RSA Certificate Manager Version 6.7 Security Target

RSA Security Inc.
174 Middlesex Turnpike
Bedford, MA 01730
USA
Tel: 877-RSA-4900
Fax: 781-515-5010
E-mail: vdc-eng@rsasecurity.com
Web: http://www.rsasecurity.com

Document ID: ASE
Issue Number: 1.7
Date: December 7, 2006

Revisions to Document			
Date	**Ver.**	**Author**	**Changes Made**
Aug. 18 2006	1.0	MJM	Update to RCM v6.7
Aug. 24, 2006	1.1	TC	Updated by SAIC for CCv2.3 changes
Oct. 15, 2006	1.2	MJM	Error corrections and updates
Oct. 22, 2006	1.4	MJM	Corrections per RSA ETR ASE – Revised (SAIC): • Changed cover page, updated year of pub. to 2006 • Section 1.1 corrected TOE identification • Section 1.1 corrected conformance "Part 3 augmented" • Many changes to SFR conventions • Section 5.1 backed out "based on the auditable event…" from FAU_GEN.1.2 (not a CCv2.3 change) • Section 5.1 fixed PP operation convention in FAU_SAR.1 • Section 5.1 backed out "no other actions" change from FAU_STG.4.1 (not a CCv2.3 change) • Section 5.2 added dependency to FMT_MOF.1.1, FMT_MSA.1.1, FMT_MTD.1.1 • Section 5.4 added FIA_USB.1.2 and FIA_USB.1.3 • Section 5.6 added AES/FIPS197 to FCS_CKM.1.1 • Section 5.6 added dependency to FCS_CKM.4.1 • Section 5.8 added algorithms, keylengths and dependency to FCS_COP.1.1 • Section 6.1 backed out "based on the auditable event…" from FAU_GEN.1.2 (not a CCv2.3 change) • Section 6.1 backed out "no other actions" change from FAU_STG.4.1 (not a CCv2.3 change) • Section 6.2 added dependency to FMT_MOF.1.1 • Section 6.5 removed reference to OCSP from assignment in FIA_UAU.1.1 and FIA_UID.1.1 • Section 6.5 added FIA_USB.1.2 and FIA_USB.1.3 • Section 6.6 reversed change in FDP_ITT.1.1 • Section 6.10 added note re. OCSP • Section 6.12 added note re. OCSP • Section 8.1.1 removed unsupported audit event from FAU_GEN.1 listing, "Local Data Entry/Remote Data Entry" listing, "CIMC Configuration" listing • Section 8.1.1 added "Final Audit Entry" to list of TOE audit startup/shutdown audit capabilities • Section 8.1.1 added clarifying text to FAU_STG.4 iteration 2 SFR mapping • Section 8.1.2 added clarifying text to Access Control

Nov. 15, 2006	1.5	MJM	Updated per ETR v0.3: • Section 6.5 FIA_USB.1 changes • Section 8.1.7 Identification & Authentication rewritten, SFR Mapping updated for FIA_USB.1
Nov. 16, 2006	1.6	MJM	Updated per SAIC comments: • Add build number to TOE Identification, Section 1.1 • Add disclaimer to Section 2.2.4 *CA Copy Tools*, indicating tools were not evaluated
Dec. 7, 2006	1.7	MJM	Updated per ETR and Evaluator comments: • Update version and remove proprietary markings • Remove Copy CA feature from list in section 2.1 • Update evidence in assurance measure sections to match actual evidence from Part 1 of the ETR • Update hardware requirements to provide a short list of known working platforms • Update to include “excluded features rationale”

Table of Contents

List of Tables

1.0 Security Target Introduction

The Security Target (ST) introduction section presents introductory information on the Security Target, the Target of Evaluation (TOE) referenced in this Security Target, and a basic introduction to the TOE.

1.1 ST and TOE Identification

This section will provide information necessary to identify and control the Security Target and the TOE; RSA Certificate Manager Version 6.7.

ST Title:	RSA Certificate Manager Version 6.7 Security Target – Version 1.7, December 7, 2006
TOE Identification:	RSA Certificate Manager Version 6.7 Build #411
CC Conformance:	Common Criteria for Information Technology Security Evaluation, Version 2.3, Part 2 – August 2005 CC Version 2.3 Part 2 - extended Common Criteria for Information Technology Security Evaluation, Version 2.3, Part 3 – August 2005 CC Version 2.3 Part 3 conformant
PP Conformance:	Certificate Issuing and Management Components (CIMC) Protection Profile Version 1.0 (Security Level 3) October 31, 2001
Assurance Level:	Evaluation Assurance Level 4 augmented with ALC_FLR.2 as required by CIMC PP SL3.
Keywords:	Public Key Infrastructure, PKI, Certificate Issuing and Management Component, CIMC. Certificate Authority, CA

1.2 Security Target Overview

This section will provide information on a Security Target's place in the Common Criteria evaluation process, a brief summary of the contents of this ST, and a statement of the Common Criteria Conformance claims made by this ST.

1.2.1 Security Target Definition

The Security Target for a TOE is a basis for agreement between the developers and evaluators on the security properties of the TOE and the scope of the evaluation. The audience for the ST is not confined to those responsible for the production of the TOE

and its evaluation, but may also include those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE.

This specific ST is based on the Certificate Issuing and Management Components (CIMC) Protection Profile authored by the National Institute for Standards and Technology (NIST) and provides all the necessary information for the Common Criteria Testing Laboratory, to perform their evaluation of the RSA Certificate Manager Version 6.7.

The RSA Certificate Manager Version 6.7 (hereafter referred to as the "Certificate Manager" or "TOE") ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the Certificate Manager meets in order to mitigate the defined threats:

- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE
- Security Environment (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- TOE Environment IT Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) met by the TOE Environment
- TOE IT Security Requirements (Section 6) – Presents the Security Functional Requirements (SFRs) met by the TOE
- Assurance Requirements (Section 7) – Presents the Security Assurance Requirements (SARs) met by the TOE
- TOE Summary Specification (Section 8) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives
- Protection Profile Claims (Section 9) – Presents the rationale concerning compliance of the ST with the CIMC PP.
- ST Rational (Section 10) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

1.2.2 Common Criteria Conformance Claims

The Certificate Manager conforms to the Certificate Issuing and Management Components (CIMC) Security Level 3 (SL3) protection profile. The TOE meets all the SL3 Functional and Assurance Requirements. Additionally, RSA has elected to pursue a more rigorous Assurance evaluation and the TOE additionally conforms to all the Assurance Requirements for an EAL4 product. The resulting assurance level is therefore CIMC SL3 with an overall EAL4, augmented with the CIMC PP SL3 Assurance Requirement: ALC_FLR.2. The Assurance and other Common Criteria required documentation, specifically this ST, conform to the Common Criteria for Information Technology Security Evaluation, Version 2.3 part 2 extended, and to part 3.

1.2.3 Conventions

There are several font variations within this ST. The table below provides an explanation of the font conventions used to show operations, as defined by the Common Criteria standard, performed on the requirements.

Operations

The Common Criteria standard defines four basic operations that can be performed on requirements to further clarify and define them: Assignment, Selection, Iteration, and Refinement. The Assignment operation allows PP and ST authors to specify requirement. The Selection operation allows the authors to make a selection of one or many from a list provided in the requirement. The Iteration operation allows the authors to reuse a base requirement to perform a different operation on it. The Refinement operation allows authors to add additional text to further clarify or define the requirement. The Protection Profile authors did not represent each type of operation separately. This ST mimics the Protection Profile and represents all operations performed in the PP with one type of formatting.

Assignment	*Requirement text will appear in Italics and underlined*
Iteration	Requirements text will be followed by the words iteration # in parenthesizes (Ex. FMT_MOF.1.1 (iteration 1))
Selection	**Requirement text will appear in bold and underlined**
Refinement	***Requirement text will appear in bold italics***
PP Operations	*[Requirement text will appear in italics in brackets]*

Roles

The CIMC PP defines four specific roles: Administrator, Officer, Auditor, and Operator. This Security Target uses only three of those CIMC PP defined Roles (Administrator, Officer, and Auditor) and the generic term “user” to refer to any of the CIMC PP Roles and/or the end-entities using the Certificate Manager. It should also be noted that the Administrator Guidance, Installation Guidance, and the Design documentation will refer to the “Officer” role using the traditional RSA terminology of “Vettor”.

2.0 TOE Description

This section will provide a general overview of the Certificate Manager, in order to provide an understanding of how this TOE functions and to aid customers in determining whether this TOE meets their needs.

2.1 RSA Certificate Manager Version 6.7

The Target of Evaluation for this evaluation is comprised of several components functioning together to provide certificate issuing and management services: a Web Front End, a PKI Server, a set of Command Line Tools, and a Log Server. The components that comprise this TOE are referred to collectively as the RSA Certificate Manager. The TOE is a digital certificate management system. The TOE provides: strong authentication, data confidentiality, integrity and non-repudiation. The RSA Certificate Manager offers services to publish to lightweight directory access protocol (LDAP)-compliant directories. The RSA Certificate Manager comes equipped to handle cryptographic hardware tokens.

The RSA Certificate Manager is a signing authority solution for large enterprises and public CAs. RSA Certificate Manager is responsible for creating and issuing both authority and end-entity public-key certificates and creating and issuing Certification Revocation Lists (CRLs). In addition to the basic CA functionality, RSA Certificate Manager provides:

- Audit recording and backup capabilities
- Use of a FIPS 140-1 or FIPS 140-2 Level 3 cryptographic module to protect all private keys and additionally for key generation.

The RSA Certificate Manager is designed to meet the CIMC Security Level 3 requirements, which are appropriate where the risks and consequences of data disclosure and loss of data integrity are moderate. A CIMC meeting Security Level 3 includes mechanisms to protect against attacks by parties with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

At the basic level the RSA Certificate Manager consists of a single Sun Solaris machine running Solaris 9, several servers, and some other supporting software modules as depicted in **Figure 1 – Physical Embodiment**

2.2 TOE Boundary

The TOE boundary includes multiple components that make up the RSA Certificate Manager and are relied on for the correct enforcement of the TSP. The TOE boundary is indicated in **Figure 2 – TOE Boundary** by the darker shaded area. As the TOE is not a hardware product the physical boundary is not easily represented. The boundary of the TOE should be drawn to encompass all RSA-provided Certificate Manager software, the configuration files associated with the CA component of the TOE, the audit files that are created by the CA component, the Log Server executable, and Database Backup Signing Tool executable. At the perimeter of the TOE Boundary are sub-components of the TOE that interact with non-TOE components. The Web Front End User Interface via web browser provides the users of the system access to configure and operate the TOE.

Additionally the Web Front End interacts with a Hardware Security Module (HSM) for cryptographic services provided by the HSM. The Log Server, the PKI Server, and the Command Line Tools also interface with the HSM for cryptographic services. Additionally, as all these programs are running on an Operating System, at a detailed level all software programs in the TOE are interfacing with the Operating System for low level calls.

2.2.1 Web Front End

The Web Based User Interface (WebUI) is the primary user interface available to manage the PKI Server (Administrator Console). The WebUI also provides a means to connect for certificate enrollment. The WebUI authenticates itself to the PKI Server using a certificate issued by the PKI Server's trusted CA System and communicates with the PKI Server over a secure Transport Layer Security (TLS) channel.

All incoming connections from administrators to the WebUI are over mutually authenticated HTTPS using TLS. Therefore all end-entities that connect to the WebUI authenticate to the WebUI using a digital certificate issued by the CA System. The WebUI then applies access control governing access to different functions displayed at the WebUI, based on the presented digital certificate. These access control rules are stored in the PKI Server, and the WebUI communicates to the PKI Server to evaluate each and every access from the mutually authenticated HTTPS clients. All security-relevant operations invoked from the WebUI are logged securely to the Secure Log Server. Other operations are logged to the webserver log stored in the IT Environment.

The WebUI stores both of its TLS authentication keys (the TLS LDAP client key, and the HTTPS server key) in a secure FIPS 140-1 or FIPS 140-2 Level 3 validated HSM. The HSM is relied upon for all security-relevant cryptographic operations.

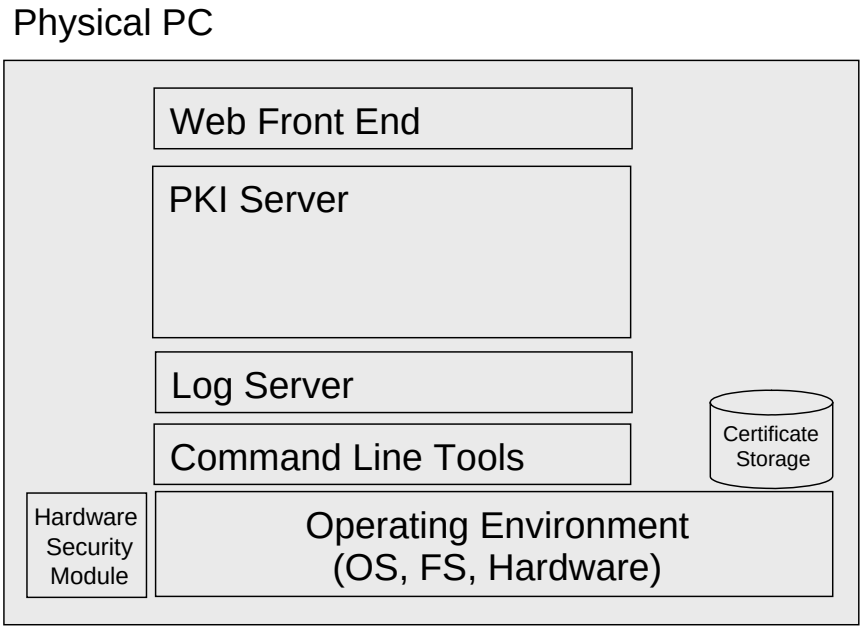

Figure 1 – Physical Embodiment

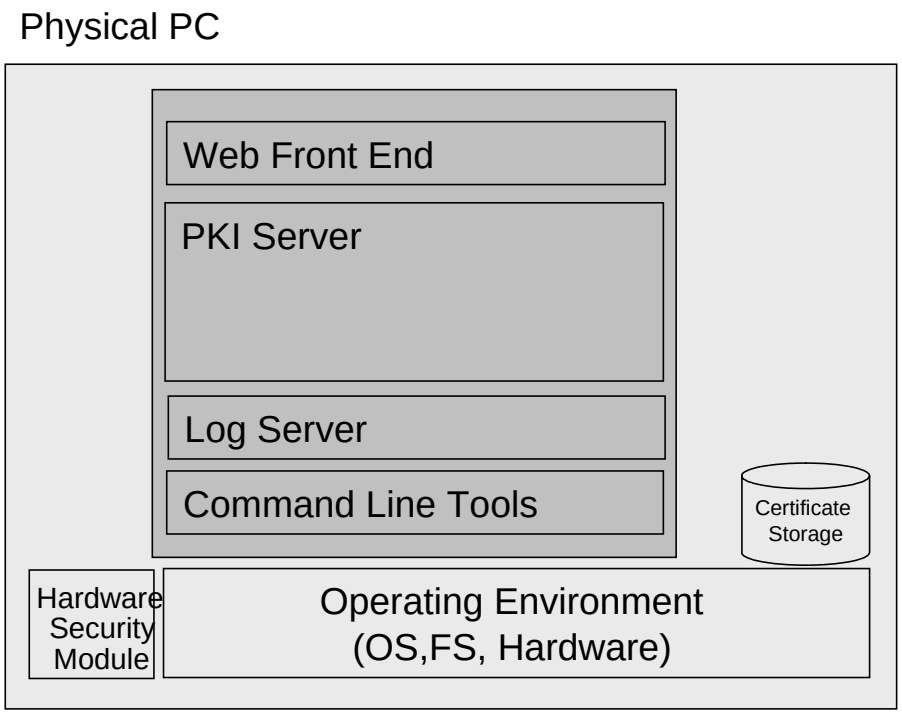

Figure 2 – TOE Boundary

2.2.2 PKI Server

The PKI Server (a separate process named “xudad” in some of the Design Documentation) is a complex server built on a highly modified LDAP directory server. Any applications communicating with the PKI Server can invoke backend services using structured LDAP commands; these services are described in more detail in the following subsections.

Access to the server is controlled through the use of the Transport Layer Security (TLS) protocol. In standard installations, the PKI Server communicates with two additional installed processes which are also part of the TOE: the Web-based user interface, and the secure log server. The interface between the web based user interface and the PKI Server is LDAP secured over mutually authenticated TLS. There is no provision for a non-secured communications interface. Additional user interfaces (such as an enrollment console) or authorities (such as a Registration Authority) can securely connect to the PKI Server through a similar mechanism, LDAP over mutually authenticated TLS, but using their own, distinct authentication keys. The PKI Server applies access controls based on the authentication keys used by any connecting applications (including the Web-based user interface).

The LDAP server contains added capability called “backends” which are additional services offered over the native database access layer. While the term “backends” refers to distinct code modules, the logic of the system is more clearly apparent when speaking in terms of backend services. There are many different types of backend services and they are unrelated to standard LDAP database operations. The Backend Services are invoked by structured queries over the mutually authenticated TLS LDAP interface. The following services are described below:

- Signing Engine
- Secure Time

Signing Engine

The Signing Engine is the cryptographic core of the PKI Server and provides the primary means through which hardware security modules (HSM) are accessed by the PKI Server. The Signing Engine makes use of a subsystem, the Keon Cryptographic Service Provider (KCSP), which provides the Signing Engine with a generic interface to the hardware cryptographic modules in a manner transparent to the PKI Server. Public key cryptography and related activities are handled by an HSM. The KCSP uses the standardized nCipher API for communication with the HSM. The HSM is relied upon for all security-relevant cryptographic operations.

Certificate Publishing is a subcomponent of the Signing Engine. Publishing certificates and certificate revocation lists (CRLs) to external LDAP directories is a common way of making these public artifacts available to external entities. Trust in certificates and CRLs is enabled through the use of internal digital signatures and does not require a secure connection to be established. Publishing is an outbound-only operation.

Secure Time
PKI systems rely on an accurate representation of the current time in order to determine the validity of certificates. The PKI server publishes its notion of the current time through an authenticated TLS-LDAP interface, serviced by the Secure Time backend. The other components of the TOE rely on this backend for time values used in their own certificate processing. (The Secure Time backend simply reports the system time of the PKI Server's host. Synchronizing the PKI Server's host system time to some globally agreed time value is left to the IT Environment.)

2.2.3 Log Server

The Log Server records security-relevant events for the components of the TOE. Event Data is stored in a signed log file that can be verified and exported in XML. Both the Web Front End and the PKI Server contain a logging client which provides event information to the Log Server to record. The Log Server leverages the FIPS-validated HSM to sign the audit logs using a specifically designated private key. This key designation is performed by the Administrator of the CA System.

2.2.4 Command Line Tools

The Command Line Tools are a set of utilities that provide additional security functionality to the TOE, and which may be executed from the Solaris command line by an Administrator with an appropriate login account to the operating system of the computer hosting RMC. There are 3 types of command line tools, as outlined below.

Data Integrity Monitor
The Data Integrity Monitor is a separate program executed from the IT Environment. The Data Integrity Monitor leverages the FIPS 140-1 or FIPS 140-2 Level 3 HSM to sign the database backup files. The tool allows a user to verify that the database backup files have not been altered since they were generated. This is achieved by hashing the database backup files and signing those hashes in a “signature file” with the System CA’s signing private key. The tool extracts the information from the signature file, rehashes the files and verifies the signature to determine that they are unaltered. The user must simply verify that the certificate of the signer is the same as the certificate designated to sign backups.

Audit Logfile Verification Tool
The Audit Logfile Verification Tool can verify the integrity of the files containing RCM’s audit trail. It does this by detecting any missing (or added, transposed or otherwise moved) signed log blocks by verifying the block signature on all signed blocks, verifying the identity of the filename and filenumber pair across all blocks, and the continuity of the record number within blocks and across block boundaries. It notifies the Auditor of any modification to the audit log files.

CA Copy Tools
The CA Copy Tools permit an Administrator to create either a Certificate Authority (CA), or just the Jurisdiction of a CA, on one instance of RCM and copy it securely to a second instance of RCM. Data transfers between instances are protected using mutually authenticated TLS connections. Note that the CA Copy Tools (cacopy and certprofcopy)

were not specifically evaluated under this Common Criteria evaluation. They play no role in meeting any of the Security Functional Requirements imposed by the CIMC PP, nor any of the additional SFRs claimed in this ST. For this reason they were not specifically tested by the CCTL evaluation team, although they are part of the product package delivery.

2.3 Non-TOE Boundary

The components excluded from the TOE boundary are the hardware and operating system platform (Abstract Machine).

2.3.1 IT Environment

The CIMC PP levies requirements on the TOE as well as the IT Environment. In the case of this TOE the IT Environment is the Operating System on which the software is running. The TOE relies on configuration files and audit capabilities which are protected by the Operating System (IT Environment). The IT Environment provides an interface to configuration files used to control and configure the TOE's functionality. The IT Environment provides TLS facilities leveraged by the TOE to secure the communications between internal and external components of the TOE. The IT Environment defines three roles to control access to the system: Administrator, Officer, and Auditor.

Operating System

The TSP is enforced by the TOE, and the Security Functional Requirements (SFRs) are completely satisfied by TOE functions (with the exception of those with environmental dependencies). The RSA Certificate Manager runs on Sun Solaris 9. The operating system with which the TOE interfaces is assumed to be trusted, meaning it can be relied upon to correctly execute the TOE functions. Sun Solaris 9 has received Common Criteria EAL4 validation.

2.3.2 Hardware Security Module

A hardware security module, HSM, is part of the TOE IT Environment. The RSA Certificate Manager relies on the nCipher nShield or NetHSM to provide all FIPS 140-1 or FIPS 140-2 approved cryptography and key management. The HSM is installed in the physical machine on which the RSA Certificate Manager is installed. Many of the TOE components rely on the HSM to provide all the security-relevant cryptographic services necessary for the TOE to perform its functions.

2.3.3 Hardware Platform

The RSA Certificate Manager software for Sun Solaris 9 does not depend on a particular hardware configuration. It will run on any Sun server (or higher end workstation) running Solaris 9 and having a processor in the UltraSPARC or SPARC64-V families that meets the following minimum system requirements:

- Server: Sun Enterprise Ultra 10S; Workstation: Sun Ultra 60
- At least 300 MB of memory (RAM)
- Minimum free hard disk space of at least 100 MB free for basic program installation. Additional space would be needed for the storage of certificates.

2.4 TOE Security Services

This section lists and describes, at a high level, the security services that are provided by the TOE. Each of these service areas is further defined and mapped to requirements in Section 8.0 - TOE Summary Specifications.

- Secure Audit Log Server
- Access Control
- Backup and Recovery
- Secure Import/Export
- Cryptographic Support and Key Management
- Certificate Management
- Identification and Authentication

- Secure Audit Log Server - The TOE collects audit data for internal user actions, provides the ability to review audit logs, and restricts access to the audit logs. The TOE tracks any actions taken to a certificate (creation, revocation, deletion), authentication attempts, changes to user's roles and access.

- Access Control - The TOE enforces user roles and access control whenever users access TOE-provided functions. To enforce its security policy, the TOE relies on the roles set per user and the access control list set per function. Both roles and access control lists are set by the Administrator. Access Control is primarily enforced by restricting the options presented to users on the Web management interface. The user's certificate is verified during the initial establishment of the TLS connection to the Web server from a browser. Access to TOE resources are controlled by the access control list (ACL) for each directory structure and Web page.

- Backup and Recovery – The TOE provides configurable backup functionality, as well as system recovery features, to allow the operators to restore the CA System and maintain the storage of logs and current certificates stored.

- Import/Export of Data – The TOE is responsible for importing and exporting certificates, public keys, certificate status, and other data. The TOE protects these data transfers through a trusted path using the TLS protocol.

- Key Management – The TOE provides access to the hardware security module (HSM). The TOE relies on the HSM in the IT Environment for key generation,

signing and encryption, and key destruction through zeroization. The HSM, the nCipher nShield or the NetHSM - is a FIPS 140-1 or FIPS 140-2 validated module as mandated by the CIMC PP requirements. No private or secret keys are stored in the TOE; the TOE accesses the HSM to perform operations with the keys stored on the HSM.

- Certificate Management – The TOE manages and securely stores all certificates that have been signed using the private key of any of the internal CAs. The TOE provides functionality to issue, suspend, reinstate, reissue, renew, revoke and delete certificates, report status of certificates, and generate CRLs. All these certificate services are provided in a secure manner, protecting the integrity of the certificate administrative data. Additionally, the TOE enforces proof of origin and verification of origin of certificate status information at all times.

- Identification and Authentication – The TOE requires identification and authentication before performing any security-relevant functions. CIMC maintains a secure database of authorized operators of the TOE, including all certificate information and roles that can be assumed. Users of the TOE are authenticated during the establishment of the mutually authenticated TLS connection.

2.5 Features Excluded From CC Evaluation

A number of functions of the RSA Certificate Manager that are identified in the *Administrator's Guide* or other customer documentation have intentionally been excluded from the scope of the Common Criteria evaluation. Most commonly, this is because:

- Use of the function or feature is incompatible with the SFRs of the CIMC PP, or
- The function or feature is an add-on (typically a subsystem) of limited general usefulness, and evaluation would require considerable additional effort not justified by commercial considerations.

Those functions or features are listed here, along with a rationale for exclusion. This helps customers to understand what features are not covered by the CC evaluation, and clarifies that these features have not simply been omitted from the *Functional Specification* and other documentation by inadvertence. The list of excluded features will be found in Section 11.0, *Annex 1: Evaluation Restrictions*.

3.0 TOE Security Environment

This section details the security environment for the TOE:

- Secure usage assumptions
- Threats
- Organizational security policies.

This information provides the basis for the Security Objectives, the Security Requirements for the IT Environment, and the TOE Security Functional Requirements. The TOE Security Environment described below is taken directly from the CIMC PP.

3.1 Secure Usage Assumptions

The usage assumptions are organized in three categories: personnel, connectivity, and physical.

3.1.1 Personnel

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

A.CPS
All Administrators, Operators, 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, Operators, 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, operators, 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 appropriate Security Level identified in this family of PPs.

3.1.3 Physical

A.Communications Protection
The system is adequately physically protected against loss of communications i.e., availability of communications.

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

3.2 Threats

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

3.2.1 Authorized Users

T.Administrative errors of omission
Administrators, Operators, 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, Operators, Officers and Auditors commit errors or hostile actions
An Administrator, Operator, 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 Organizational Security Policies

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

P.Cryptography
FIPS-approved or NIST-recommended cryptographic functions shall be implemented.

4.0 Security Objectives

This section includes the security objectives for the TOE and for the TOE Environment, including IT TOE security objectives, non-IT security objectives, non-TOE IT security objectives and objectives which for the both the TOE and IT Environment. The Security Objectives described below is taken directly from the CIMC PP.

4.1 Security Objectives for the TOE

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

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 External Attacks

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

4.1.4 Cryptography

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

4.2 Security Objectives for the TOE Environment

4.2.1 Non-IT security objectives for the TOE Environment

O.Administrators, Operators, Officers and Auditors guidance documentation
Deter Administrator, Operator, 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 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, Operators, Officers and Auditors
Provide capable management of the TOE by assigning competent Administrators, Operators, Officers and Auditors to manage the TOE and the security of the information it contains.

O.CPS
All Administrators, Operators, 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, Operators, 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.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.)

O.Operating System
The operating system used is validated to provide adequate security, including domain separation and non-bypassability, 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

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, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and 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.

5.0 TOE Environment IT Security Requirements

This section specifies the Security Functional Requirements (SFRs) v2.3 for the TOE Environment. All the requirements are from the CIMC Protection Profile (Security Level 3) and all operations that were left to the Security Target have been completed. There are several explicitly stated requirements defined by the PP authors; these can all be recognized by the present "CIMC" in the requirement's name. This section organizes the SFRs by CC class. These requirements are provided as guidance to CIMC PP (updated with CCv2.3) implementers and do not apply directly to the TOE; however, they do detail the environment in which the TOE is to be implemented.

Table 1 – Functional Requirements for the TOE Environment

Functional Requirements	ST Operations
FAU_GEN.1 Audit data generation (iteration 1)	None
FAU_GEN.2 User identity association (iteration 1)	None
FAU_SAR.1 Audit Review	None
FAU_SAR.3 Selectable audit review	None
FAU_SEL.1 Selective audit (iteration 1)	Selection/Assignment
FAU_STG.1 Protected audit trail storage (iteration 1)	None
FAU_STG.4 Prevention of audit data loss (iteration 1)	None
FCS_CKM.1 Cryptographic key generation	Assignment
FCS_CKM.4 Cryptographic key destruction	Assignment
FCS_COP.1 Cryptographic operation	Assignment
FDP_ACC.1 Subset access control (iteration 1)	Assignment
FDP_ACF.1 Security attribute based access control (iteration 1)	Assignment
FDP_ITT.1 Basic internal transfer protection (iterations 1 and 2)	None
FDP_UCT.1 Basic data exchange confidentiality (iteration 1)	None
FIA_AFL.1 Authentication failure handling	Assignment
FIA_ATD.1 User attribute definition	Assignment
FIA_UAU.1 Timing of authentication (iteration 1)	Assignment
FIA_UID.1 Timing of identification (iteration 1)	Assignment
FIA_USB.1 User-subject binding (iteration 1)	None
FMT_MOF.1 Management of security functions behavior (iteration 1)	None
FMT_MSA.1 Management of security attributes	Assignment
FMT_MSA.2 Secure security attributes	None
FMT_MSA.3 Static attribute initialization	Selection
FMT_MTD.1 Management of TSF data	None

FMT_SMR.2 Restrictions on security roles	None
FPT_AMT.1 Abstract machine testing	Selection
FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 1)	None
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 1 and 2)	None
FPT_RVM.1 Non-bypassability of the TSP (iteration 1)	None
FPT_SEP.1 TSF domain separation	None
FPT_STM.1 Reliable time stamps (iteration 1)	None
FPT_TST_CIMC.2 Software/firmware integrity test	Assignment
FPT_TST_CIMC.3 Software/firmware load test	Assignment
FTP_TRP.1 Trusted path	Selection/Assignment

The following sections present the TOE Security Functional Requirements (SFRs) with any ST operations performed on them based on the requirements from the CIMC PP.

5.1 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 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 ***(if applicable)***, 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 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 2 - Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
5.1: 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.	
5.4: Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a roles	

	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		The access control privileges of a user account or a role are modified Roles and users are added or Deleted	

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 3 below.]*

Dependencies: FAU_SAR.1 Audit review

Table 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) *Success or Failure of the event to be logged*

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]* unauthorized modifications to the stored audit records in the audit trail.

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.

5.2 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*].
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 the conditions:

[*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] are satisfied.

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: 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 4*] to *[the authorized roles as specified in Table 4.]*

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

Table 4 - Authorized Roles for Management of Security Functions Behavior

Section/Function	Function/Authorized Role
5.1: Security Audit	The capability to configure the audit parameters shall be restricted to Administrators.
5.4: 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 10.1]* ***of the CIMC PP*** to restrict the ability to [*modify*] the security attributes *Role attributes for users , Access Control attributes for objects* to [*Administrators*].

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

FMT_MSA.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 10.1*] ***of the CIMC PP*** 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_SMF.1 Specification of Management Functions

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

5.3 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 10.1*] ***of the CIMC PP*** on *all subjects, objects and operations defined in Table 5.*

Table 5 - Access Control Elements

Elements	
Subject	User context processes associated with each user
Object	Files or directories containing user interface web pages
Operations	Open web page and utilize web page functionality.

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 10.1*] ***of the CIMC PP*** to objects based on the following [*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*s 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, Officers, and* Operators.]

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 explicit denial 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

5.4 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*] *and a group identifier and file permissions.*

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 *only the request for login to the IT Environment* 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 *request for login to the IT Environment* 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 *following* user security attributes with subjects acting on behalf of that user: *User Identity and User Role.*

FIA_USB.1.2 The ***IT environment*** shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

1. *Subsequent to a successful login by a user, the IT environment will assign the user's login name from the user's system account to be the User Identity associated with subjects acting on behalf of the user.*
2. *Subsequent to a successful login by a user, the IT environment will assign the user's principal group to be the User Role associated with subjects acting on behalf of the user*.

FIA_USB.1.3 The ***IT environment*** shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

1. *Authorized Administrators can change the User Identity, associated with a subject acting on behalf of that user, that is assigned to any user by changing the user's login name.*
2. *Subjects acting on behalf of a user shall be able to change associated User Identity*

autonomously, based on internally programmed setuid system calls.

3. *Authorized Administrators can change the User Role, associated with a subject acting on behalf of that user, by changing the user's principal group.*
4. *An Administrator shall not assign more than one User Role to any user at a given time.*

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 authorized administrator configurable integer]*** unsuccessful authentication attempts occur related to *[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 [*log the authentication failures and terminate the connection*].

Dependencies: FIA_UAU.1

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 **local 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 **the TSF, local users, and 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 all communications with the WebUI.*

Dependencies: No dependencies

5.5 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 10.1*] ***of the CIMC PP*** 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 10.1**of the CIMC PP]*** 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 10.1 **of the CIMC PP]*** 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

5.6 Key Management

5.6.1 Key Generation

This subsection specifies the requirements for the generation of cryptographic keys by the IT environment.

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

FCS_CKM.1.1 The [*FIPS 140-1 validated cryptographic module*] shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES, DES, TDES, DSS, and SHA-1 Algorithms and specified cryptographic key sizes DES & TDES – 56-bits & 168-bits; DSA – 1024 bits; RSA – 2048 bits; ECDSA – 384 bits* that meet the following *FIPS 197 for AES, FIPS 46-3 for DES and TDES, FIPS 186-2 for DSA and RSA, and FIPS 180-2 for SHA-1*.

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

5.6.2 Private and Secret Key Destruction
This section specifies requirements for the zeroization/destruction of plaintext private and secret keys stored within the IT environment.

FCS_CKM.4 Cryptographic key destruction
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 Publication 140-1.*

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

5.7 Self-tests
The IT environment shall implement the following 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 *on-demand*** 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 *log the test failure.*

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 *enter an error state and not execute any software or firmware which has failed this test.*

Dependencies: FPT_AMT.1 Abstract Machine Testing

5.8 Cryptographic Modules

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The *[FIPS 140-1 validated cryptographic module]* shall perform *encryption, decryption, random number generation, signature generation, signature verification, hash generation, hash verification, keyed-hash message, and authentication code generation* in accordance with a specified cryptographic algorithm [:

- DES & TDES
- DSA, RSA signatures, & ECDSA 2
- SHA-1, SHA-256, SHA-384, SHA-512]

and a cryptographic key sizes *[DES & TDES – 56-bits & 168-bits; DSA – 1024 bits; RSA – 2048 bits; and ECDSA -384 bits]* that meet the following: *[DES & TDES - FIPS 46-3; DSA, RSA signatures, & ECDSA – FIPS 186-2; and SHA-1, SHA-256, SHA-384, SHA-512 – FIPS 180-2]*

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

6.0 TOE IT Security Requirements

This section specifies the Security Functional Requirements (SFRs) v2.3 for the TOE. All the requirements are from the CIMC Protection Profile (Security Level 3) with updates from the CCv2.3, and all operations that were left to the Security Target have been completed. There are several explicitly stated requirements defined by the PP authors;

these can all be recognized by the presence of “CIMC” in the requirements name. This section organizes the SFRs by CC class.

Table 6 - Functional Requirements for TOE

Functional Requirements	***ST Operations***
FAU_GEN.1 Audit data generation (iteration 2)	None
FAU_GEN.2 User identity association (iteration 2)	None
FAU_SEL.1 Selective audit (iteration 2)	Selection/Assignment
FAU_STG.1 Protected audit trail storage (iteration 2)	None
FAU_STG.4 Prevention of audit data loss (iteration 2)	None
FCO_NRO_CIMC.3 Enforced proof of origin and verification of Origin	Assignment
FCO_NRO_CIMC.4 Advanced verification of origin	None
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	None
FDP_ACC.1 Subset access control (iteration 2)	Assignment
FDP_ACF.1 Security attribute based access control (iteration 2)	Assignment
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	None
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	None
FDP_CIMC_CER.1 Certificate Generation	Assignment
FDP_CIMC_CRL.1 Certificate Revocation	None
FDP_CIMC_CSE.1 Certificate Statue Export	Assignment
FDP_CIMC_OCSP.1 Basic Response Validation	None
FDP_ETC_CIMC.5 Extended user private and secret key export	None
FDP_ITT.1 Basic internal transfer protection (iterations 3 and 4)	None
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	Assignment
FDP_UCT.1 Basic data exchange confidentiality (iteration 2)	None
FIA_UAU.1 Timing of authentication (iteration 2)	Assignment
FIA_UID.1 Timing of identification (iteration 2)	Assignment
FIA_USB.1 User-subject binding (iteration 2)	None
FMT_MOF.1 Management of security functions behavior (iteration 2)	Assignment
FMT_MOF_CIMC.3 Extended certificate profile management	None
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	None
FMT_MOF_CIMC.6 OCSP Profile Management	None
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None
FMT_MTD_CIMC.7 Extended TSF private and secret key export	None
FPT_CIMC_TSP.1 Audit log signing event	None
FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 2)	None
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 3 and 4)	None

FPT_RVM.1 Non-bypassability of the TSP (iteration 2)	None
FPT_STM.1 Reliable time stamps (iteration 2)	None

6.1 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 7 below.*]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity ***(if applicable)***, and the outcome (success or failure) of the event; and
b) For each audit event type, [*the information specified in the Additional Details column in Table 7 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 7 - Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
6.1: 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	
5.6.1: Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the TSF requests generation of a cryptographic key. (Not	The public component of any asymmetric key pair generated

		mandatory for single session or one-time use symmetric keys.)	
Private Key Load		The loading of Component private keys	
6.7.1: 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.
6.7.3: Secret Key Storage		The manual entry of secret keys used for authentication	
6.7.5: 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)	
6.11: Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
Certificate Status Change Approval		All requests to change the status of a certificate	Whether the request was Accepted or rejected.
CIMC Configuration		Any security-relevant changes to the configuration of the TSF.	
6.8: 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
6.9: 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
6.10: Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP Profile Management	All changes to the OCSP profile	The changes made to the Profile

FAU_GEN.2 User identity association (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**
b) *Success or Failure of the event to be logged.*

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*] unauthorized modifications to the audit records in the audit trail.

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: FAU_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 functions behavior

6.2 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 8]* to *[the authorized roles as specified in Table 8.*]

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

Table 8 - Authorized Roles for Management of Security Functions Behavior

Section/Function	Component Function	Authorized Role
6.1: 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.
6.3: 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 *Administrators*.
6.11: Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers. If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Officers.
Data Export and		The export of CIMC private keys shall

Output		require the authorization of at least two Administrators or one Administrator and one Officer, Auditor, or Operators.
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.)
6.8: 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.
6.9: Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.
6.10: Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.

6.3 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

6.4 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 10.2*] **of the CIMC PP** on *all subjects, objects and operations defined in Table 9 - Access Control Elements.*[1]

Table 9 - Access Control Elements

Elements	
Subject	User context processes associated with each user
Object	Files or directories containing user interface web pages
Operations	Open web page and utilize web page functionality.

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACF.1 Security attribute based access control (iteration 2)

[1] It should be noted that the TOE controls user access to functions by restricting access to view web pages that present the functionality to the users. Therefore by controlling access to view or access the web page files the users are limited to the functions they are authorized to perform.

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [*CIMC TOE Access Control Policy specified in section 10.2*] ***of the CIMC PP*** to objects based on the following: [*the identity of the subject, and the set of roles that the subject is authorized to assume*.]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*specified in Table 10 - Access Controls*]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *no additional rules.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *no additional explicit denial rules.*

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

Table 10 - Access Controls

Section/Function	Component	Event
Certificate Request Remote and Local Data Entry		The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry		The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked.
Data Export and Output		The export or output of confidential and security-relevant data shall only be at the request of authorized users.
5.6.1: 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.
6.7.1: Private Key Storage		The capability to decrypt certificate subject private keys within a CIMC 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, Auditor, or Operator 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.
6.7.3: Secret Key Storage		The capability to request the loading of CIMC secret keys into cryptographic modules shall be restricted to Administrators.
6.7.4: Private and Secret Key Destruction		The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators, Auditors, Officers, and Operators.
6.7.5: 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, Auditor, or Operators.
Certificate Status Change Approval		Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold. Only Officers shall be capable of removing a

		certificate from on hold status. Only Officers shall be capable of approving the placing of a certificate on hold. Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate. Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

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

6.5 Identification and Authentication

FIA_UAU.1 Timing of authentication (iteration 2)

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow *request for enrollment, request for public certificate and request for CRL* 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 *request for enrollment, request for public certificate and request for CRL* 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_USB.1 User-subject binding (iteration 2)

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the *following* user security attributes with subjects acting on behalf of that user: *User Identity and User Role.*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

1. The TSF determines the User Identity and User Role from the digital certificate presented by the user for authentication.
2. Every subject (user session) is associated with the User Identity and User Role of the user on whose behalf the subject will act.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

Once a user's session is established, the security attributes associated with a subject acting on behalf of a user cannot be changed for the duration of that user's session.

Dependencies: FIA_ATD.1 User attribute definition

6.6 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 *the identity of the originator's certificate issuer* 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 10.2*] ***of the CIMC PP*** 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 10.2*] ***of the CIMC PP*** 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 10.2*] ***of the CIMC PP*** 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

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

6.7 Key Management

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 not start or not allow a TLS connection to be made to the TOE.*

Dependencies: No dependencies.

ST Rational: The TOE stores all Public keys within digitally signed certificates. When the TSF starts up, it accesses the CA System public key and verifies the public key with a challenge from the CA System private key. If the CA System public key verification fails, the TSF will log the error and not start up. The client digital signatures are verified when the client's certificate is checked during the authentication process of establishing an TLS connection to the CA. If a client signature fails the TLS connection will not be established and an entry is made on the log server.

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_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

6.8 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

6.9 Certificate Revocation List Profile Management

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: FMT_MOF_CIMC.4

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

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

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

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

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

6.10 Online Certificate Status Protocol (OCSP) Profile Management

FMT_MOF_CIMC.6 OCSP profile management

Hierarchical to: No other components.

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

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

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

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

Note that the RCM TOE does not issue OCSP responses.

6.11 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.

6.12 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:

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

Dependencies: No dependencies

FDP_CIMC_OCSP.1 OCSP basic response validation

Hierarchical to: No other components.

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

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

Dependencies: No dependencies

Note that the RCM TOE does not issue OCSP responses.

7.0 Assurance Requirements

This section specifies the Security Assurance Requirements (SAR) v2.3 for the TOE. The table below provides a complete listing of the Assurance Requirements for the TOE, at EAL 4 augmented. All of the SAR specified in the CIMC Protection Profile for Security Level 3 are met, additionally all the SAR specified in EAL 4 are met. This section organizes the Assurance Requirements by CC class.

Table 11 - Assurance Requirements

Assurance Class	Component ID	Component Title	EAL Level
Configuration Management	ACM_AUT.1	Partial CM automation	EAL4
	ACM_CAP.4	Generation support and acceptance procedures	EAL4
	ACM_SCP.2	Problem tracking CM coverage	EAL4
Delivery and Operation	ADO_DEL.2	Detection of modification	EAL4
	ADO_IGS.1	Installation, generation, and start-up procedures	EAL4
Development	ADV_FSP.2	Fully defined external interfaces	EAL4
	ADV_HLD.2	Security enforcing high-level design	EAL4
	ADV_IMP.1	Subset of the implementation of the TSF	EAL4
	ADV_LLD.1	Descriptive low-level design	EAL4
	ADV_RCR.1	Informal correspondence demonstration	EAL4
	ADV_SPM.1	Informal TOE security policy model	EAL4
Guidance Documents	AGD_ADM.1	Administrator guidance	EAL4
	AGD_USR.1	User guidance	EAL4
Life Cycle Support	ALC_DVS.1	Identification of security measures	EAL4
	ALC_LCD.1	Developer defined life cycle model	EAL4
	ALC_FLR.2	Flaw reporting procedures	None
	ALC_TAT.1	Well-defined development tools	EAL4
Tests	ATE_COV.2	Analysis of coverage	EAL4
	ATE_DPT.1	Testing: high-level design	EAL4
	ATE_FUN.1	Functional testing	EAL4
	ATE_IND.2	Independent testing – sample	EAL4
Vulnerability Assessment	AVA_MSU.2	Validation of analysis	EAL4
	AVA_SOF.1	Strength of TOE security function evaluation	EAL4
	AVA_VLA.2	Independent vulnerability analysis	EAL4

8.0 TOE Summary Specifications

This section provides a high-level definition of the IT Security Functions and the Assurance Measures provided by the TOE to met the SFRs and SARs specified in the Certificate Issuing and Management Components PP. A complete mapping is provided in Section 10.0 Rationale.

8.1 TOE Security Functions

The TOE provides the following Security Functions:

- Secure Audit Log Server
- Access Control
- Backup and Recovery
- Secure Import/Export
- Cryptographic Support and Key Management
- Certificate Management
- Identification and Authentication

8.1.1 Secure Audit Log Server

The RSA Certificate Manager collects audit data for internal actions and user actions. Additionally the Certificate Manager provides the ability to review audit logs and restrict access to the audit logs. The TOE tracks any actions taken to a certificate (creating, suspending, reinstating or revoking, or deletion), authentication attempts, changes to the user roles and access rights. The TOE includes a log server which handles the audit recording. The log server writes audit records to the audit trail for all events that are configured to be audited. The log records are encoded in XML (E**x**tensible **M**arkup **L**anguage) and the digital signature is taken across all records written since the previous signature was made. The digital signature is Base64-encoded and stored in an XML element associated with the group of signed records. In addition to the events logged by the Log Server, the IT Environment performs logging of authentication attempts.

SFR Mapping

The Secure Audit/Logging Service satisfies the following security functional requirements (SFRs):

- *FAU_GEN.1 (Iteration 2)* – The TOE logging services are capable of generating audit logs with the following event types:
    1. Key generation
    2. Sign an end-entity certificate
    3. Sign a CA certificate
    4. Download an end-entity certificate to a client
    5. Download a CA certificate to a client
    6. Download a Signer certificate to a client
    7. Generate a Revocation List
    8. Resign an end-entity certificate
    9. Create a CA
    10. Create an administrative certificate
    11. Update a CA certificate
    12. Create a Signer Certificate
    13. Sign a Signer Certificate

14. Reinstate a CA Certificate
15. Suspend a CA Certificate
16. Revoke a CA Certificate
17. Reinstate an end-entity Certificate
18. Suspend an end-entity Certificate
19. Revoke an end-entity certificate
20. Revoke a Signer Certificate
21. Sign a Reverse Cross-Certificate
22. Import a Forward Cross-Certificate
23. Revoke a Reverse Cross-Certificate
24. Suspend a Reverse Cross-Certificate
25. Reinstate a Reverse Cross-Certificate
26. Delete a Forward Cross-Certificate
27. Download a Reverse Cross-Certificate
28. Delete a Secure Log Server audit log
29. Copy the contents of a Secure Log Server audit log
30. Change the access role of an end-entity certificate
31. Modify a Web ACL
32. Modify an LDAP ACL
33. Apply Jurisdiction changes
34. Apply changes to Audit Parameters
35. Apply Certificate Profile changes
36. Receive a Certificate Request
37. Delete an end-entity certificate
38. Database full backup
39. Database incremental backup
40. Database transactional log file cleanup
41. Issue a Certificate Manager Server certificate
42. Change the status of a certificate request by a vettor or an administrator
43. Final Audit Entry
44. Log Server Started
45. Log Server Stopped
46. Certificate expiry notification

The TOE provides the capability to generate any number of audit log files which are stored on the Log Server. These files are stored in the LogServer/logs directory and the log files are named according with the following standard:

- Xslog-<date>[-<number>].xml for instance, xslog_20020405_1.xml.

Each audit record is stored in XML format and contains the following fields:

- Log Number
- Log Source – TOE component which produced the audit record
- Event condition (attempt, completion)
- Log Data – Text event description (type of event, success or failure, identity and other details)
- Log Date Stamp – Date of the event
- Log Time Stamp – Time of the event
- Log ID Element – MD5 hash of the log client's TLS entities certificate
- Log IP Address – IP address of log client

Table 7 - Auditable Events and Audit Data details the auditing events and audit data required by the CIMC PP. Each audit function is identified in the paragraphs below.

Security Audit – As indicated above in the complete auditing list, the TOE audits when an Auditor deletes a Secure Log Server audit log. Auditing selection settings are also audited via the WebUI on the Administration Workbench. Upon completing the setting changes, the new auditing selections are set and an audit record is written containing the identity of the Administrator and the time that the changes were made. The TOE does not create an event log entry for each log signing event because the log blocks (groupings of log entries) themselves contains the signature block. It would be redundant to create an additional audit record that recorded that the audit block was signed.

Local Data Entry / Remote Data Entry – The TOE audits the entry of security-relevant information, regardless if the WebUI is installed on a local machine or on a remote machine. The following audit events from the complete auditing list above capture the entry of security-relevant information:

- Sign a CA certificate
- Sign a Signer Certificate
- Sign a Reverse Cross-Certificate
- Modify a Web ACL
- Modify an LDAP ACL
- Apply changes to Audit Parameters
- Apply Jurisdiction changes
- Apply Certificate Profile changes

CIMC Configuration – These items from the complete list above are auditable events that capture the actions of an Administrator configuring the CIMC.

- Modify a Web ACL
- Modify an LDAP ACL
- Apply changes to Audit Parameters
- Apply Jurisdiction changes
- Apply Certificate Profile changes
- Log Server Started
- Log Server Stopped
- Change the access role of an end-entity certificate

Certificate Registration - As indicated above in the complete audit events list, the TOE logs when the TOE receives a certificate request from an end-entity. If the signature on the certificate request cannot be verified, the audit record shows an unsuccessful request. The certificate request is included in the audit log record.

Certificate Status Change Approval – As indicated above in the complete audit events list, the TOE logs when a vettor changes the status of an unprivileged end-entity certificate request, or an administrator changes the status of an administrative certificate request.

Certificate Profile Management - As indicated above in the complete audit events list, the TOE logs when an operator edits any property of an existing Certificate Profile and when an operator applies Certificate Profile changes.

There are several auditing events that are listed in Table 7 - Auditable Events and Audit Data which are not necessary for this TOE because the functionality being audited is not present in the TOE.

Data Export and Output – While the TOE does export or output certificates and certificate status information, it does not export any data that is directly security-relevant to the TOE.

Key Generation – Key generation and key maintenance is managed by the FIPS 140-1 or FIPS 140-2 level 3 validated HSM external to the TOE.

Private Key loading, Private Key Storage, Secret Key Storage, and Private and Secret Key Export - Private Key loading, Private Key Storage, Secret Key Storage, and Private and Secret Key Export are not audited because the TOE does not provide a means to perform these functions. All Public/Private keys are generated in a FIPS 140-1 or FIPS 140-2 Level 3 validated module. The manual entry of secret keys is not audited because all authentication and encryption is performed using the Public/Private key pair.

Revocation Profile Management - The TOE does not make use of Revocation Profiles; therefore, no auditing is associated with Revocation Profile Management.

CRL and OCSP Profile Management - The requirement for auditing changes to CRL profiles does not apply as CRL Profiles are defined in the underlying source code of the module and are not modifiable. The requirement for auditing changes to OCSP profiles also does not apply as the TOE does not implement an OCSP server.

There are several auditing requirements levied on the TOE by the FAU_GEN.1.1b requirement of a “minimum” level of auditing. A description of how the TOE handles each of these minimum auditing requirements is provided in the listing below.

- FAU_GEN.1 – Including in the TOE’s auditable events listed above are events for the Startup and Shutdown of the auditing capabilities.
    1. Log Server Started
    2. Log Server Stopped
    3. Final Audit Entry
- FAU_SEL.1 – Auditing selection settings are modified via the WebUI on the Administration Workbench). Upon completing the setting changes the Administrator clicks an on-screen button to accept the changes. At this time the new auditing selections are set and an audit record is

written containing the identity of the Administrator, the time that the changes were made, and a complete record of all the current audit selections.

- FDP_ACF.1 – All attempts to access items covered by the Security Functional Policy are audited. A complete lists of auditable events is provided in the numbered list under FAU_GEN.1 above.
- FDP_ITT.1 – All components of the TOE reside on a single computer, therefore there are no external transfers of user data which need to be audited.
- FDP_UCT.1 – As users perform actions to import or export any security-relevant data, these actions are captured by the auditing functions as defined in the FAU_GEN.1 and stored by the Log Server. The audit logs contain the identity of the user performing the action, the time of the action, and a record of the action.
- FIA_UAU – Identification and Authentication attempts are audited by the Webserver in the TOE. If a user is unsuccessful in authenticating to the TOE, the Webserver will record the identity of the user presenting a certificate during the TLS session establishment. The IT Environment provides the TLS library used by the TOE.
- FIA_UID – Identification and Authentication attempts are audited by the Webserver in the TOE. If a user is unsuccessful in authenticating to the TOE, the Webserver will record the identity of the user presenting a certificate during the TLS session establishment. The IT Environment provides the TLS library used by the TOE.
- FIA_USB.1 – When a user authenticates via TLS to the Web Front End, any services performed at the request of the Web Front End are bound to the user that initially requested the service. A binding would fail only if the user did not have the access privileges to perform the service, in which case the ACL failure would be logged to the audit records.
- FPT_STM.1 – The TOE itself does not provide a method for changing the clock time and therefore does not audit the changing of the system clock time.

- FAU_GEN.2 (Iteration 2) - The TOE associates each auditable event with the identity of the user that caused the event. The subject's identity is known upon authentication. The user identity is associated with the on-going TLS connection which is established during the user's interaction with the TOE. The TOE does this using the (MD5) hash of the user's identity certificate. The directory of certificate objects is indexed by this hash value, so that hash is a pointer to all the information that the system knows about that user. All requests made through

the established TLS session are associated with the user's identity certificate from that session. The user's identity information is recorded in all subsequent event records of that session.

- FAU_SEL.1 (Iteration 2)– The TOE's System Configuration Workbench, a webpage screen available from the Administrator console, enables selection of logging conditions [always, on success, on failure, or never] for each auditable event type listed under FAU_GEN.1 (Iteration 2). These setting are established during initial setup of the TOE and can be reconfigured by the Administrator during the normal operation of the TOE.
- FAU_STG.1 (Iteration 2)– Audit Records are protected from undetected modification by digital signatures performed by the Secure Log Server on blocks of the audit records. The Secure Log System provides an attribute and value in each digitally-signed signature block that will permit the Auditor to detect if any signature blocks have been added, deleted or moved. The attribute is the XML element <LOG_NUMBER> and the value is the filename followed by a colon followed by a monotonically increasing sequence number. The Secure Log Server also creates a final log record ("Final Entry") when a log file is being closed. The entry `log_number` follows the sequence numbering scheme and prevents any earlier records from being deleted (or added) without the auditor being able to detect that fact.
- FAU_STG.4 (Iteration 2)– All auditable events are written in a "two-phase" fashion. There are 2 different thresholds settings for remaining disk space; a smaller one for the completion log and a larger one for the attempt log. Prior to each event, an "attempt" message is logged, signifying that the system is about to perform the event. If the logging subsystem is able to record the "attempt" message, the event proceeds and a "completion" message is logged recording the outcome of the event. If the attempt message exceeded the configurable "Full" threshold, the logging server will return a warning that the audit log is full. Events initiated by an Auditor proceed regardless of the success or failure of the "attempt" message, but no other auditable events are permitted to occur. Thus, if the audit trail is full, non-Auditor events are prevented.
- FPT_STM.1 (Iteration 2) - The TOE relies on the system clock of the Log Server for a reliable time stamp. The log entries from both the PKI Server and the Webserver are time stamped when received by the Log Server. Using this central source for all time stamps ensures that the audit records are not receiving timing information for multiple sources which could potentially be out of sync. The time on the Log Server is set by the Administrator and access to the `set time` functionality is protected by the IT Environment Access Control on the Log Server.
- FPT_CIMC_TSP.1 –The TOE allows the Administrator to configure the frequency of the audit log signing by changing a parameter value in the logserver configuration file. After every event that is logged, the TOE checks to see if a digital signature should be performed on the last block of audit records.
- "Minimum" Audit Requirements – In addition to the specifically stated auditing described above, the TOE additionally audits all the events required under the minimum audit requirements. The TOE records the identity of the user that is accessing components of the TOE and records actions taken by the user when interacting with the system.

8.1.2 Access Control

During the initial establishment of the TLS connection to the Web server from a browser the user's certificate is verified. The user's identity and the role assigned to the user are retrieved from the secure directory. Access to the Web pages, containing the commands permitted to each user's role, is controlled by the ACL for individual pages. The ACL is checked against the user's certificate and role, as described in the following paragraph. Additionally, the TOE relies on the environment and the definition of the CIMC roles in the environment to further control access to the TOE and its components.

The TOE enforces access control based on roles whenever a user attempts to access the TOE-provided functions. To enforce its security policy, the TOE relies on the role assigned per user and the access control list set per group of functions. Both the role associated with a user and access control list associated with functions are set by the Administrator. Access Control by the ACL engine provides authorization for an administrative user to use a system resource. The controlled resources are "workbenches" that contain only groups of functions assigned to a single role, and are hard-coded in the TOE. Authorization is enforced by presenting only role-restricted functions appropriate to the user of the web management interface.

SFR Mapping

- FMT_MOF.1 (Iteration 2)– Predefined Access Control Lists restrict functionality of each role as defined in Table 12 below copied from the CIMC PP - Page 42. The rules are implemented through the Web ACL engine and control access to the System Workbenches. Each rule is stored in the database. Administrators receive detailed directions on how to configure the TOE for CIMC PP compliance in the Administrator Guide. These access control rules are checked before allowing a user access to any System Workbench The IT Environment for the TOE will have the three PP-required roles defined in the Operating System. Access Control to some components of the TOE are controlled by the Operating System's reference monitoring.

Table 12 - Access Controls

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 *Administrators.*
Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers.

Section/Function	Component	Function/Authorized Role
		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, Auditor, or Operator.
Certificate Status Change Approval		Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.
CIMC Configuration		The capability to configure any TSF functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)
Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administrators.
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
Certificate Revocation list Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.
Online Certificate Status Protocol Profile Management	FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.

The TOE access control for “Data Export and Output” as defined by Table 12 does not apply to this TOE as private keys are not held in the TOE and therefore not exported from the TOE. The TOE access control for “Revocation Profile Management” as defined in Table 12 does not apply to this TOE as the TOE does not provide a Revocation Profile. Publication of certificate revocation is managed by CRLs, which are identified in Table 12. The requirements to restrict access to modify CRLs to Administrators also does not apply as the CRL profiles are defined in the underlying source code of the module and are not modifiable.

- FDP_ACC.1 (Iteration 2) - To enforce its security policy, the TOE relies on the rules that are implemented through the Web ACL engine and control access to

the System Workbenches. TOE enforces access control policy on following entities:

- Subjects - User context processes associated to each user
- Objects - Files or directories containing user interface web pages
- Operation – Open web page

- FDP_ACF.1 (Iteration 2)– The TOE enforces the access control policy by use of the following security attributes:
  - Role - Attribute associated with a user's certificate
  - ACL – Access control list associated with an object. ACLs are lists of "Rule" and "Access Right" pairs. A "Rule" is a Boolean expression computed on the subject's attributes (including Role) and "Access Right" attribute permits or prevents opening of the object. Several rules are predefined in the TOE; however the TOE allows for additional rules to be defined. For a complete list of ACLs that are required for this TOE see the Installation Guidance Release Notes provided for the evaluated version of the TOE.

The ACLs are applied as users authenticate to the TOE and the ACLs determine which web pages the user can access. As the web pages contain the buttons and forms that allow the users to perform actions on the TOE, controlling access to the web pages controls user access to functionality within the TOE.

The TOE's Access Control Lists are configured to enforce the access control rules defined in Table 13.The full description of how to perform this setup is provided in the Installation Guidance Documentation.

Table 13 - Access Control List

Section/Function	Component	Event
Certificate Request Remote and Local Data Entry		The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry		The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked.
Data Export and Output		The export or output of confidential and security-relevant data shall only be at the request of authorized users.
Key Generation	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 TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures.

Section/Function	Component	Event
		At least two Officers or one Officer and an Administrator, Auditor, or Operator 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, Officers, and Operators.
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, Auditor, or Operator.
Certificate Status Change Approval[2]		Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold. Only Officers shall be capable of removing a certificate from on hold status. Only Officers shall be capable of approving the placing of a certificate on hold. Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate. Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

The TOE access control requirements for “Private Key Storage”, Private Key Load”, and “Private and Secret Key Destruction” do not apply for the Certificate Manager. The Certificate Manager does not store the certificate subject Private Keys. Additionally, the “Private and Secret Key Export” requirements are not applicable as the TOE does not contain the certificate Subject private keys. Believing that speed in revoking a compromised certificate is critical, in addition to allowing the Officer to revoke a subject’s certificate, the TOE allows the

[2] Every request to change certificate status, for example, revoke a certificate, place a certificate on hold, or remove a certificate from hold must be accepted or rejected. If a request is accepted, any information about the request that may be exported from the TOE must be approved. Approval may be manual or automated.

certificate subject to also revoke the certificate. Similarly, the TOE does not provide a certificate subject with the ability to request that a certificate be placed on hold. The TOE meets FIA_UAU.1 (iteration 2) and FIA_UID.1 (iteration 2) which restrict the actions that can be performed before an operator has identified and authenticated himself. By meeting the FIA_UAU.1 and FIA_UID.1 requirements only authorized operators will have access to issue commands to export or output security-relevant data from the TOE.

- FPT_RVM.1 (Iteration 2)– Non-bypassability – The TOE enforces the Access Control Policy at the Web Front End. Typical user interactions with the TOE will come through the Webserver, either through the Administrator Console or the Enrollment Console. Users of the Webserver interface are simply not presented with options to perform functions that they are not authorized to perform. When a user requests a Web interface the ACLs are checked to determine if the user has permissions to access the requested page. A user can also access components of the TOE through the underlying Operating System. The Installation and Setup guide specifically defines how the Operating System should be configured to setup the CIMC PP required roles and the access control to be placed on TOE files that reside on the file system.

8.1.3 Backup and Recovery

Certificate Manager provides configurable backup functionality, as well as system recovery features, to allow the operators to restore the CA System and maintain the logs and current certificates stored.

SFR Mapping

- FDP_CIMC_BKP.1 – The TOE has a configurable backup facility which is configured via the Web-based System Configuration Workbench pages. The following manually-initiated one-time operations are available:
  - Full backup
  - Incremental backup

  The same functions can be selected for automated backup. The backup start time and interval between backups (days and hours) is specified, as well as the mix of full and incremental backups. Both the current state of the database and the transaction log (for hot backup) are backed up. To fully recover the TOE after a complete system failure, the Certificate Manager software may need to be reinstalled from a CD and the backup database information will be imported to restore the TOE to a prefailure condition. There are no private keys or other critical security parameters stored within the TOE; all private keys are stored in the HSM.
- FDP_CIMC_BKP.2 – The system provides the capability to create a digital signature for each file created or modified in the backup process. These signatures are performed by the Data Integrity Monitor with the key from the Administration CA that issued the backup administration operator's certificate. There are no private keys or other critical security parameters stored within the TOE; all private keys are stored in the HSM.

8.1.4 Secure Import/Export

The Certificate Manager is responsible for importing and exporting certificates, enrollment data, certificate status, and other data. The TOE protects these data transfers through a trusted path using the IT Environment's TLS facility.

SFR Mapping

- FCO_NRO_CIMC.3 – The TOE enforces proof of origin and verification of origin of certificate status information. This is completed by signature verification and a status check of the certificate. For the purpose of authenticating administrators that have the authority to access or alter security relevant information, the TOE accepts only certificates that it has issued. In this case, it can always obtain verification of origin and certificate status information directly from its own database. The TOE provides digitally-signed certificate status information to its clients (for instance by CRL). Any input of security-relevant data or certificate status change is logged, and the log entry identifies the originator of the data.
- FDP_UCT.1 (Iteration 2) – All policy-relevant communications external to the TOE and internal on remote components are performed over an encrypted and authenticated TLS session trusted path. The TOE will only establish connections with users or entities that have a certificate stored in the certificate listing of the CA. Further, before a user is allowed to perform an action the TOE will check the ACL rules to ensure they have rights to perform the requested action (function).
- FPT_ITC.1 (Iteration 2) – All confidential communications external to the TOE and internal on remote components are performed over an encrypted and authenticated TLS session. The TLS session will protect the data transmitted from unauthorized disclosure.
- FCO_NRO_CIMC.4 – A trusted path is established via mutually authenticated TLS for all communications (import and export of data) with the TOE, with the exception of the Enrollment Console. Certificate requests made by a browser or by PKCS#10 request must be signed using the private key corresponding to the public key in the certificate request. This provides proof of possession of the private key as well as protecting the message against modification.

  FDP_CIMC_CSE.1 - The TOE provides certificate status information by means of CRLs (X.509 [3]/ RFC3280 compliant) The TOE provides the ability to configure the specific details of the CRLs for each CA to the Administrator. However, the system enforces compliance with X.509 by limiting the options of what is configurable. The CRLs will always contain the RFC-required fields: Signature Algorithm identifier, issuer Name, thisUpdate Date, Revoked Certificate and a Signature.
- FDP_ITT.1 (Iteration 3 & 4) - All policy-relevant communications external to the TOE and internal on remote components are performed over a tamper-evident, encrypted, and authenticated TLS session. The TLS session will protect the data transmitted from unauthorized modification or disclosure.
- FPT_ITT.1 (Iteration 3 & 4) – All communication of security-relevant and/or confidential data among the TOE's components is performed over a trusted path, TLS-LDAP session. The TLS session will protect the data transmitted from unauthorized modification or disclosure.

[3] RSA has tested and verified that the certificates and CRLs are X.509 compliant. Additionally the CRL's were found to be RFC3280 compliant and the OCSPs were found to be RFC 2560 compliant.

8.1.5 Cryptographic Support and Key Management

Certificate Manager relies on a FIPS 140-1 Level 3 validated cryptographic security module for key generation for certificates and encryption, key storage, and key destruction through zeroization.

SFR Mapping

- FDP_ACF_CIMC.2 – The TOE does not support personnel private keys. FMT_MTD.CIMC.4 – All private keys are stored on the FIPS 140-1 validated hardware security module(HSM).
- FDP_SDI_CIMC.3 – Public keys are all stored signed with a digital signature in the TOE database within a signed certificate or are received as part of the TLS handshake. When the TOE starts up, it accesses the CA System public key and verifies the public key with a challenge from the CA System private key. If the CA System public key verification fails, the TSF will log the error and not start up. The client public keys are verified when the client's certificate is checked during the authentication process of establishing an TLS connection to the CA. If a client signature fails the TLS connection will not be established and an entry is made on the log server.
- FDP_ACF_CIMC.3 – No user secret keys are stored by the TOE.
- FMT_MTD_CIMC.5 – No user secret keys are stored by the TOE. All TSF secret keys are stored in the HSM.
- FCS_CKM_CIMC.5 – The TOE does not contain any private or secret keys. All private and secret keys are stored on the FIPS 140-1/140-2 validated HSM.
- FDP_ETC_CIMC.5 – The TOE does not support key export. User private and secret keys are not stored in the TOE.
- FMT_MTD_CIMC.7 – The TOE does not support key export. User private and secret keys are not stored in the TOE.

8.1.6 Certificate Management

RSA Certificate Manager manages and securely stores all certificates that have been signed using the private key of any of the internal CAs. The Certificate Manager provides functionality to issue, suspend, reinstate, reissue, renew, revoke and delete certificates, report status of certificates, and generate CRLs. All of these certificate services are provided in a secure manner, protecting the integrity of the certificates. Additionally, the TOE enforces proof of origin and verification of origin of certificate status information and all other security-relevant information at all times.

SFR Mapping

- FMT_MOF_CIMC.3 - The TOE provides standard profiles for certificates and ensures that certificates it creates are consistent with the currently selected profile. These profiles conform to the X.509 standard. Certificate profiles are stored as objects in the database. A default set of X.509-compliant profiles is assigned to each CA when it is created, and the profile selection may be modified by the Administrator through the Administration console. Certificates issued by a CA must conform to one of its assigned profiles. The TOE provides the ability to configure the specific details of the certificates (i.e. DN Attributes or Extensions) for each CA to the Administrator.

The default set of X.509 profiles will always contain the required fields: Version, Certificate Serial Number, Signature Algorithm Identifier, Issuer Name, Period of Validity, Subject name, and Subject's Public Key information.

- FMT_MOF_CIMC.5 - The TOE generates CRLs according to an X.509 compliant profile implemented directly in code, to ensure CRLs are always consistent with the standard certificate revocation list profile. The CRL profile is not able to be modified by Administrators. The values of the `Issuer` and `issuerAltName` fields are determined by the name of the issuing CA, while `nextUpdate` is controlled by the Administrator. Administrators can choose 1 of 3 alternate forms for the `authorityKeyIdentifier` extension, as well as whether to include the `invalidityDate` and `freshestCRL` extensions. The configurable values are stored in the secure directory.
- FMT_MOF_CIMC.6 - The TOE does not implement an OCSP responder.
- FDP_CIMC_CER.1 - The TOE provides standard profiles for the certificates and ensures that certificates are consistent with the currently selected profile (same as FMT_MOF_CIMC.3 above).
- FDP_CIMC_CRL.1 – The TOE provides standard profiles for the CRLs to ensure that CRLs are consistent (same as FMT_MOF_CIMC.5 above).
- FDP_CIMC_OCSP.1 – The TOE does not implement an OCSP responder.

8.1.7 Identification and Authentication

RSA Certificate Manager requires identification and authentication before performing any security-relevant functions. The user identity is associated with the on-going TLS session which is established during the user's initial interaction with the TOE. All requests made through this established TLS session are associated with the user's ID from that session. The TSF does this using the (MD5) hash of the user's identity certificate. The TOE maintains a secure database of certificate objects, which is indexed by this hash value, so that hash is a pointer to all the information that the system knows about the user of that certificate. The User Role is part of this user information, and the TOE associates the User Role with subjects acting on behalf of the user. Additional attributes, such as the identity of the CA that issued the user's certificate, can be determined from the user's certificate or the user's database record. Web Front End ACLs consider some or all of User Identity, User Role and Issuing CA Identity in granting or denying access to services. A user-subject binding would fail only if the user did not have the access privileges to invoke the service, in which case the ACL failure would be logged to the audit records.

Because the User Identity is bound to an ongoing TLS connection, there is no mechanism whereby the User Identity associated with a subject can be altered while a user is connected to the TOE.

In addition, the TOE benefits from the Identification and Authentication performed by the Operating System in the IT Environment. The PP-required roles are defined in the OS and the OS will require Identification and Authentication to access TOE components and supporting files. The TOE audits failed and successful attempts at identifying or authenticating as any type of user of the TOE.

SFR Mapping

- FIA_UAU.1 (Iteration 2) – The TOE will only allow the following actions before a user is identified and authenticated: request Enrollment, request a public certificate or request for a CRL. Users are identified during the establishment of the TLS connection. When attempting to establish a connection with the TOE remote entities will present a certificate containing their identification and public key, as well as the identify of the CA that issued the certificate. This identification is authenticated through the TLS protocol as the remote entity confirms they have the private key via the key agreement protocol of TLS. Only remote entities whose certificate was issued by a CA trusted by the TOE (normally a CA within the TOE) can successfully complete authentication. Identification and Authentication attempts are audited by the Webserver in the TOE.
- FIA_UID.1 (Iteration 2) – (See FIA_UAU.1 (Iteration 2))

  FIA_USB.1 (Iteration 2) – The TSF determines the User Identify from the user's TLS certificate, and associates the User Identity with subjects acting on behalf of the user. The User Role is also associated with subjects acting on behalf of the user. There is no mechanism to alter the user's identity or other security attributes for the duration of the TLS session.

8.2 Strength of Function Claims

The Certificate Manager can operate in a range of environments, from benign to hostile. The Certificate Manager relies on a FIPS 140-1 or FIPS 140-2 Level 3 evaluated cryptographic module for cryptographic functions and provides integrity, confidentiality, nondisclosure, and authentication through its cryptographic functions. The Certificate Manager module meets the CIMC PP requirements of Strength of Function (SOF)-Basic. In addition to the SOF-Basic requirement, the CIMC PP requires several explicit SOF claims. The following subsections describe how these explicit SOF claims are addressed by the TOE.

Authentication Mechanisms

The requirement for Authentication Mechanisms specified in FIA_UAU.1 (iterations 1&2) requires an explicit strength of function as defined by the CIMC PP. The authentication mechanisms in the TOE rely on the certificate authentication performed during the TLS session negotiation. Certificate-based authentication falls outside of the scope of permutational or probabilistic mechanisms required in Common Criteria.

Encryption Algorithms

The requirements for Encryption Algorithms specified in the following table require an explicit strength of function as defined by the CIMC PP. Encryption Algorithms fall outside the scope of permutational or probabilistic mechanism required in Common Criteria

Encryption
FAU_STG.1
FCO_NRO_CIMC.4
FDP_ACF_CIMC.2
FDP_ACF_CIMC.3

FDP_CIMC_BKP.2
FDP_ETC_CIMC.5
FDP_SDI_CIMC.3
FMT_MTD_CIMC.4
FMT_MTD_CIMC.5
FMT_MTD_CIMC.7
FPT_CIMC_TSP.1
FPT_TST_CIMC.2
FPT_TST_CIMC.3

All encryption/decryption is performed within the nCipher nShield which received FIPS 140-1 Level 3 certificate #180.

FIPS 140-1 and FIPS 140-2 Validated Cryptographic Modules
The requirements for a FIPS 140-1/FIPS 140-2 device specified in the following table require an explicit strength of function as defined by the CIMC PP.

FIPS 140-1
FCS_CKM.1
FDP_ACF_CIMC.2
FDP_ACF_CIMC.3
FDP_ETC_CIMC.4
FDP_SDI_CIMC.3
FMT_MTD_CIMC.4
FMT_MTD_CIMC.5
FMT_MTD_CIMC.7
FPT_CIMC_TSP.1

There are several CIMC PP functional requirements that specify the use of a FIPS 140-1 validated cryptographic module. The TOE relies on the nCipher netHSM which received FIPS 140-2 Level 3 certificate #680.

Split Knowledge Procedures
The requirements for split knowledge procedures specified in the following table require an explicit strength of function as defined by the CIMC PP.

Split Knowledge Procedures
FDP_ETC_CIMC.5
FMT_MTD_CIMC.7

The TOE does not provide a mechanism for the export of private or secret keys and therefore does not employ any split key procedures.

Authentication Code
The requirements for authentication codes specified in the following table require an explicit strength of function as defined by the CIMC PP.

Authentication Codes
FAU_STG.1
FCO_NRO_CIMC.4
FDP_CIMC_BKP.2
FPT_CIMC_TSP.1
FDP_SDI_CIMC.3
FPT_TST_CIMC.2
FPT_TST_CIMC.3

All cryptographic operations including authentication codes are performed within the nCipher netHSM which received FIPS 140-2 Level 3 certificate #680.

Private and Secret Keys
The TOE relies on the nCipher netHSM which received FIPS 140-2 Level 3 certificate #680, to perform all cryptographic operations (encryption/decryption & hashing) and all non-ephemeral secret and private key generation and management. The TOE's use of this Level 3 FIPS validated device meets or exceeds the Overall Cryptographic modules requirements specified in the CIMC PP, from Table 9 on Page 62.

Required Overall FIPS 140-1 Level for CIMC Cryptographic Modules	
Category of Use	**CIMC Security Level 3**
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

Other Cryptographic Functions
All cryptographic operations including Signature Verification are performed within the nCipher netHSM which received FIPS 140-2 Level 3 certificate #680. As the HSM utilized by the TOE performs more than just signature verification and/or keyless hash

generation the Other Cryptographic SOF requirements levied in Section 7.2.3 of the CIMC Protection Profile are not applicable.

8.3 TOE Security Assurance Measures

The Certificate Manager was developed with the following security Assurance measures in place, which constitutes a Common Criteria EAL 4 augmented level of assurance.

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documentation
- Life Cycle Support
- Tests
- Vulnerability Analysis

This section of the ST provides the mapping demonstrating that the Assurance Measures listed meet the Assurance Requirements necessary to achieve an EAL4 augmented. In this case the specification of assurance measures is done by referencing the appropriate documentation. An analysis by an evaluation lab of the referenced documentation to ensure that the documentation listed meets Assurance Requirements for EAL4 augmented is necessary.

Configuration Management – The Configuration Management documentation provides a description of automation tools used to control the configuration items and how they are used at the RSA development facilities. The documentation provides a complete configuration item list, a unique reference for each item, and an acceptance plan for accepting those items into the configuration management system. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE and how the TOE is generated from the configuration items. The documentation further details the TOE configuration items that are controlled by the configuration management system. This assurance measure is meet by the documentation referenced in Table 14 in the rows labeled ACM.

Delivery and Operation – The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by RSA to protect against TOE modification during product delivery. It includes special procedures implemented to demonstrate authenticity of the delivered TOE and demonstrates the techniques and methods used to detect modifications. The Installation Documentation provided by RSA details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they effect the TSF. This assurance measure is meet by the documentation referenced in Table 14 in the rows labeled ADO.

Development – The Certificate Manager Design documentation consist of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high level design identifies the basic structure of the TSF, the major software elements, a listing of all interfaces, the purpose and method of use for each interface, and a list of effects, exceptions, and errors message for each interface.
- The Implementation Representation captures the detailed internal workings of the TSF in terms of source code that implements the functions detailed in the Low Level Design. The Implementation Representation provided by RSA is a subset of the TSF.
- The Low Level Design provides a detailed design specification that refines the high level design into a level of detail that can be used as a basis for software programming. The document describes the TOE in terms of modules. The purpose of each module, the interrelationship of modules, the TSF-enforcing functions, and the interfaces are detailed.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the Low Level Design.
- The Security Policy Model provides a structured representation of the security policies of the TSP, and demonstrates how the functional specification corresponds to the security policies of the TSP. The document describes the rules and characteristics of all the TSP policies.

This assurance measure is meet by the documentation referenced in Table 14 in the rows labeled ADV.

Guidance Documentation – The RSA Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. RSA provides a single document which addresses the Administrator Guidance and User Guidance. This assurance measure is meet by the documentation referenced in Table 14 in the rows labeled AGD.

Life Cycle Support – RSA ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of life cycle management documentation. The Life Cycle Management documentation describes the physical, procedural, and personnel security measures as well as tool and techniques used in the

development environment to produce the TOE. Additionally it details a plan for tracking and addressing flaws identified with the TOE and defines the life cycle development model used by RSA to develop the TOE. This assurance measure is met by the documentation referenced in Table 14 in the rows labeled ALC.

Tests – There are a number of components that make up the Test documentation. The Depth and Coverage Analysis document demonstrates the systematic testing performed against the functional specification and high level design. The Depth and Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which RSA tested the TOE. RSA's Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided. This assurance measure is meet by the documentation referenced in Table 14 in the rows labeled ATE.

Vulnerability Analysis – The Misuse Analysis of the Guidance provided by RSA discusses the modes of operation of the TOE, the environmental assumptions, and the completeness of the guidance documentation provided. A Vulnerability Analysis is provided by RSA to demonstrate ways in which an operator could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious penetration attacks. The Strength of TOE Security Functions Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements. This assurance measure is meet by the documentation referenced in Table 14 in the rows labeled AVA.

Table 14 - Assurance Measures Mapping to SARs

	Assurance Requirement	Description	Documents Required
ASE	**ASE**	*Evaluation of the Security Target*	• RSA Certificate Manager Version 6.7 Security Target Version 1.7, December 7, 2006 (this document)
ACM	**ACM_AUT.1**	*Evaluation of CM automation*	• RSA Certificate Manager version 6.7, Configuration Management, November 17, 2006, Version 1.2
	ACM_CAP.4	*Evaluation of CM capabilities*	• RSA Certificate Manager version 6.7, Configuration Management, November 17, 2006, Version 1.2
	ACM_SCP.2	*Evaluation of CM scope*	• RSA Certificate Manager version 6.7, Configuration Management, November 17, 2006, Version 1.2
ADO	**ADO_DEL.2**	*Evaluation of delivery*	• RSA Certificate Manager version 6 .7 Delivery and Operation Secure Delivery, Version 1.1, November 9, 2006.
	ADO_IGS.1	*Evaluation of installation, generation, and start-up*	• RSA Certificate Manager 6.7 Installation Guide, First printing: October 2006

	Assurance Requirement	Description	Documents Required
			• RSA Certificate Manager v6.7 Delivery and Operation Installation, Generation and Start-Up Release Notes, Version 1.9, December 8, 2006 o README RSA Certificate Manager 6.7 High Availability, October 2006 o README RSA Certificate Manager 6.7 High Availability – Sun ONE LDAP Directory Configuration, October 2006 o RSA Certificate Manager version 6.7 README TLS-LDAP Directory Server Configuration, Version 1.2, November 7, 2006
ADV	**ADV_FSP.2**	*Evaluation of functional specification*	• RSA Certificate Manager 6.7 Security Functional Specification for Common Criteria Evaluation Against the CIMC PP at Security Level 3, Issue number 1.5, December 8, 2006
	ADV_HLD.2	*Evaluation of high-level design*	• RSA Certificate Manager 6.7 Security-Enforcing High Level Design for Common Criteria Evaluation Against the CIMC PP, Version 1.3, November 15, 2006
	ADV_IMP.1	*Evaluation of implementation representation*	• RSA Certificate Manager 6.7 Implementation Representation for Common Criteria Evaluation Against the CIMC PP at Security Level 3, version 1.3, November 30, 2006 and corresponding source files
	ADV_LLD.1	*Evaluation of low-level design*	• RSA Certificate Manager 6.7 Security-Enforcing Low Level Design for Common Criteria Evaluation Against the CIMC Protection Profile, Version 1.5, December 1, 2006
	ADV_RCR.1	*Evaluation of representation correspondence*	• RSA Certificate Manager Version 6.7 Representation Correspondence for Common Criteria Evaluation Against the CIMC PP at Security Level 3, Version 1.1, November 30, 2006
	ADV_SPM.1	*Evaluation of security policy modeling*	• RSA Certificate Manager Version 6.7 Informal Security Policy Model, Version 1.2, November 30, 2006

	Assurance Requirement	Description	Documents Required
AGD	**AGD_ADM.1**	*Evaluation of administrator guidance*	• RSA Certificate Manager 6.7 Administrator's Guide • RSA Certificate Manager 6.7 Vettor's Guide • RSA Certificate Manager version 6.7 Guidance Documents Administrator's Guide Release Notes, 1.3
	AGD_USR.1	*Evaluation of user guidance*	• RSA Certificate Manager 6.7 Administrator's Guide • RSA Certificate Manager 6.7 Vettor's Guide • RSA Certificate Manager version 6.7 Guidance Documents Administrator's Guide Release Notes, 1.3
ALC	**ALC_DVS.1**	*Evaluation of development security*	• RSA Certificate Manager version 6.7, Life Cycle Support Development Security Tools and Techniques Development Life Cycle Model, November 6, 2006, version 1.1
	ALC_FLR.2	*Flaw Reporting procedures*	• RSA Certificate Manager version 6.7, Life Cycle Support Flaw Remediation, November 29, 2006, version 1.2
	ALC_LCD.1	*Evaluation of life-cycle definition*	• RSA Certificate Manager version 6.7, Life Cycle Support Development Security Tools and Techniques Development Life Cycle Model, November 6, 2006, version 1.1
	ALC_TAT.1	*Evaluation of tools and techniques*	• RSA Certificate Manager version 6.7, Life Cycle Support Development Security Tools and Techniques Development Life Cycle Model, November 6, 2006, version 1.1
ATE	**ATE_COV.2**	*Evaluation of coverage*	• RSA Certificate Manager Version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP Test Plan v1.6
	ATE_DPT.1	*Evaluation of depth*	• RSA Certificate Manager Version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP Test Plan v1.6
	ATE_FUN.1	*Evaluation of functional tests*	• RSA Certificate Manager Version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP Test Plan v1.6 • All test cases and test results documents referenced in the folowing sub-Table
	ATE_IND.2	*Evaluation of independent testing*	Evaluation laboratory performs testing to provide assurance.

	Assurance Requirement	Description	Documents Required
AVA	**AVA_MSU.2**	*Evaluation of misuse*	• RSA Certificate Manager version 6.7 Vulnerability Assessment: Vulnerability Analysis, Strength of TOE Security Function, Misuse, 17 November 2006,Version 1.4
	AVA_SOF.1	*Evaluation of the strength of TOE security functions*	• RSA Certificate Manager version 6.7 Vulnerability Assessment: Vulnerability Analysis, Strength of TOE Security Function, Misuse, 17 November 2006,Version 1.4
	AVA_VLA.2	*Evaluation of vulnerability Analysis*	• RSA Certificate Manager version 6.7 Vulnerability Assessment: Vulnerability Analysis, Strength of TOE Security Function, Misuse, 17 November 2006,Version 1.4

Test Procedure Document Reference	Version
	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Management of Security Functions Behavior	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Import and export of data	1.2
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Certificate Status Export	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Certificate Revocation List	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Backup and Recovery	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Access Control	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Identification & Authentication	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Key Management	1.1

Test Procedure Document Reference	Version
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Protected Audit Trail Storage	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Prevention of Audit Data Loss	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Reliable Time Stamps And Audit Log Signing Event	1.1
RSA Certificate Manager version 6.7 Functional Tests for Common Criteria Evaluation Against the CIMC PP: Audit Data Generation	1.2

9.0 PP Claims

This section provides PP conformance claims

9.1 PP Conformance

The TOE conforms to the following PP:

- Certificate Issuing and Management Component (CIMC) Protection Profile Security Level 3 (which specifies EAL3 augmented) authored by NIST dated October 31, 2001.

9.2 PP Refinements

As stated above, this ST conforms to the CIMC PP with these refinements:

- The CIMC PP Security Level 3 specifies an EAL3 augmented. RSA elected to pursue more rigorous assurance evaluation and has provided evidence to demonstrate an EAL4 augmented with ALC_FLR.2.

- In addition to the Security Level 3 Assurance Requirements, ACM_AUT.1 – Partial CM Automation and ALC_LCD.1 – Developer defined life cycle model were added. Further, the CM Capabilities requirement was upgraded from ACM_CAP.3 to ACM_CAP.4. These changes were made to bring the assurance up to a complete EAL4 augmented. The one augmentation is ALC_FLR.2. Flaw Reporting Procedures – ALC_FLR.2 was an augmentation required in the CIMC PP for Security Level 3.

9.3 PP Tailoring

The ST directly conforms to the PP with the following exceptions:

1. Security requirement updates from CCv2.1 to CCv2.3 – The PP was evaluated in 2001 and this ST was originally prepared in 2002, when CCv2.1 was in force, extended by interpretations. At this time, CCv2.3 is the controlling version of the specification. In updating the ST for changes to the RCM TOE, it was necessary to update it also for changes to the Common Criteria.

   Each iteration of every SFR in the ST was compared with the corresponding SFR in the PP, and at the same time with the corresponding SFR as it appears in CC v2.1 part 2 and CC v2.3 part 2. In each case, when operations (selection, assignment, refinement) were performed by the PP, these were evaluated for consistency with CC part 2. The following rules were applied:

   - When the SFR statement in CCv2.1 was identical to the statement in CCv2.3, the statement in the PP was consistent, considering any operations by the PP author, with the statement in CCv2.3, and the statement in the ST was consistent with the PP, considering any operations performed in the ST, then no action was taken to the ST SFR statement.

- When the SFR statement in CCv2.3 was different from that in CCv2.1, the difference was analyzed to determine whether the change made an **effective** difference to the SFR. Minor wording changes were carried directly through to the ST when they did not affect any operation carried out by the PP author. When a PP operation was affected, the ST either was updated with the CCv2.3 wording or an ST refinement was applied to the CCv2.3 SFR to retain the PP author's apparent intention. A written rationale has not been provided for individual changes. When additional elements were added to an SFR component in CCv2.3 (such as for FIA_USB.1), these were carried through to the ST directly, as including them was not judged to introduce any apparent conflict with the goals of the PP in specifying the security requirements of a CIMC.
- When the SFR statement was identical in CCv2.3 and CCv2.1, but different from the statement in the PP (accounting for operations performed by the PP), in general the ST follows the PP form of the SFR. The rationale is that such differences must be assumed to have been refinements made through conscious choice by the PP author, working with CCv2.1. Because the CIMC PP is an evaluated PP, it must further be assumed that the SFR as it appears in the PP is consistent with CC part 2, despite wording differences or changes to operations.

2. The table numbering in the ST varies from the number in the PP. Some Tailoring of the PP requirements was necessary to allow the table and figuring number to remain in sequence. The following requirements were tailored to adjust table numbering to allow the ST to reference the exact same table as the PP with a different Table number.
   - Section 6.1 – FAU_GEN.1 (Iteration 2), FAU_GEN.1.1 item "c"
   - Section 6.1 – FAU_GEN.1 (Iteration 2), FAU_GEN.1.2 item "b"
   - Section 6.2 – FMT_MOF.1.1
   - Section 6.4 – FDP_ACF.1.2
3. Refinement by the ST:
   - Section 5.1 – FAU_GEN.1 (iteration 1), FAU_GEN.1.2 item "a", added "(if applicable)" because some audit events are automated system functions where the subject is not bound to an identifiable User
   - Section 5.2 – FMT_MSA.1, FMT_MSA.1.1, added "of the CIMC PP" to identify the section cited
   - Section 5.3 – FDP_ACC.1 (iteration 1), FDP_ACC.1.1, added "of the CIMC PP" to identify the section cited
   - Section 5.3 – FDP_ACF.1 (iteration 1), FDP_ACF.1.1, added "of the CIMC PP" to identify the section cited
   - Section 5.4 – FIA_AFL.1, FIA_AFL.1.1 refinement to PP selection: "an authorized administrator configurable integer" (combined PP operation and refinement conventions used)
   - Section 5.5 – FDP_ITT.1 (iteration 1 & 2), FDP_ITT.1.1, added "of the CIMC PP" to identify the section cited
   - Section 5.5 – FDP_UCT.1 (iteration 1), FDP_UCT.1.1 added "of the CIMC PP" to identify the section cited

- Section 5.7 – FPT_AMT.1, FPT_AMT.1.1 added “and on demand”
- Section 6.1 – FAU_GEN.1 (iteration 2), FAU_GEN.1.2 item “a”, added “(if applicable)” because some audit events are automated system functions where the subject is not bound to an identifiable User
- Section 6.4 – FDP_ACF.1 (iteration 2), FDP_ACF.1.1, added “of the CIMC PP” to identify the section cited
- Section 6.6 – FDP_ITT.1 (iteration 3 & 4), FDP_ITT.1.1, added “of the CIMC PP” to identify the section cited
- Section 6.6 – FDP_UCT.1 (iteration 2), FDP_UCT.1.1 added “of the CIMC PP” to identify the section cited

10.0 Rationale

This section demonstrates that all threats, assumptions, and organizational security policies are countered by the security objectives. Additionally, the section shows that each security objective addresses at least one threat, assumption, or security policy.

10.1 Security Objectives Coverage

The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective counters at least one threat, policy or assumption, and that each threat, policy or assumption is covered by at least one security objective. The rationale presented in Table 15 was taken directly from the CIMC PP. Non-IT Security Objectives Rationale are addressed in Table 16. The Organizational Security Policies Related to Security Objectives are presented in Table 18.

Table 15. Relationship of Security Objectives for the TOE to Threats

IT Security Objective	Threat
O.Certificates	T.Administrators, Operators, 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 16. Relationship of Security Objectives for the Environment to Threats

Non-IT Security Objective	Threat
O.Administrators, Operators, Officers and Auditors guidance documentation	T.Disclosure of private and secret keys, T.Administrators, Operators, Officers and Auditors commit errors or hostile actions T.Social engineering

Table 16. Relationship of Security Objectives for the Environment to Threats

Non-IT Security Objective	Threat
O.Competent Administrators, Operators, Officers and Auditors	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.CPS	T.Administrative errors of omission
O.Cryptographic functions	T.Disclosure of private and secret keys, T.Modification of secret/private keys
O.Installation	T.Critical system component fails
O.Lifecycle security	T.Critical system component fails, T.Malicious code exploitation
O.Notify Authorities of Security Issues	T.Hacker gains access
O.Periodically check integrity	T.Malicious code exploitation
O.Physical Protection	T.Hacker physical access
O.Repair identified security flaws	T.Flawed code T.Critical system component fails
O.Security roles	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Social Engineering Training	T.Social Engineering
O.Trusted path	T.Hacker gains access, T.Message content modification
O.Validation of security function	T.Malicious code exploitation, T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

Table 17. 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

Table 17. Relationship of Security Objectives for Both the TOE and the Environment to Threats

Non-IT Security Objective	Threat
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, Operators, 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, Operators, 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, Operators, Officers and Auditors commit errors or hostile actions
O.Maintain user attributes	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Manage behavior of security functions	T.Critical system component fails, T.Administrators, Operators, 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, Operators, 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

Table 17. Relationship of Security Objectives for Both the TOE and the Environment to Threats

Non-IT Security Objective	Threat
O.Respond to possible loss of stored audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Restrict actions before authentication	T.Hacker gains access, T.Administrators, Operators, 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, Operators, Officers and Auditors commit errors or hostile actions

Table 18. 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 19. 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, Operators, Officers and Auditors	O.Competent Administrators, Operators, Officers and Auditors

Table 19. Relationship of Assumptions to IT Security Objectives

Assumption	IT Security Objective
A.Disposal of Authentication Data	O.Disposal of Authentication Data
A. Hardware Integrity	O.Hardware Integrity
A.Malicious Code Not Signed	O.Malicious Code Not Signed
A.Physical Protection	O.Physical Protection
A.Operating System	O.Operating System
A.Social Engineering Training	O.Social Engineering Training
A.Cooperative Users	O.Cooperative Users

10.1.32

The following discussions provide information regarding:

1. Why the identified security objectives provide for effective counter measures to the threats;
2. Why the identified security objectives provide complete coverage of each organizational security policy;
3. Why the identified security objectives up hold each assumption.

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.

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.

- 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.

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, Operators, Officers and Auditors ensures that users are capable of maintaining effective security practices. This reduces the likelihood that they will commit errors.

O.Administrators, Operators, 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.

10.1.33 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.

10.1.34 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, Operators, Officers and Auditors establishes that security of the TOE is dependent upon those that manage it. This is addressed by **O.Competent Administrators, Operators, Officers and Auditors**, which ensures that the system managers will be competent in its administration.

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

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

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

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

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

Connectivity

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

Physical

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

A.Physical Protection establishes that physical modification of the TOE hardware, software, and firmware will compromise system security. This is addressed by **O.Physical Protection**, which ensures that adequate physical protection will be provided.

Personnel

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.

10.2 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. This rationale is taken directly from the CIMC PP.

10.2.1 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. Table 20. Security Functional Requirements Related to Security Objectives, in this section, addresses the mapping of security functional requirements to security objectives. Table 21. Security Assurance Requirements Related to Security Objectives, in this section, addresses the mapping of security Assurance Requirements to security objectives.

Table 20. 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
FAU_SAR.3 Selectable audit review	O.Individual accountability and audit records
FAU_SEL.1 Selective audit (iterations 1 and 2)	O.Individual accountability and audit records

Table 20. Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
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	O.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_COP.1 Cryptographic operation	O.Cryptographic functions
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_CIMC_OCSP.1 OCSP basic response validation	O.Certificates
FDP_ETC_CIMC.5 Extended user private and secret key export	O.Data import/export
FDP_ITT.1 Basic internal transfer protection	O.Integrity protection of user data and

Table 20. Security Functional Requirements Related to Security Objectives

Functional Requirement	Objective
(iterations 1 and 3)	software, 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_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_MOF_CIMC.6 OCSP 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	O.Data import/export

Table 20. Security Functional Requirements Related to Security Objectives

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

Table 21 addresses the mapping of security Assurance Requirements to security objectives.

Table 21. Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
ACM_AUT.1 Partial CM automation	selection of EAL 4, O.Configuration management

Table 21. Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
ACM_CAP.4 Generation support and acceptance procedures	selection of EAL 4, O.Configuration management
ACM_SCP.2 Problem tracking CM Coverage	selection of SL3, EAL 4, O.Configuration management
ADO_DEL.2 Detection of modification	selection of SL3, EAL 4
ADO_IGS.1 Installation, Generation, and Start-up Procedures	selection of SL3, EAL 4, O.Installation
ADV_FSP.2 Fully defined external interfaces	selection of SL3, EAL 4, O.Lifecycle security
ADV_HLD.2 Security enforcing high-level design	selection of SL3, EAL 4, O.Lifecycle security
ADV_IMP.1 Subset of the implementation of the TSF	selection of SL3, EAL 4, O.Lifecycle security
ADV_LLD.1 Descriptive low-level design	selection of SL3, EAL 4, O.Lifecycle security
ADV_RCR.1 Informal Correspondence Demonstration	O.Lifecycle security, selection of SL3, EAL 4
ADV_SPM.1 Informal TOE security policy model	selection of SL3, EAL 4, O.Lifecycle security
AGD_ADM.1 Administrator Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.Auditors Review Audit Logs, O.Competent Administrators, Operators, 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 SL3, EAL 4
AGD_USR.1 User Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.Malicious Code Not Signed,

Table 21. Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
	O.Procedures for preventing malicious code, O.Require inspection for downloads, selection of SL 3, EAL 4
ALC_DVS.1 Identification of security measures	selection of SL 3, EAL 4
ALC_FLR.2 Flaw reporting procedures	O.Lifecycle security, O.Repair identified security flaws, selection of SL 3
ALC_LCD.1 Developer defined life-cycle model	selection of EAL 4
ALC_TAT.1 Well-defined development tools	selection of SL 3, EAL 4
ATE_COV.2 Analysis of coverage	selection of SL 3, EAL 4
ATE_DPT.1 Testing - High-Level Design	selection of SL 3, EAL4
ATE_FUN.1 Functional testing	selection of SL 3, EAL 4
ATE_IND.2 Independent Testing - Sample	selection of SL 3, EAL 4
AVA_MSU.2 Validation of analysis	selection of SL 3, EAL 4
AVA_SOF.1 Strength of TOE Security Function Evaluation	selection of SL 3, EAL 4
AVA_VLA.2 Independent vulnerability analysis	selection of SL3, EAL 4

10.2.2 Security Requirements Sufficiency

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)**, and **FDP_CIMC_OCSP.1 (OCSP basic response validation)** which ensure that certificate revocation lists and certificate status information are valid. In the case that the TOE maintains a copy of the certificate subject's private key**, 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. In the case that a secret key is used by the certificate subject as an authenticator in requesting a certificate, **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 cover 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 cover 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.

O.Administrators, Operators, 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, Operators, 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 also 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.

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

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, Operators, Officers, and Auditors be provided with documentation describing the procedures necessary to securely install and operate the TOE. **A.Competent Administrators, Operators, Officers and Auditors** covers the requirement that competent Administrators, Operators, 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, operators, officers, and auditors are trained in techniques to thwart social engineering attacks.

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.

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.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)** cover 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 cover the requirement that vendor repair security flaws that have been identified by a user.

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.

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)** cover 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)** cover the requirement that Administrators be able to control to the types of information that are included in generated certificate revocation lists. **FMT_MOF_CIMC.6 (OCSP Profile Management)** covers the requirement that Administrators be able to control to the types of information that are included in generated OCSP responses. **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, Operators, 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 CIMC. **FDP_ETC_CIMC.5 (Extended user private and secret key export)**, **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.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.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, can not 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, Operators, 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, Operators, 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, Operators, Officers, and Auditors can not perform operations that they are not authorized to perform by bypassing the TSP enforcement 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.1 (CIMC backup and recovery)**, **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery),** cover 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, Operators, 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, Operators, 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, Officer, or Operator.

10.3 Explicitly Stated Security Requirements Rationale

The explicitly stated components provided below are necessary to specify a unique set of requirements for certificate issuing and management components that are not addressed by the CC. All explicitly stated requirements are directly from the CIMC Protection Profile. More detailed rational for the inclusion of each explicitly stated requirement can be located in the CIMC PP directly below the prose requirement description.

Additional Assurance Requirements ACM_CAP.4, ACM_AUT.1, and ALC_LCD.1, were added to the CIMC PP Security Level 3 assurance requirements. The Assurance Requirements specified at Security Level 3 were found to be satisfactory The addition of more assurance requirements should not negatively impact the appropriateness or applicability of the Assurance requirements to support any explicitly stated TOE security functional requirements. ACM_CAP.4 is similar to ACM_CAP.3 and does not change appropriateness of functional requirements. ACM_AUT.1 requires automation of the

Configuration Management system which applies regardless of security function. ALC_LCD.1 requires a life cycle definition which is appropriate regardless of security functions.

Explicitly Stated TOE Security Functional Requirements
FCO_NRO_CIMC.3 Enforced proof of origin and verification of Origin
FCO_NRO_CIMC.4 Advanced verification of origin
FCS_CKM_CIMC.5 CIMC private and secret key zeroization
FDP_ACF_CIMC.2 User private key confidentiality protection
FDP_ACF_CIMC.3 User secret key confidentiality protection
FDP_CIMC_BKP.1 CIMC backup and recovery
FDP_CIMC_BKP.2 Extended CIMC backup and recovery
FDP_CIMC_CER.1 Certificate Generation
FDP_CIMC_CRL.1 Certificate Revocation
FDP_CIMC_CSE.1 Certificate Statue Export
FDP_CIMC_OCSP.1 Basic Response Validation
FDP_ETC_CIMC.5 Extended user private and secret key export
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
FMT_MOF_CIMC.3 Extended certificate profile management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management
FMT_MOF_CIMC.6 OCSP Profile Management
FMT_MTD_CIMC.4 TSF private key confidentiality protection
FMT_MTD_CIMC.5 TSF secret key confidentiality protection
FMT_MTD_CIMC.7 Extended TSF private and secret key export
FPT_CIMC_TSP.1 Audit log signing event
Explicitly Stated Environmental Security Functional Requirements
FPT_TST_CIMC.2 Software/firmware integrity test
FPT_TST_CIMC.3 Software/firmware load test

10.4 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.

10.4.1 Rationale that Requirements are Mutually Supportive

The requirements represented in this ST were taken from the CIMC PP, which was developed from a variety of sources. The security requirements work mutually so that each SFR is protected against bypassing, tampering, deactivation, and detection by other SFRs.

Bypass

Prevention of bypass is derived as described below:

FIA_UID.1 (iteration 1&2) and FIA_UAU.1 (iteration 1&2) support other functions allowing user access to data by limiting the actions that the user can take prior to identification and authentication.

The management functions, including FMT_MOF.1 (iteration 1&2), 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.

Tamper

Prevention of tamper is derived as described below:

FAU_STG.1 (iteration 1&2) 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 (iteration 1&2) and FIA_UAU.1 (iteration 1&2) 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 (iteration 1&2), 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.

FIA_AFL.1 supports all SFRs dealing with authentication by limiting the number of entry attempts, and then mandating an appropriate action to protect the TOE if too many attempts have been made.

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.

Deactivation

Prevention of deactivation is derived as described below:

The access control SFP detailed in FDP_ACF.1 (iteration 1&2), 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 (iteration 1&2), 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.

Detection

Detection is derived as described below:

The security audit functions, including FAU_GEN.1 (iteration 1&2), FAU_GEN.2 (iteration 1&2), and FAU_SEL.1 (iteration 1&2), 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 (iteration 1&2), and FAU_STG.4 (iteration 1&2) provide for the protection of the audit records.

The management functions, including FMT_MOF.1 (iteration 1&2), 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.

10.5 Rationale for Strength of Function

The TOE described in this Security Target is intended to operate in a range of environments, from benign to hostile. Therefore, the TOE requires cryptographic functions to provide for integrity, confidentiality, nondisclosure, and authentication. A strength of Function rating of SOF-Basic was designated for this TOE to meet the CIMC PP requirements which specify SOF-Basic as a satisfactory level for Security Level 3 CIMC TOEs. Section 8.2 details the complete Strength of Function Claims for this TOE.

10.5.1 Rationale for Security Level 3/EAL4

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 protection against someone with physical access to the components and includes additional Assurance Requirements to ensure the CIMC is functioning securely.

In the CIMC, the recommended Assurance level for this security level is EAL3 augmented. The RSA Certificate Manager was designed to meet EAL4 augmented. EAL4 augmented was selected for this TOE because of the PP requirements, as well as potential customer requirements – specifically the Department of Defense. EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. It is thus applicable in those circumstances where users require a moderate to high level of independently assured security in conventional commodity TOEs. Augmentation results from the selection of ALC_FLR.2.

ALC_FLR.2 Flaw Report Procedures

EAL4 does 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.

10.6 TOE Summary Specification Rationale

This section intends to show that the TOE Security Functions are suitable to meet the TOE Functional requirements given in the CIMC PP. The following table demonstrates

the mapping of the TOE Security Functions to Security Requirements from the CIMC PP. The details on how these requirements meet the specific Security requirements specified in the CIMC PP is provided in Section 8.0 - TOE Summary Specifications.

TOE Security Function	Functional Requirement
Secure Audit/Logging Services	FAU_GEN.1 (iteration 2) FAU_GEN.2 (iteration 2) FAU_SEL.1 (iteration 2) FAU_STG.1 (iteration 2) FAU_STG.4 (iteration 2) FPT_CIMC_TSP.1 FPT_STM.1 (iteration 2)
Access Control	FMT_MOF.1 (iteration 2) FDP_ACC.1 (iteration 2) FDP_ACF.1 (iteration 2) FPt_RVM.1 (iteration 2)
Backup and Recovery	FDP_CIMC_BKP.1 FDP_CIMC_BKP.2
Secure Import/Export	FCO_NRO_CIMC.3 FDP_UCT.1 (iteration 2) FPT_ITC.1 FCO_NRO_CIMC.4 FDP_CIMC_CSE.1 FDP_ITT.1 (iteration 3 & 4) FPT_ITT.1 (iteration 3 & 4)
Cryptographic Support and Key Management	FDP_ACF_CIMC.2 FMT_MTD.CIMC.4 FDP_SDI_CIMC.3 FDP_ACF_CIMC.3 FMT_MTD_CIMC.5 FCS_CKM.CIMC.5 FDP_ETC_CIMC.5 FMT_MTD_CIMC.7
Certification Management	FMT_MOF_CIMC.3 FMT_MOF_CIMC.5 FMT_MOF_CIMC.6 FDP_CIMC_CER.1 FDP_CIMC_CRL.1 FDP_CIMC_OCSP.1
Identification & Authentication	FIA_UAU.1 (iteration 2) FIA_UID.1 (iteration 2) FIA_USB.1 (iteration 2)

10.7 TOE Assurance Measure Requirements

All of the TOE Assurance measures can be mapped to the SARs specified in the CIMC PP. Table 14 in Section 8.3 provides this mapping.

In addition to the Security Level 3 Assurance Requirements, ACM_AUT.1 – Partial CM Automation and ALC_LCD.1 –Developer defined life cycle model were added. Further the CM Capabilities requirement was upgraded from ACM_CAP.3 to ACM_CAP.4. These changes were made to bring the Assurance up to a complete EAL4 augmented. This augmentation is required by specific customers of RSA and will provide other customers with the level of assurance from a complete EAL4 rather than EAL3 augmented. The augmentation is ALC_FLR.2. Flaw Reporting Procedures – ALC_FLR.2 was an augmentation required in the CIMC PP for Security Level 3.

10.8 Rationale for SFR Dependencies

The following table demonstrates that all SFR dependences are addressed. This table was taken directly from the CIMC PP, with the exception that iteration number is indicated[4].

Component	Dependencies	Which is:
FAU_GEN.1 (iteration 1&2) Audit data generation	FPT_STM.1 (iteration 1&2) Reliable time stamps	Included
FAU_GEN.2 (iteration 1&2) User identity association	FAU_GEN.1 (iteration 1&2) Audit data generation	Included
	FIA_UID.1 (iteration 1&2)Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 (iteration 1&2) Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 (iteration 1&2) Selective audit	FAU_GEN.1 (iteration 1&2) Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 (iteration 1&2) Protected audit trail storage	FAU_GEN.1 (iteration 1&2) Audit data generation	Included
FAU_STG.4 (iteration 1&2) Prevention of audit data loss	FAU_STG.1 (iteration 1&2) Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 (iteration 1&2) Timing of identification	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	Included

[4] When no iteration number is shown, the SFR is used only one time in the ST.

Component	Dependencies	Which is:
	destruction	
	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 (iteration 1&2) Subset access control	FDP_ACF.1 (iteration 1&2) Security attribute based access control	Included
FDP_ACF.1 (iteration 1&2) Security attribute based access control	FDP_ACC.1 (iteration 1&2)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 (iteration 1&2) 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	None	

Component	Dependencies	Which is:
export		
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	None	
FDP_ITT.1 (iteration 1,2,3,&4) Basic internal transfer protection	FDP_ACC.1 (iteration 1&2) Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 (iteration 1&2) Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 (iteration 1&2) Basic data exchange confidentiality	FDP_ACC.1 (iteration 1&2) Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 (iteration 1&2) Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	NOT Included
FIA_AFL.1 (iteration 1&2) Authentication failure handling	FIA_UAU.1 (iteration 1&2) Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 (iteration 1&2) Timing of authentication	FIA_UID.1 (iteration 1&2) Timing of identification	Included
FIA_UID.1 (iteration 1&2) Timing of identification	None	
FIA_USB.1 (iteration 1&2) User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 (iteration 1&2) Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
	FMT_SMF.1 Specification of Management Functions	NOT Included
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF.1 (iteration 1&2) 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 (iteration 1&2) Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)

Component	Dependencies	Which is:
FMT_MOF_CIMC.6 OCSP profile management	FMT_MOF.1 (iteration 1&2) 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 (iteration 1&2) Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 (iteration 1&2) 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 (iteration 1&2) Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 (iteration 1&2) 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.7 Extended TSF private and secret key export	None	Included
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 (iteration 1&2) Audit data generation	Included
	FMT_MOF.1 (iteration 1&2) Management of security functions behavior	Included

Component	Dependencies	Which is:
FPT_ITC.1 (iteration 1&2) Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 (iteration 1,2,3,&4) Basic internal TSF data transfer protection	None	
FPT_RVM.1 – Non-Bypassability of TSP (iteration 1&2)	None	
FPT_SEP.1 – TSF Domain Separation (iteration 1&2)	None	
FPT_STM.1 (iteration 1&2) 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	

*10.8.1 **Justification of Unsupported Dependency FMT_SMF.1***

Component FMT_SMF.1 Specification of management functions is a dependency for FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1 in CC version 2.3, though it was not in CC version 2.1. As a result of updating to CCv2.3, it is so shown in this ST. However, FMT_SMF.1 is not included in the ST because the requirement only explicitly states what is implied with the inclusion of the security functional requirements FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1. The management requirements identify all the functions that the TOE provides. Any functions not provided by the TOE are clearly identified in Section 8.0 *TOE Summary Specification*.

10.9 Rationale for SAR Dependencies

The following table demonstrates that all SAR dependencies are addressed. This table was taken directly from the CIMC PP. A table representing the additional assurance requirements that were added to the Security Level 3 requirements appears below Table 22.

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
ACM_AUT.1	ACM_CAP.3	included (hierarchical to ACM_CAP.4)
	(indirect) ALC_DVS.1	included

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
ACM_CAP.4	ACM_SCP.1	Included (hierarchical to ACM_SCP.2)
	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_FSP.2	ADV_RCR.1	included
ADV_HLD.2	ADV_FSP.1	included (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
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
ADV_RCR.1	no dependencies	not applicable

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
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	no dependencies	not applicable
ALC_FLR.2	no dependencies	not applicable
ALC_LCD.1	no dependencies	not applicable
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	no dependencies	not applicable

Table 22. Summary of Security Assurance Requirements Dependencies for Security Level 3

Component	Depends On:	Which is:
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

11.0 Annex I: Evaluation Restrictions

There are a number of functions of the RSA Certificate Manager that are identified in the *Administrator's Guide* or other distribution documents, but which have intentionally been excluded from the scope of the Common Criteria evaluation. This has been done for several different reasons, the most common being:

- Use of the function or feature is incompatible with the SFRs of the CIMC PP.
- The function or feature is an add-on (typically a subsystem) of limited general usefulness; the function or feature is not interesting to known customers that require CC evaluation; documentation and evaluation would require considerable additional effort not justified by commercial considerations.

The functions or features that are intentionally excluded from the scope of the Evaluation are listed here, along with a rationale for exclusion. This helps customers to understand what features are not covered by the CC evaluation, and clarifies for evaluators that these features have not simply been omitted from the *Functional Specification* and other documentation by inadvertence. The *Administrator's Guide Release Notes* instructs Evaluators and customers which features of RSA Certificate Manager must be prevented from use, whether by being disabled or by instituting policies that prohibit use. Thus comparable tables appear in both the *Functional Specification* and the *Administrator's Guide Release Notes*. In the case of any incompatibilities in these tables, this document (ST) is to be considered definitive.

Table 23 - Omitted Features

Function or Feature	Rationale for Exclusion from Scope of Evaluation
RSA OneStep CGI Program	Subsection 11.3.1
Certificate Management Protocol (CMP) Server	Subsection 11.3.2
Simple Certificate Enrollment Protocol (SCEP) Server	Subsection 11.3.3
Certificate Request Syntax (CRS) Server	Subsection 11.3.4
Xudad Database Plugin API	Subsection 11.4
Trusting External CAs	Subsection 11.2
Trusting an External RCM CA	
Trusting an External CA Certificate	
Importing CRLs from Trusted CAs	
Use of Private Keys in Software	Subsection 11.5
Software CAs	
Software Signers	
Software TLS Server Key Storage	
Exporting CA to PKCS#12	
Importing CA from PKCS#12	
CryptoPro Cryptographic Service Provider	
Configuring Unattended Startup and Operation	Subsection 11.6
TLS Passphrases in `startup.conf`	
CA Private Key PIN in `setpin` *directive*	
Local LDAP Publication	Subsection 11.7
Multiple Administrative Roles per Certificate	Subsection 11.8

Function or Feature	Rationale for Exclusion from Scope of Evaluation
Modification of Web Front End Scripts	Subsection 11.1
Generating Complete CRLs Every Time a Certificate's Status Changes	
Generating ARLs Every Time a CA's Status Changes	

11.1 Modification of Web Front End Scripts

"Generating CRLs on Certificate Status Change" is not a function provided by the as-installed RCM. However, the Administration Guide (Chapter 18 *Revocation Lists*, Section "Generating Complete CRLs", Subsection "Generating Every Time a Certificate's Status Changes") describes two operations that can be enabled programmatically, every time a certificate's status changes, by modifying a number of *xuda* templates:

- Generating Complete CRLs Every Time a Certificate's Status Changes
- Generating ARLs Every Time a CA's Status Changes

Consider that "*xuda* templates" are files containing X-Parse directives. X-Parse is a scripting language developed by Xcert International, Inc.[5], a language that enables web pages to invoke a broad range of "backend" functionality contained within the PKI Server. The Administration, Vetting, Auditing and Enrollment consoles are instantiated by a mix of HTML files and *xuda* templates. RCM access control is based on ACLs that mediate access to the directories and files that comprise these consoles.

An Administrator or IT specialist who is permitted to modify or construct *xuda* templates can re-create any administrative function in a filesystem location that is independent of whatever access control rules normally apply to that functionality. Whether through ignorance, unconcern for access control rules or malfeasance, it is perfectly possible to construct a set of HTML pages and *xuda* templates that allow any operation of which the CIMC is capable to be performed outside of PP-mandated access controls.

In essence, *xuda* templates containing X-Parse calls that are constructed by customers are no different from C language plugins written by customers. Each introduces untrusted, unevaluated code into the TSF. For this reason, we chose to exclude any modification of *xuda* pages, including those that generate CRLs on certificate status change, from CC evaluation.

The query remains: "It is not clear why this would conflict with SFRs. It seems this could actually be used and tested without any changes to the ST. Perhaps we are missing something – perhaps this introduces a new interface?" Clearly, if RSA Security were to provide options in the Administration console to exercise these functions, there would not be an issue in evaluating them. Since RSA has chosen not to do so, the presumption is that these functions are not of interest to most customers. Although they are detailed in the Administration Guide, they are but one of a multitude of additional functions that *might* be implemented by modifying or creating new *xuda* pages. There does not seem

[5] Xcert International, Inc. was purchased by RSA Security, Inc., in 2001.

to be sufficient justification for selecting them for evaluation, particularly given the potential for access control bypass once the principle of modifying *xuda* files is established.

Still, Administrators are permitted to perform security-relevant configuration by unstructured, policy driven editing of flat files. By analogy, it is conceivable that instructing Administrators to follow the procedure outlined in the Administration Guide, to edit a set of *xuda* pages in order to enable generation of a CRL on any certificate status change, may be found to be acceptable by the evaluators. Nevertheless, in our judgment establishing the policy that files comprising the Administration and Enrollment console are not to be edited in a CC-evaluated configuration of RCM is a far less ambiguous stance than permitting just a certain list of files to be edited in a particular way. Generating CRLs on certificate status change is not a practice that would be recommended for most customers, and it useful mainly for testing. Conversely, some large commercial customers (who do not require CC certification) edit all the HTML and *xuda* files in order to customize and personalize the operation and appearance of RCM to their own corporate standards. Such customers are responsible for the security of their deployment, but anyone depending on an evaluated product must accept some restriction on user customization.

11.2 Trusting External CAs

See the Administration Guide Chapter 15 *Trusting External CAs* for background information on this functionality. There are several forms of “Trusting External CAs”. All have a similar goal, which is that an instance of RCM can be configured to share user and system information with another instance of RCM, in such a way that users of the “client” instance of RCM can query it for status information about certificates issued by a CA hosted in the “server” instance of RCM. Note that any instance of RCM can be either “client” or “server” in this arrangement, and in fact, 2 instances can each be a client of the other for this purpose. Bearing in mind that RCM takes the somewhat unusual approach of permitting multiple CAs to be hosted in a single instance of RCM, trusting an external CA has the effect of making a CA in the remote instance of RCM appear to be hosted in the local instance of RCM, from an end-entity perspective. From an Administrator perspective, trusted external CAs can be suspended, reinstated or revoked as if local CAs, but they cannot be used to issue certificates. This is a mechanism to enable end-entities to trust certificates for authentication of subjects that have been issued by remote CAs with which they, individually, have no trust relationship.

This functionality is unique to RSA’s Certificate Manager. It is not shared by other vendors of PKI systems, nor is it the trust arrangement envisioned by the author(s) of the CIMC Protection Profile. Technically there is little doubt that the “trusting external CA” functions can be evaluated and shown to provide secure transport of user and system information to and from a remote trusted system. The “server” RCM interface is the TLS-LDAP interface by which the Web Front End connects to the PKI Server, and is currently treated strictly as an internal interface of the TOE. The “client” (unexported) interface is not documented in the CC evidence, since it has no other function than its use in enabling trust for external CAs.

In the general PKI world, trust between clients of remote CAs is normally enabled through cross-certification of CAs, accompanied by certificate signature chain validation and status queries via OCSP or CRLs. Trusting external CAs was developed by Xcert International, Inc., and incorporated into RSA Certificate Manager. Despite being efficient and interesting, it is not the common way to handle trust management. Time

and resource constraints, accompanied by the likelihood of limited demand for this function, convinced RSA to exclude the TLS-LDAP server interface as an external interface of the TOE. It may be introduced in a future evaluation.

11.3 Enrollment Servers

In addition to the normal use of RCM's certificate registration functions (Vettor console), the RCM distribution includes several optionally enabled enrollment servers. While any of them can be configured to accept certificate requests that are subsequently acted upon by a Vettor, their real utility is for automated certificate enrollment (enrollment with auto-vetting, i.e. no human Vettor involved). In general, a customer wishing to use one of these facilities is most likely to wish to implement auto-enrollment for low-security certificates, an application not requiring a CC-validated CIMC. See the Administration Guide Chapter 21 *Certificate Enrollment Protocols*, Subsection "Autovetting of Certificate Requests".

The Evaluators have observed that excluding the CMP, SCEP and CRS servers seems to involve entirely disabling certain interfaces, and question whether there other impacts to the interfaces based on disabling these features. CMP is a standalone server subsystem (running in its own process) that implements a TCP/IP interface for the CMP protocol. It communicates with RCM by means of the same TLS-LDAP interface by which the Web Front End connects to the PKI Server. When the CMP server is disabled, there is no effect on RCM itself except to remove one client of the PKI Server TLS-LDAP interface. SCEP and CRS protocols are handled by modules in the webserver that embodies the Web Front End. They appear as additional virtual hosts ("vhosts") in the webserver configuration file. Vhosts in the Apache httpd webserver are designed to have as little interaction with one another as possible, and disabling these two vhosts has no effect on the Consoles provided by the Web Front End.

11.3.1 One-Step CGI Program

One-Step is implemented as a CGI program that runs in a webserver – typically, though not necessarily, the RCM webserver that hosts the Web Front End. See the Administration Guide Chapter 21 *Certificate Enrollment Protocols*, Subsection "RSA OneStep CGI Program". It is not, strictly speaking, an enrollment program, but rather a module that facilitates autovetting using authentication plugins. Its purpose is to retrieve information about a potential certificate subject from a 3rd party database, in order to fill in the required fields of a certificate request automatically, without intervention by the subject. It also retrieves shared secret information from the external database, typically an LDAP UserID and password, to allow the subject to authenticate to the CA. It can be used for bulk certificate issuance (i.e. "Issue a certificate to every employee with an entry in this LDAP directory"). It requires customers to write custom plugins to access whatever database or directory contains the authentication information, in whatever form it is stored. It runs in the same process as the webserver, so when used with the Web Front End webserver, it introduces untested, untrusted customer code into the TOE. For this reason, it is not a suitable candidate for CC evaluation against the CIMC PP.

11.3.2 CMP Server

CMP (Certificate Management Protocol) is an IETF standard enrollment protocol (RFC2511/RFC2511bis). Its purpose is to provide automated certificate enrollment to trusted remote entities. It would be a suitable candidate protocol for a Registration Authority to use in issuing and managing certificates at a Certification Authority. RSA provides an optional CMP server module, which implements a subset of the full CMP

protocol – see the Administration Guide Chapter 21 *Certificate Enrollment Protocols*, Subsection “Certificate Management Protocol”. Like SCEP, CMP is most commonly employed by automated equipment (such as routers) that use certificate-based authentication as part of network security. It uses authentication plugins (the Administration Guide provides instructions for configuring it to work with the One-Step CGI program) so it is not a good candidate for CC evaluation against the CIMC PP, and is unlikely to be used by a customer who needs a CC-certified CIMC. Additionally, this server is implemented as an RCM API application that functions as a “gateway” to the PKI server. It is responsible its own access control, independent of the Web Front End. It has not been analyzed to know whether it is consistent with PP SFRs, but evaluation would be a significant effort.

11.3.3 SCEP Server

SCEP (Simple Certificate Enrollment Protocol) is an earlier automated enrollment protocol developed by Cisco. It has been in the IETF standardization process for some years but has not yet been standardized (the 13th draft specification recently expired). It fulfills the same functions as CMP, and has the same benefits and liabilities. Its external interfaces differ, in that it operates as a module in the Web Front End and uses the webserver HTTP interface. It shares the webserver client TLS-LDAP interface to the PKI Server. It was excluded for most of the same reasons given for the CMP Server (above).

11.3.4 CRS Server

CRS (Certificate Request Syntax) is an older enrollment protocol that was introduced primarily for backward compatibility with some VPN and other network clients – see Chapter 21 *Certificate Enrollment Protocols*, Subsection “Certificate Request Syntax”. Unlike the previously discussed enrollment protocols, CRS is not intended for automated enrollment procedures, and auto-vetting is not supported for CRS by RCM. It is basically a means of transporting PKCS#10 certificate requests from an application to RCM, as well as providing a certificate revocation request message. The CRS server has not been analyzed to know whether its design makes it a suitable evaluation candidate. Given the limited deployment of this protocol, and uncertain future (in competition with CMP in particular), it was felt that including it in the CC evaluation was unlikely to be of benefit to those customers who require a CC evaluated CIMC, and inclusion was unlikely to drive any product sales.

11.4 Xudad Database Plugin API

The Xudad Database Plugin API is an unsecured, internal interface of the TOE. It provides a client (therefore unexported) interface which can optionally be used by the PKI Server to connect to alternative database modules in the TOE. Because it is a plugin API, it can only access other server modules when these have been explicitly linked and configured by Administrators. It is not possible for either a remote or local attacker to use it without having superuser privileges on the operating system of the computer that hosts RCM.

Whatever module the Database Plugin API links to runs in the same process, e.g. is part of the PKI server subsystem. Therefore, no untrusted, unevaluated module can be employed. This API was originally developed in answer to customer requests to be able to use arbitrary external databases or directory servers as a PKI repository. While this makes sense in many commercial enterprises, it is generally incompatible with a highly secured installation. As a compromise, RSA developed a default plugin (the *PKI Server*

External TLS-LDAP Directory Client; see the Functional Specification, Section 4.7) for this API that provides a secure connection to an external LDAP directory server. The TLS-LDAP Directory Client is the external interface corresponding to the Xudad Database Plugin API, and is part of the CC evaluation.

11.5 Use of Private Keys in Software

Evaluators have observed that "It is not clear these really conflict with CIMC PP SFRs, though a number of currently unapplied requirements added when dealing with software would come into play."

It is true that the CIMC PP does not explicitly prohibit the use of software cryptographic providers for any cryptographic function in a CIMC. That, however, is because the PP defers to FIPS validation when specifying cryptographic strength of function for secret and private key generation and storage. Table 9 *FIPS 140-1 Level for Validated Cryptographic Module* from the PP Section 7.2.2 "Cryptographic module levels for cryptographic functions that involve private or secret keys" is reproduced below:

Category of Use	**CIMC Security Level 1**	**CIMC Security Level 2**	**CIMC Security Level 3**	**CIMC Security Level 4**
Certificate and Status Signing				
- single party signature	1	2	3	4
- multiparty signature	1	2	2	3
Integrity or Approval Authentication				
- single approval	1	2	2	3
- dual approval	1	2	2	2
General Authentication	1	2	2	2
Long Term Private Key Protection	1	2	3	4
Long Term Confidentiality	1	2	2	2
Short Term Private key Protection	1	1	2	2
Short Term Confidentiality	1	1	1	2

At Security Level 3 we note that private keys used for certificate and status signing must be stored and used within a module validated at FIPS 140-1/2 Level 3. Consulting the NIST Cryptographic Module Validation Program database, we see that of 720 FIPS 140-1 and FIPS 140-2 certificates, just 25 have been issued to software modules at overall Level 2 and none at overall Level 3. This gives some indication of the difficulty of validating cryptographic software running on a general purpose computer under FIPS 140-1/2 above Level 1. Moreover, the issue is not whether **any** software cryptographic provider could legitimately be used, but whether the built-in RCM software cryptographic provider may be used for private key storage and private key signing operations. RCM software cryptography (except for the CryptoPro Cryptographic Service Provider) is performed by the RSA BSAFE Crypto-C library. Crypto-C has been submitted for FIPS validation and certified to FIPS 140-1 Level 1. CryptoPro has not been evaluated under the FIPS cryptographic module validation program. The only alternative to the use of the built-in software cryptographic provider is an external hardware security module. Based on these observations, we stand by the claim that RCM can only be CC evaluated when configured with an HSM that has been validated to an appropriate FIPS 140-1/2 level.

11.6 Configuring Unattended Startup and Operation

The Administration Guide provides instructions for enabling unattended startup of RCM. This mode of operation is useful when RCM runs unattended, often the case in a commercial enterprise where it may be called upon to provide CRLs and accept certificate requests, certificate renewal requests and revocation requests at any time, even when Administrative personnel are not present. If the RCM instance is inadvertently shut down temporarily, for instance due to power failure, it is desirable for it to restart and begin functioning even when no Administrator is present to provide the passwords it needs to access system private keys and cryptographically protected storage. In order to allow unattended startup, all configurations of RCM need to use "TLS Passphrases in `startup.conf`". CA private keys are normally protected either in an HSM or by software encryption, and in either case a PIN is required whenever a private key operation is invoked. PIN provision can be automated by "CA Private Key PIN in `setpin` directive". In the first case, a secret passphrase or password is stored in a system file *en clair*, while in the second case a PIN is stored in the same manner.

Whether or not such configurations are contrary to the PP security functional requirements depends on the distinction between passwords and secret keys. The PP Table 9 shown above requires FIPS 140-1/2 Level 2 protection for keys that are used for general authentication, which is a reasonable summary of the purpose of TLS private-key passphrases and CA private key PINs in RCM – the intention is that only legitimate Administrators should be able to start RCM in execution. It has been argued that secret passwords are not secret keys, and that the PP places no explicit requirements on handling passwords. We do not make that argument to justify these modes of operation for a CC-evaluated CIMC, rather we claim that such configuation is excepted from evaluation.

11.7 Local LDAP Publication

For a discussion of local LDAP publication, see the Administration Guide Chapter 19 *Certificate and Revocation List Publishing*, Subsections "Configuring CAs to Locally Publish Complete CRLs for LDAP Retrieval", "Configuring CAs to Locally Publish Delta CRLs for LDAP Retrieval" and "Configuring CAs to Locally Publish ARLs for LDAP Retrieval".

As described by the Administration Guide: "For local LDAP-based complete CRL publishing, complete CRLs are published to the Secure Directory in DER format. The location of the complete CRL in the Secure Directory corresponds to the subject DN of the CA certificate for which complete CRL publishing has been enabled". It is the view of the software engineers involved with RSA's CC evaluation process that the local LDAP directory (a.k.a. "Secure Directory) should be treated strictly as an internal database. It should not be opened up to access by unsecured channels. CRLs are public documents, and CRL retrieval is normally available to any end-entity, without requirement for authentication. When local LDAP publication is enabled, there is no (RCM-mediated) control over who can open an LDAP connection to the Secure Directory, search for and retrieve CRLs. In a perfectly secure system, this would not be a concern. In reality, making unsecured public access to the secure directory available removes all but one layer of a layered security approach., and exposes the system to any new attack that might be found against LDAP directories. For this reason, the Functional Specification treats the Secure Directory as an internal module of the PKI server subsystem.

Security-conscious enterprises tend to deploy their CAs on internal subnets behind one or more firewalls, while publication directory servers are more likely to be exposed within a DMZ accessible from a low-security internal network, or even from a public network. Local LDAP publication is available for small customers that have neither the interest nor the expertise to set up external LDAP directory servers for public CRL and certificate retrieval. This scenario is not what we expect for customers who need to set up their PKI in conformance with the CIMC PP. It is doubtful whether any enterprise customer uses this feature, except possibly during product pre-purchase evaluation. The preferred means of CRL publication – publication to an external LDAP directory and web publication – are part of this evaluation. See the Functional Specification, Section 4.6 *PKI Server LDAP-based Publishing Client Interface* and Section 4.4 *PKI Server Web-based Publishing Server Interface*, respectively.

In summary, while agreeing that it is not clear that local LDAP publication conflicts with PP SFRs, we believe enabling it is not the best security practice and should not be part of a CC evaluation.

11.8 Multiple Administrative Roles per Certificate

Some RSA customers that use RCM are small organizations without dedicated security staff, and RCM is installed and managed by IT personnel. In such instances, mutually exclusive role assignments would be bypassed (for instance, by issuing different identities to a single administrator) and would still result in inconvenience for the customer. For this reason, RCM has the capability that an Administrator can assign a particular identity to more than one role.

This is, however, clearly prohibited by the SFRs in the PP that define role assignment. No individual may be assigned more than one role in the system. For this reason, RCM's capability for multiple role assignment is excluded from the CC evaluation, and policy guidance must be established to prevent its use in a PP-compliant installation of the TOE.