypassing the TSP enforcement functions.
FIA_SOS.1 ensures that password rules used for authentication are enforced against all operators (and end users), preventing the selection of weak passwords and reducing the likelihood of unauthorized access to administrative functions.

O.Maintain user attributes is provided by **FIA_ATD.1 (User attribute definition)** and **FIA_USB.1 (User-subject binding) (iterations 1 and 2)** which cover the requirement to maintain a set of security attributes associated with individual users and/or subjects acting on users' behalves. **FMT_MSA.1 (Management of security attributes)** ensures that only authorized users can modify security attributes.

O.Manage behavior of security functions is provided by **FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2)** which 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 is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** which cover the requirement that the recovered state is free from malicious code.
FDP_CIMC_BKP.2 (Extended CIMC backup and recovery) covers the requirement to be able to recover to a viable state.

O.Procedures for preventing malicious code is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** which ensures that only signed code can be executed and **AGD_ADM.1 (Administrator Guidance**), **AGD_USR.1 (User Guidance)** and **A.Malicious Code Not Signed** which ensure that those who are capable of signing code do not to sign malicious code. It is also 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)** which ensure that an untrusted entity can not use a trusted entity's key to sign malicious code.

O.Protect stored audit records is provided by **FAU_STG.1 (Protected audit trail storage) (iterations 1 and 2)** which covers the requirement that audit records be protected against modification or unauthorized deletion and **FMT_MTD.1 (Management of TSF data)** which covers the requirement that audit records be protected from unauthorized access.
FPT_CIMC_TSP.1 (Audit log signing event) is required so that modifications to the audit logs can be detected.

O.Protect user and TSF data during internal transfer is provided by **FDP_ITT.1 (Basic internal transfer protection) (iterations 1-4)** which covers the requirement that user data be protected during internal transfer and **FPT_ITT.1 (Basic internal TSF data transfer protection) (iterations 1-4)** which covers the requirement that TSF data be protected during internal transfer.

O.Require inspection for downloads is provided by **FPT_TST_CIMC.3 (Software/firmware load test)** which covers the requirement that downloaded software can not be loaded until it has been signed and by **AGD_ADM.1 (Administrator Guidance)**, **AGD_USR.1 (User Guidance)**, and **A.Malicious Code Not Signed** which ensure that those who are capable of signing code do not to sign malicious code.

O.Respond to possible loss of stored audit records is provided by **FAU_STG.4 (Prevention of audit data loss) (iterations 1 and 2)** which 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) (iterations 1 and 2)** which 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 by **FMT_MSA.3 (Static attribute initialisation)** and **FMT_MSA.2 (Secure security attributes)** which cover the requirement that security attributes have secure values. **FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2)** ensures that security-relevant configuration data can only be modified by those who are authorized to do so. O.Security-relevant configuration management is also supported by **AGD_ADM.1 (Administrator Guidance)** which covers the requirement that Administrators be provided with documentation describing the configuration management features of the TOE and by **A.Competent Administrators, Officers and Auditors** and **A.CPS** which ensure that 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) (iterations 1 and 2)** which covers the requirement that the time stamps be reliable.

O.User authorization management is provided by **FMT_MSA.1 (Management of security attributes)** which covers the requirement that Administrators manage and update user's security attributes. O.User authorization management is also supported by **AGD_ADM.1 (Administrator Guidance)** which covers the requirement that Administrators be provided with documentation describing the user authorization management features of the TOE and by **A.Competent Administrators, Officers and Auditors** and **A.CPS** which ensure that Administrators are competent and are familiar with the CPS under which the TOE is to be operated.

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)** which cover the requirement that the user who detected the attack be able to destroy any plaintext keys within the TOE in order to prevent the attacker from obtaining copies of these keys. **FIA_AFL.1 (Authentication failure handling)** covers the requirement that the TSF respond to detected attacks (in the form of repeated authentication attempts) by taking actions to prevent the attacker from successfully authenticating him/herself in the case that an attack is detected by an Administrator, Auditor, or Officer.

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

8.3 Internal Consistency and Mutual Support

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole. Internal consistency is demonstrated in an analysis of dependencies. Mutual support is shown through consideration of the interactions between and among the SFRs.

8.3.1 Rationale that Dependencies are Satisfied

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

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

Table 8-8 Summary of Security Functional Requirements Dependencies

Component	Dependencies	Which is:
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification Included	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3	Included
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ACF.1 Security attribute based access control	Included
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	FMT_MOF.1 Management of security functions behavior	Included
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_ETC_CIMC.5 Extended	None	

Component	Dependencies	Which is:
user private and secret key export		
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	FTP_TRP.1 Included
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_SOS.1 Selection of secrets	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.2 Secure security attributes	ADV_SPM.1 Informal TOE security policy model	Included
	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security Roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FMT_MTD_CIMC.6	Included

Component	Dependencies	Which is:
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_AMT.1 Abstract machine testing	None	
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1 Audit data generation	Included
	FMT_MOF.1 Management of security functions behavior	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_AMT.1 Abstract machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_AMT.1 Abstract Machine Testing	Included
FTP_TRP.1 Trusted path	None	

8.3.2 Security Assurance Requirements Dependencies

Table 8-9 below provides a summary of the security assurance requirements dependency analysis.

Table 8-9 Summary of Security Assurance Requirements Dependencies

Component	Depends On:	Which is:
ACM_AUT.1	ACM_CAP.3	Included (hierarchical to ACM_CAP.4)
ACM_CAP.4	ACM_SCP.1	Included (hierarchical to ACM_SCP.3)
	ALC_DVS.1	Included
ACM_SCP.2	ACM_CAP.3	Included (hierarchical to ACM_CAP.4)
	(indirect) ALC_DVS.1	Included
ADO_DEL.2	ACM_CAP.3	Included (hierarchical to ACM_CAP.4)
	(indirect) ACM_SCP.1	Included (hierarchical to ACM_SCP.2)
	(indirect) ALC_DVS.1	Included
ADO_IGS.1	AGD_ADM.1	Included
	(indirect) ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	Included
ADV_HLD.2	ADV_FSP.1	(hierarchical to ADV_FSP.2)
	ADV_RCR.1	Included
ADV_IMP.1	ADV_LLD.1	Included
	ADV_RCR.1	Included
	ALC_TAT.1	Included
	(indirect) ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	Included
ADV_LLD.1	ADV_HLD.2	Included
	ADV_RCR.1	Included

Component	Depends On:	Which is:
	(indirect) ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
ADV_RCR.1	None	
ADV_SPM.1	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	Included
AGD_ADM.1	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	Included
AGD_USR.1	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	Included
ALC_DVS.1	None	
ALC_FLR.2	None	
ALC_TAT.1	ADV_IMP.1	Included
	(indirect) ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	Included
	(indirect) ADV_LLD.1	Included
	(indirect) ADV_RCR.1	Included
ATE_COV.2	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	ATE_FUN.1	Included
	(indirect) ADV_RCR.1	Included
ATE_DPT.1	ADV_HLD.1	Included (hierarchical to ADV_HLD.2)
	ATE_FUN.1	Included
	(indirect) ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	Included
ATE_FUN.1	None	
ATE_IND.2	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	Included
	AGD_USR.1	Included
	ATE_FUN.1	Included
	(indirect) ADV_RCR.1	Included
AVA_MSU.2	ADO_IGS.1	Included
	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	Included
	AGD_USR.1	Included
	(indirect) ADV_RCR.1	Included
AVA_SOF.1	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	Included (hierarchical to ADV_HLD.2)
	(indirect) ADV_RCR.1	Included
AVA_VLA.2	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	ADV_HLD.2	Included
	ADV_IMP.1	Included
	ADV_LLD.1	Included
	AGD_ADM.1	Included
	AGD_USR.1	Included
	(indirect) ADV_RCR.1	Included
	(indirect) ALC_TAT.1	Included

8.4 Rationale that Requirements are Mutually Supportive

The security requirements work mutually so that each SFR is protected against bypassing, tampering, deactivation, and detection attacks by other SFRs.

8.4.1 Bypass

Prevention of bypass is derived as described below:

FIA_UID.1 and **FIA_UAU.1** support other functions' allowing user access to data by limiting the actions the user can take prior to identification and authentication.

FIA_SOS.1 reduces the likelihood of successful direct attack aimed at the authentication function, and thus supports **FIA_UAU.1**.

The management functions, including **FMT_MOF.1**, **FMT_MSA.1**, and **FMT_MTD.1** support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for bypass.

FMT_MSA.2 and **FMT_MSA.3** limit the acceptable values for secure data, thus providing protection from bypass to those SFRs dependent on that data.

FPT_RVM.1 ensures that SFRs cannot be bypassed.

8.4.2 Tamper

Prevention of tamper is derived as described below:

FAU_STG.1 protects the integrity of the audit trail.

FCS_CKM.1 and **FCS_COP.1** provide for the secure generation and handling of keys, and therefore support those SFRs that may rely on the use of those keys.

FIA_UID.1 and **FIA_UAU.1** support other functions allowing user access to data by limiting the actions the user can take prior to identification and authentication.

The management functions, including **FMT_MOF.1**, **FMT_MSA.1**, and **FMT_MTD.1** support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for tampering.

FDP_ETC_CIMC.5 prevents modification errors during export of secret and/or private keys.

FMT_MSA.2 and **FMT_MSA.3** limit the acceptable values for secure data, thus providing protection from tampering to those SFRs dependent on that data.

FPT_SEP.1 prevents tampering attacks against SFRs from external domains by preventing external interference by untrusted subjects, as supported by the abstract machine.

8.4.3 Deactivation

Prevention of deactivation is derived as described below:

The access control SFP detailed in **FDP_ACF.1** along with the other SFRs dealing with access control, provide for rigorous control of allowed data manipulations and thus prevent unauthorized deactivation.

The management functions, including **FMT_MOF.1**, **FMT_MSA.**1, and **FMT_MTD.1**, support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for tampering.

FMT_MSA.2 and **FMT_MSA.3** limit the acceptable values for secure data, thus providing protection from deactivation to those SFRs dependent on that data.

8.4.4 Detection

Detection is derived as described below:

The security audit functions, including **FAU_GEN.1**, **FAU_GEN.2**, and **FAU_SEL.1** provide for the generation of audit data that may be used to detect attempts to defeat specific SFRs or potential misconfiguration that could leave the TOE prone to attack.

FAU_SAR.1 and **FAU_SAR.3**, support the audit generation SFRs by providing the capability to selectively search the audit records.

FAU_STG.1, and **FAU_STG.4** provide for the protection of the audit records.

The management functions, including **FMT_MOF.1**, **FMT_MSA.1**, and **FMT_MTD.1**, support all other SFRs by restricting the ability to change certain management functions to certain specified roles, thus ensuring that other users cannot circumvent these SFRs.

FMT_MSA.2 and **FMT_MSA.3** limit the acceptable values for secure data, thus providing detection protection to those SFRs dependent on that data.

FMT_SMR.2 provides for the specification of multiple roles, thus supporting the other detection SFRs.

8.5 TOE Summary Specification Rationale

The TOE summary specification rationale is intended to show that the TOE security functions are suitable to meet the TOE security functional requirements. This is best accomplished by mapping the IT security functions onto the SFRs by means of a table. This mapping, as shown in Table 8-10, will show that:

- Each SFR is mapped onto at least one IT security function, and
- Each IT security function is mapped onto at least one SFR.

The details on how these functions meet the specific SFRs is provided in section 6.

Table 8-10 Security functions mapping

IT Security Function	CC Component	
Security Audit		
Section 6.1.1.1 Specification of auditable events and recorded information	FAU_GEN.1	Audit data generation (iteration 1)
Section 6.1.1.2 Accountability of users	FAU_GEN.2	User identity association (iteration 1)
Section 6.1.1.3 Audit data	FAU_SEL.1	Selective audit (iteration 1)
Section 6.1.1.4 Audit Data Protection	FAU_STG.1	Protected audit trail storage (iteration 1)
Section 6.1.1.5 Prevention of Audit Data Loss	FAU_STG.4	Prevention of audit data loss (iteration 1)
Section 6.1.1.6 Reliable Time Source	FPT_STM.1	Reliable time stamps (iteration 2)
Section 6.1.1.4 Audit Data Protection	FPT_CIMC_TSP.1	Audit log signing event
Roles		
Section 6.1.2.1 Role D Section 6.1.2.2 Management of security functions behavior	FMT_MOF.1	Management of security functions behavior (iteration 1)
Backup and Recovery		
Section 6.1.3 Backup and Recovery	FDP_CIMC_BKP.1	CIMC backup and recovery
Section 6.1.3 Backup and Recovery	FDP_CIMC_BKP.2	Extended CIMC backup and recovery
Access Control		
Section 6.1.4.1 Scope of Policy and Access Rules	FDP_ACC.1	Subset access control (iteration 1)
Section 6.1.4.1 Scope of Policy and Access Rules	FDP_ACF.1	Security attribute based access control (iteration 1)
Section 6.1.4.2 Non-bypassability of security functions	FPT_RVM.1	Non-bypassability of the TSP (iteration 1)
Identification and Authentication		
Section 6.1.5.1 Authentication of users	FIA_UAU.1	Timing of authentication (iteration 1)
Section 6.1.5.2 Identification of users	FIA_UID.1	Timing of identification (iteration 1)
Section 6.1.5.3 User-Subject Binding	FIA_USB.1	User-subject binding (iteration 1)
Section 6.1.5.4 Password Rules	FIA_SOS.1	Selection of secrets
Remote Data Entry and Export		
Section 6.1.6.1 Enforced Proof of Origin and Verification of Origin	FCO_NRO_CIMC.3	Enforced proof of origin and verification of Remote Data Entry and Export
Section 6.1.6.2Protection of data communications between Security Manager and SMA	FDP_ITT.1	Basic internal transfer protection (iterations 3 and 4)
Section 6.1.6.3 Trusted channel	FDP_UCT.1	Basic data exchange confidentiality (iteration 2)
Section 6.1.6.3 Trusted channel	FPT_ITC.1	Inter-TSF confidentiality during transmission (iteration 2)
Section 6.1.6.2Protection of data communications between Security Manager and SMA	FPT_ITT.1	Basic internal TSF data transfer protection (iterations 3 et 4)
Section 6.1.6.3 Trusted channel	FCO_NRO_CIMC.4	Advanced verification of origin
Certificate Status Export		
Section 6.1.7.2 Certificate Status Export	FDP_CIMC_CSE.1	Certificate status export
Key Management		
Section 6.1.9.1 Key Generation	FCS_CKM.1	Cryptographic key generation (iteration 2)
Section 6.1.9.2 Private Key Protection	FDP_ACF_CIMC.2	User private key confidentiality protection
Section 6.1.9.2 Private Key Protection	FMT_MTD_CIMC.4	TSF private key confidentiality protection
Section 6.1.9.3 Public Key Protection	FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
Section 6.1.9.2 Private Key Protection	FDP_ACF_CIMC.3	User secret key confidentiality protection
Section 6.1.9.2 Private Key Protection	FMT_MTD_CIMC.5	TSF secret key confidentiality protection
Section 6.1.9.4 Key Zeroization	FCS_CKM.4	Key Destruction (Iteration 2)
Section 6.1.9.4 Key Zeroization	FCS_CKM_CIMC.5	CIMC private and secret key zeroization
Section 6.1.9.2 Private Key Protection	FDP_ETC_CIMC.5	Extended user private and secret key export
Section 6.1.9.2 Private Key Protection	FMT_MTD_CIMC.7	Extended TSF private and secret key export
Certificate Profile Management		

IT Security Function	CC Component	
Section 6.1.7.3 Certificate Profile Management	FMT_MOF_CIMC.3	Extended certificate profile management
Certificate Revocation List Profile Management		
Section 6.1.8.1 CRL Profile Management	FMT_MOF_CIMC.5	Extended certificate revocation list profile management
Certificate Registration		
Section 6.1.7.1 Certificate Generation	FDP_CIMC_CER.1	Certificate Generation
Certificate Revocation		
Section 6.1.8.2 CRL Validation	FDP_CIMC_CRL.1	Certificate Revocation
Cryptographic module		
Section 6.1.10 Cryptographic Operations	FCS_COP.1	Cryptographic operation (iteration 2)

8.6 Rationale for Strength of Function

The TOE described in this PP is intended to operate in a range of environments, from benign to hostile. Also, the users may be hostile. Therefore, the TOE requires cryptographic functions to provide for integrity, confidentiality, nondisclosure, and authentication. The cryptographic functions must be included in a cryptographic module that has been validated against FIPS 140-1, Security Requirements for Cryptographic Modules. The level required for the cryptographic module depends on the type and use of the key. The cryptographic module levels are specified in Table 5-10. The increasing FIPS 140-1 level addresses the increased threats and potential for loss at the higher levels.

The user-selected secret (password) verification requirement specified in section 5.2.5 (FIA_SOS.1 Verification of secrets), and satisfied by the Password Rules security function described in section 6.1.5.4, provides adequate protection against unsophisticated attackers attempting to break or bypass authentication. This addresses the authentication strength of function requirements identified in section 5.4.1.

The TOE mechanisms will resist technical attacks by unauthorized users. The TOE mechanisms will also resist user errors, system errors, or non-malicious actions by authorized users. Resistance to higher-grade sophisticated types of attacks, when such resistance is required, is provided by the TOE operational environment. The environment also assumes that those individuals who have authorized physical access to the TOE are trusted to not behave maliciously.

Consequently, a level of strength of function basic (SoF-Basic) which indicates that a function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential is consistent with the security objectives of the TOE.

8.7 Assurance Requirements Rationale

CIMCs designed to meet Security Level 3 may be appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. Level 3 requires additional integrity controls to ensure data is not modified. A CIMC at Security Level 3 includes protections to protect against someone with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

The assurance level for this Security Level is EAL 3/EAL 4 augmented. Augmentation results from the selection of:

ACM_SCP.2 Problem tracking configuration management coverage

A vendor can be expected to apply configuration management to the items called out in ACM_SCP.2. Specifically, since the product is security related, the tracking of security flaws is a very reasonable expectation and within the bounds of standard, best commercial practice.

ADO_DEL.2 Detection of modification

A vendor can be expected to use a signature or other method to ensure that the code has not been tampered with prior to installation. Since the product is security related, this type of precaution should be expected.

ADV_FSP.2 Fully defined external interfaces

It is not a difficult task to fully define all external interfaces to the product. Indeed, this is necessary to correctly develop the product for interaction with other products. This will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ADV_IMP.1 Subset of the implementation of the TSF

This high a level of assurance requires that additional documentation regarding the implementation of the product be provided. It is through examination of this portion of the implementation that the product can be adequately evaluated with regard to the requirements.

ADV_LLD.1 Descriptive low-level design

This high a level of assurance requires that additional documentation regarding the design of the product be provided. It is through examination of this design that the product can be adequately evaluated with regard to the requirements.

ADV_SPM.1 Informal TOE security policy model

While the generation of a security policy does require security expertise, this can be performed by a consultant (if necessary) and does not otherwise impact the vendor's existing development process at this Security Level.

ALC_FLR.2 Flaw Report Procedures

EAL 3 and EAL 4 do not have the ALC_FLR component. It is within best commercial practices for a vendor of security products to have flaw reporting procedures covering:

- Addressing user reported problems
- Correcting flaws
- Notifying users and
- Revising procedures to reduce the potential for introducing new and/or additional flaws.

Specific procedures are not defined in the assurance requirement, therefore this should have minimal impact on vendors who have already implemented a flaw reporting program.

ALC_TAT.1 Well-defined development tools

It is important that very secure products be unambiguous.

AVA_MSU.2 Validation of analysis components

A security vendor implementing standard, best commercial practices will not be impacted by this component. AVA_MSU.2 requires that the vendor produce user and administrator documentation

that is adequate for understanding the operating modes of the TOE and the required external security controls necessary for secure operation. The vendor is required to analyze this documentation for conformance to the requirements.

AVA_VLA.2 Independent vulnerability analysis

Penetration attacks are very likely given the threat model for this Security Level. As a result, it is important that some penetration analysis and testing be performed..

8.7.1 Rationale for EAL4

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.

8.8 Assurance measures rationale

This part of the ST rationale is to show that the identified assurance measures are appropriate to meet the assurance requirements of Section 5.3. This is best demonstrated in the form of a table, mapping the identified assurance measures onto the assurance requirements, as shown below in Table 8-11.

In this case, the specification of assurance measures is done by reference to the appropriate document (e.g., Configuration Management Plan, System Architecture, User Guide, etc.). Rationale is provided to show that the referenced document (assurance measure) meets the requirements of the associated assurance requirement.

Table 8-11 Assurance measures

CC Assurance Component		Assurance Measure (Entrust document)	Rationale
ACM_AUT.1	Partial CM Automation	Configuration Management Plan	The assurance measure describes the automated means by which only authorized changes are made to the TOE implementation and addresses the requirements for automatic generation of the TOE and automated tools used in the CM system.
ACM_CAP.4	Generation Support and Acceptance Procedures	Configuration Management Plan	TOE releases are adequately identified with the version number. All Configuration Items (CI's) that comprise the TOE are under Configuration Management and are included on a CI List. The CM system is effective at ensuring that only authorized changes are made to CI's. The CM system generates records that will demonstrate that the CM system is used and include an acceptance plan.
ACM_SCP.2	Problem Tracking CM Coverage	Configuration Management Plan	The assurance measure addresses the documentation required to be under configuration control and describes the problem tracking system.
ADO_DEL.2	Detection of Modification	Delivery Procedures	The assurance measure addresses the requirement for secure delivery of the TOE. Secure delivery refers to tamper-evident delivery

CC Assurance Component		Assurance Measure (Entrust document)	Rationale
			and detection of modification.
ADO_IGS.1	Installation, Generation, and start-up	Installing Entrust Authority Security Manager 7.0 on Windows	The assurance measure addresses the requirement for installation procedures that are adequate to ensure that the user starts the TOE into a secure configuration.
ADV_FSP.2	Fully Defined External Interfaces	• Entrust Authority Security Manager 7.0 Operations Guide for Windows • Entrust Authority Security Manager Administration 7.0 User Guide for Windows • Entrust Authority 7.0 Addendum to Functional Specification	The assurance measure addresses the requirement for an informal functional specification. A detailed description of the external interfaces and rationale that the TSF is completely represented is provided.
ADV_HLD.2	High Level Design	Entrust Authority 7.0 High-Level Design	The assurance measure addresses the requirement for High-level design documentation that describes the informal TOE design, subsystem interfaces, and the security functionality provided by each subsystem.
ADV_IMP.1	Subset of the Implementation of the TSF	Code samples	The assurance measure addresses the requirements for providing the implementation representation for a selected subset of the TSF.
ADV_LLD.1	Descriptive Low-Level Design	Entrust Authority 7.0 Low-Level Design	The assurance measure addresses the requirement for Low-level design documentation that describes the informal low-level TOE design in terms of modules, including purpose of each module, interrelationship between the modules and module interfaces.
ADV_RCR.1	Informal Correspondence Demonstration	Entrust Authority 7.0 Informal Correspondence Demonstration	The assurance measure addresses the requirement for correspondence between the TOE summary specification and functional specification, the functional specification and high-level design, high-level design and low-level design, and low-level design and implementation.
ADV_SPM.1	Informal Security Policy Model	Entrust Authority 7.0 Informal Security Policy Model	The assurance measure addresses the requirement for informal security policy model and correspondence between the security policy model and the functional specification.
AGD_ADM.1	Administrator Guidance	Entrust Authority Security Manager 7.0 Operations Guide for Windows Entrust Authority Security Manager Administration 7.0 User Guide for Windows	The assurance measure addresses the requirement for administration guidance that is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AGD_USR.1	User Guidance	Entrust Authority Security Manager 7.0 Operations Guide for Windows Entrust Authority Security Manager Administration 7.0 User Guide for Windows	The assurance measure addresses the requirement for user guidance that is adequate to provide users with the required knowledge to securely access the TOE within the environment.
ALC_DVS.1	Identification of Security Measures	Identification of Security Measures	The assurance measure addresses the requirement for site development security

CC Assurance Component		Assurance Measure (Entrust document)	Rationale
			procedures.
ALC_FLR.2	Flaw Reporting Procedure	Problem Reporting System	The assurance measure addresses the requirement for flaw reporting and correction procedures.
ALC_LCD.1	Developer Defined Life-cycle Model	High Level Product Development Process	This assurance addresses the requirements for life-cycle model used in the development and maintenance of the TOE.
ALC_TAT.1	Well-defined Development Tools	Development Tools	This assurance measure addresses the requirements for definition of development tools and configuration used for the TOE.
ATE_COV.2	Analysis of Coverage	Entrust Authority 7.0 Analysis of Coverage	The assurance measure addresses the requirement for test coverage analysis that is complete.
ATE_DPT.1	Testing - High Level Design	Entrust Authority 7.0 Analysis of Depth of Testing	The assurance measure addresses the requirement for analysis that demonstrates that the TOE was tested to the high-level design documentation.
ATE_FUN.1	Functional Testing	Entrust Authority 7.0 Administrative Restrictions Test Case Suite Entrust Master Control 7.0 Full Test Case Suite Entrust SMA 7.0 Full Test Case Suite Entrust Authority 7.0 Security Function Tests Security Manager 7.0 Regression Test Plan Audit Customization Test Plan LunaCA3 driver upgrade to v2 Test Plan CA Hardware improvements Test Plan Entrust Authority 7.0 Functional Test Results (ATE_FUN.1)	The assurance measure addresses the requirement for test documentation produced by the TOE developer.
ATE_IND.2	Independent Testing	Entrust Authority Security Manager 7.0 Independent Testing Resources	The assurance measure addresses the requirement for test documentation that can be re-run by an independent third party.
AVA_MSU.2	Validation of Analysis	Entrust Authority 7.0 Validation of Analysis	The assurance measure addresses the requirement for guidance documentation for secure operation of the TOE in all modes of operations.
AVA_SOF.1	Strength of TSF Evaluation	Entrust Authority 7.0 Strength of Function Analysis	The assurance measure addresses the requirement for a SOF analysis that justifies the SOF claim.
AVA_VLA.2	Independent Vulnerability Analysis	Entrust Authority 7.0 Vulnerability Analysis	The assurance measure addresses the requirement for a vulnerability analysis that

CC Assurance Component		Assurance Measure (Entrust document)	Rationale
			addresses the search for ways to violate the TOE security. Justification is provided that the TOE is resistant to obvious penetration attacks.

9 ACCESS CONTROL POLICIES

9.1 IT Environment Access Control Policy

The IT environment shall support the administration and enforcement of an IT Environment 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.

9.2 TOE Access Control Policy

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

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

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.

10 Glossary

ADM-API	Administration API
AES	Advanced Encryption Standard
API	Application Programming Interface
ARL	Authority Revocation List
AS	Administration Service
CA	Certification Authority
CAST	Carlisle Adams, Stafford Tavares [Entrust symmetric key algorithm]
CC	Common Criteria
CIMC	Certificate Issuing and Management Component
COTS	Commercial Off The Shelf
CRL	Certificate Revocation List
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS PUB	Federal Information Processing Standard Publication
GUI	Graphical User Interface
I&A	Identification and Authentication
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union
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
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman [public key algorithm]
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

11 References

Reference 1 Entrust Authority Security Manager 7.0 Operations Guide for Windows, Entrust Inc., version 1.1, 2003.

Reference 2 Installing Entrust Authority Security Manager 7.0 on Windows. Entrust, Inc. 2003

Reference 3 FIPS 140-1 Validation Report: Entrust Cryptographic Kernel Version 7.0 2001.

Reference 4 ODBC 2.5 (Informix-CLI v2.8) Programmer's Reference. Informix Corporation. December 1998.

Reference 5 Microsoft Windows 2000 Common Criteria Evaluation http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/secureev.asp

Reference 6 RFC 1777. Lightweight Directory Access Protocol v2. W. Yeong, T. Howes, S. Kille. March 1995.

Reference 7 RFC 2251. Lightweight Directory Access Protocol v3. M. Wahl, T. Howes, S. Kille. December 1997.

Reference 8 Common Criteria for Information Security Evaluation. Version 2.1. CCIMB-99-031. August 1999.