Microsoft Windows Server 2003 Certificate Server Security Target

(EAL4 augmented with ALC_FLR.3 and AVA_VLA.4)

Revision 1.0
April 1, 2007

Prepared for:

Microsoft Corporation

Corporate Headquarters
One Microsoft Way
Redmond, WA 98052-6399

Prepared by:

Science Applications International Corporation

Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

1.1 ST, TOE and Common Criteria (CC) Identification

ST Title – Microsoft Windows Server 2003 Certificate Server Security Target *(EAL4 augmented with ALC_FLR.3 and AVA_VLA.4)*

ST Version – Version 1.0

ST Date – April 1, 2007

TOE Identification – Microsoft Windows Server 2003 Certificate Server

CC Identification – Common Criteria for Information Technology (IT) Security Evaluation, Version 2.1, August 1999, International Organization for Standardization (ISO)/International Electro-technical Commission (IEC) 15408.

1.2 Conformance Claims

This TOE conforms to the following CC specifications:

- CC for IT Security Evaluation Part 2: Security Functional Requirements (SFRs), Version 2.1, August 1999, ISO/IEC 15408-2.
    - Part 2 extended
- CC for IT Security Evaluation Part 3: Security Assurance Requirements (SARs), Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 conformant
    - Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.3 and AVA_VLA.4.
- Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile (PP), Version 1.0, October 31, 2001.

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the ST.

1.3.1 Conventions

The following conventions have been applied in this document:

- All requirements in this ST are reproduced relative to the requirements defined in CC v2.1.
- SFRs – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, a letter placed at the end of the component indicates iteration. For example FMT_MTD.1 (a) and FMT_MTD.1 (b) indicate that the ST includes two iterations of the FMT_MTD.1 requirement, a and b.

- Assignment: allows the specification of an identified parameter.
- Selection: allows the specification of one or more elements from a list.
- Refinement: allows the addition of details.

The conventions for the assignment, selection, refinement, and interaction operations are described in Section 5.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

See sections 10 (Glossary of Terms) and 11 (Acronyms).

1.4 ST Overview and Organization

The Microsoft Windows Server 2003 Certificate Server TOE, henceforth referred to as the Microsoft Certificate Server or TOE, is a CIMC that facilitates the use of public key cryptography by issuing, revoking, and managing public key certificates and certificate status information. The TOE supports the following security functionality: control of access to the certificate services (access control), unambiguous identification of the person and/or entity performing CIMC functions (identification and authentication), recognition of distinct roles to maintain the security of the CIMC (Security Management or Roles), audit generation (Audit), backup and recovery procedures (Backup & Recovery), protection of data imported and exported (Remote Date Entry & Export), use of Federal Information Processing Standard (FIPS) 140-1 Level 3 validated cryptographic security modules for protection of security critical keys (Key Management), and management of certificates (Certificate Management). These capabilities are provided within an enterprise network of computers running evaluated Microsoft Windows 2003 Server and Microsoft Windows/XP operating systems.

The ST contains the following additional sections:

- TOE Description (Section 2) – Provides an overview of the TOE Security Functions and boundary.
- Security Environment (Section 3) – Describes the threats, organizational security policies and assumptions that pertain to the TOE.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- IT Security Requirements (Section 5) – Presents the security functional and assurance requirements met by the TOE and the TOE environment.
- TOE Summary Specification (Section 6) – Describes the security requirements provided by the TOE to satisfy the security requirements and objectives.
- PP Claims (Section 7) – Presents the rationale concerning compliance of the ST with the CIMC Security Level 3 PP.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and TOE Summary Specifications (TSS') as to their consistency, completeness and suitability.
- Access control policies (Section 9) – Presents the TOE and TOE environment access control policies.
- Glossary of terms (Section 10) – Presents the definition of terms
- Acronyms (Section 11) – Presents the definition of acronyms.

2. TOE Description

This section provides a general overview of the Microsoft Certificate Server to aid customers in determining whether this TOE meets their needs.

2.1 Product Type

The Microsoft Certificate Server implements a Public Key Infrastructure (PKI) that issues and manages public key certificates to facilitate the use of public key cryptography. To achieve this goal, the Microsoft Certificate Server implements the following core functional components:

- Policy-based generating and distributing Public Key (including X.509) Certificates to bind user public keys to other information after validating the accuracy of the information provided
  - Certificate Enrollment or Request based on
    - Public Key Certificate Standard (PKCS) #7 (Cryptographic Message Syntax Standard),
    - PKCS #10 (Certification Request Syntax Standard),
    - Request for Comment (RFC) 2797 Certificate Management protocol using Content Management System (CMS) (CMC) (Certificate Management Messages over Cryptographic Message Syntax)
  - Certificate Renewal
  - Certificate Revocation
  - Certificate Retrieval
  - Request Pending Management
- Maintaining and distributing certificate status information for unexpired certificates
  - Certification and Certificate Revocation List (CRL) Management
- Certificate database backup and restore
- Security configuration and management of Microsoft Certificate Server

Microsoft Certificate Server has passed the "insider" Federal Bridge Certificate Authority (CA) interoperability test plan (see http://www.cio.gov/fbca/documents/fbca_testplan9-17-01.htm for further details).

The TOE is comprised of the executables and Dynamic Link Library (DLLs) that implement certificate issuance enforcement, certificate and CRL publication, a database manager, and several Microsoft Management Console (MMC) snap-ins (CA, Certificate Server, and Certificate Template). To interact with the services of the aforementioned functional components, the TOE provides authorized users of different roles with Graphical User Interface (GUI) based and command-line based tools that can be executed remotely or locally. These tools use the underlying network based programmatic interfaces implemented by the TOE. This set of programmatic interfaces is capable to support automatic certificate enrollment for both user and computer accounts defined for a distributed Windows Operating System (OS) environment within the same network of the TOE.

The Microsoft Certificate Server exceeds the CIMC Security Level 3 PP 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.

The Microsoft Certificate Server is available on a server class hardware running Microsoft Windows Server 2003 Enterprise Edition (32-bit) OS software. Additionally, the Microsoft Certificate Server must be installed in the Enterprise mode. -

2.2 Product Description

The Microsoft Certificate Server (the TOE) is packaged as a component of the Microsoft Server 2003 Enterprise Edition operating system. Specifically, the TOE is included in the following product:

- Microsoft Windows Server 2003, Enterprise Edition (32-bit version); Service Pack (SP) 1

The following security updates must be applied:

MS05-042 – Vulnerabilities in Kerberos Could Allow Denial of Service (DoS), Information Disclosure, and Spoofing (899587)

MS05-039 – Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)

MS05-027 – Vulnerability in Server Message Block (SMB) Could Allow Remote Code Execution (896422)

A hotfix that updates the Internet Protocol (IP) Security (IPSec) Policy Agent is available for Windows Server 2003 and Windows XP (907865)

The TOE is installed by selecting the Certificate Services windows component from the Add/Remove Windows Components Wizard. (See section 2.4 Security Environment TOE Boundary for more information on the differences between the TOE and the IT Environment.)

An enterprise CA should be used, if

- A large number of certificates should be enrolled and approved automatically,
- Availability and redundancy is mandatory,
- Clients requesting certificates wish to benefit from Active Directory (AD) integration, and
- Features, like auto-enrollment or modifiable certificate templates to define certificates being issued are required.

2.3 Product Features

This section lists and describes, at a high level, the services that are provided by the TOE. Each of these service areas is further defined and mapped to requirements in Section 6, TSS.

2.3.1 Identification

The TOE in conjunction with the IT Environment ensures that users are identified before they can access any other security relevant services. All local or remote communications with the TOE are completed over Kerberos-enabled secure Distributed Component Object Model (COM) (DCOM) channels which require the client to be known to the IT Environment prior to allowing the communication channel to be established. The IT Environment enforces the Identification and Authentication (I&A) prior to allowing any security services to be available to users.

2.3.2 Access Control

The TOE enforces user roles and access control whenever users access TOE-provided services. To enforce its security policy, the TOE enforces roles through the use of IT Environment policies and TOE managed Access Control Lists (ACLs). IT Environment administrators are responsible for assigning users IT Environment policies and Certificate Administrators are responsible for defining the access control lists maintained by the Microsoft Certificate Server. Access Control is primarily enforced by ensuring a user is mapped to a role before any security relevant operation is performed.

2.3.3 Roles

The TOE uses the access control functions to control the actions of administrative personnel. In order to accomplish this, predefined access control lists are assigned to the applicable services.

2.3.4 Security Audit

By using the auditing infrastructure of the IT Environment, the TOE has the capability to generate audits for security relevant events associated with the services that it provides. Certificate issuance and management related audit records (including the responsible user, date, time, and other details) are generated when their associated audit events occur inside the TOE. The TOE tracks actions taken to a certificate (creation, revocation, publication, request pending, and request denial), changes to user's roles and access, certificate database backup and restore operations, and modifications to the TOE configuration. After receiving the audit records from the TOE, the IT Environment audit infrastructure protects them, together with other IT Environment security relevant audit records, in its in-memory audit queue. Concurrently, the IT Environment empties its audit queue by writing the queue elements to a persistent audit log file that it has opened executively for its own access only during system boot.

2.3.5 Backup & Recovery

The TOE has a backup/restore service for its certificate database that can be used by an authorized user to save a snapshot of it and then restore the certificate database at a later date.

2.3.6 Remote Certificate Request Data Entry & Certificate and Certificate Status Export

The TOE processes certificate requests formatted according to the following standards, together with the identification function and Identification and Authentication (I&A) performed in the IT Environment, which provide the verification of origin framework for the TOE to follow:

- PKCS #7 (Cryptographic Message Syntax Standard),
- PKCS #10 (Certification Request Syntax Standard),
- RFC 2797 CMC (Certificate Management Messages over Cryptographic Message Syntax).

The TOE generates certificates and CRLs according to the following standard which provides a verification of origin framework for users of certificates and CRLs to follow:

- RFC 3280 Internet X.509 PKI Certificate and CRL Profile.

The CRLs generated by the TOE are in a format specified in RFC 3280 with the following exception: the critical Issuing Distribution extension is not asserted in specific circumstances when the CRL does not cover certificates where the CA key signing the certificates is different from the CA key signing the CRL. Thus, in order to ensure the security of PKI, the relying parties using these CRLs must ensure that CRL is signed using the same key as the certificate whose revocation status is being checked.

In the evaluated configuration, the TOE does not verify signatures or perform certificate path validation on certificates or certificate revocation lists produced by third parties.

2.3.7 Key Management

The TOE uses a hardware cryptographic service module for a number of key management functions. In particular, security critical keys and other information are protected by either encrypting it or storing it within a hardware cryptographic service module. Digital signatures are used when appropriate to ensure the integrity of key management related information.

2.3.8 Certificate Management

The TOE includes a number of certificate management functions. In particular, administrators can control, limit, or mandate values in certificates and CRLs.

2.3.9 Certificate Templates for Certificate Profile Management

Certificate templates define the attributes for certificate types. Authorized users can configure the TOE to issue specific certificate types to authorized users and computers. When the TOE creates a certificate, a corresponding certificate template is used to specify its attributes, such as the authorized uses for the certificate, the cryptographic algorithms that are to be used with it, the public key length, and the certificate lifetime. Certificate templates are stored in AD and provide information for each of the certificate types. The TOE queries the AD for the set of templates that it uses for issuing certificates. A number of pre-configured, commonly used certificate templates are available.

2.3.10 Qualified Subordination

Qualified subordination allows cross-certification of CA certificates with constraints (name and policy constraints) and provides for more granular control of certificate trusts. With qualified subordination an authorized administrator can also include or exclude certificate purposes (through the use of Microsoft private extension: application policies). In order for a certificate to be acceptable for an application, the application policy OID (if present) must be present in all the certificates in the certificate chain. Thus, through the use of application polices, qualified subordination can be formed to reject IPSec usage with a third (3rd) party certificate but allow secure email with the same certificate even if the certificates extended key usage and application policies would allow IPSec and secure email.

2.3.11 Role Separation

When Role Separation is enabled, which is required in the evaluated configuration, the TOE does not allow any user account to be assigned to more than a single role; each role must have a different account. The TOE enforces the actions for each role to be performed by accounts that have been assigned that specific role. The following roles are defined:

- Certificate Administrator,
- Officer,
- Auditor,
- Backup Operator, and
- Enrollee.

2.3.12 Support for Auto-Enrollment

As AD can define the permission for a specific account to enroll to a certificate template, the use of certificate templates in the TOE allows automatic certificate issuing based on the certificate profile information contained in a particular certificate template that a certificate requester has permission to enroll to.

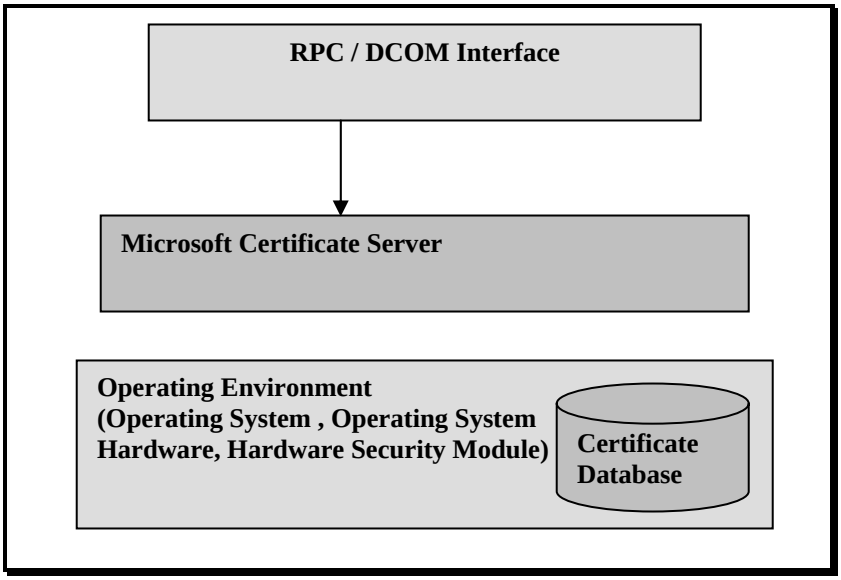
2.4 Security Environment TOE Boundary

The TOE includes both physical and logical boundaries.

2.4.1 Physical Boundaries

The TOE has two types of physical interfaces, the interface to its IT Environment and DCOM-based interfaces to access the security functions of the TOE. The TOE is not physically distributed.

The TOE exists as an application program interacting with other components to implement its security functions. In the above figure, the TOE is represented as the darker shading. All other components are considered to be located outside of the TOE in the IT Environment.



2.4.2 Logical Boundaries

Since the TOE is an application, its logical and physical boundaries largely coincide. The TOE requires basic program execution, data storage support, and network connectivity services from its IT environment. The TOE uses Lightweight Directory Access Protocol (LDAP) connections to the IT environment for communication to the AD where the certificate database is stored. The DCOM TOE external interfaces are available for TOE users to request Microsoft Certificate Server operations to be performed.

The TOE is a service that is packaged with the Windows Server 2003 OS. The TOE is a subset of its product as described in Section 2.1, Product Type and provides the security features described in Section 2.3, Product Features using services from the environment as described in 2.4.3 Non-TOE Boundary.

2.4.3 Non-TOE Boundary

The IT Environment of the TOE is the Windows Server 2003 OS on which the TOE software is running and FIPS 140-1 Level 3 validated hardware cryptographic security modules.

2.4.3.1 OS

The TOE relies upon the OS upon which the TOE is installed (Windows Server 2003 Operating System) to perform the following security functions: I&A; Audit; Security Management.

In addition to the security functions, the TOE relies upon of Windows Server 2003, the TOE also utilizes Windows 2003 Server features to perform its functions. Windows Server 2003 provides DCOM facilities leveraged by the TOE to secure the communications to the TOE. The TOE stores certificate templates in the Windows Server 2003 AD (Certificate Database) and uses roles defined by Windows Server 2003 (e.g. Backup Operator, Auditor).

2.4.3.2 Hardware Cryptographic Security Module (HSM)

The TOE relies on FIPS 140-1 Level 3 validated cryptographic security modules for key generation for certificates, key storage and key destruction through zeroization.

3. Security Environment

This section includes the following:

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

This information provides the basis for the Security Objectives specified in Section 4, the SFRs for the TOE and environment specified in Sections 5.1 and 5.2, and the TOE SARs specified in Section 5.3.

3.1 Secure Usage Assumptions

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

3.1.1 Personnel Assumptions

A.Auditors Review Audit Logs

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

A.Authentication Data Management

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

A.Competent Administrators, 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 Physical Assumptions

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.

3.1.3 Connectivity Assumptions

A.Operating System

The OS 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.[1]

3.2 Threats

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

3.2.1 Authorized Users

T.Administrative errors of omission

Administrators, 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

[1] This assumption has been copied directly from the CIMC PP. In the context of this ST, "appropriate Security Level identified in this family of PPs" reflects Security Level 3 as represented by this ST.

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

3.2.3 Cryptography

T.Disclosure of private and secret keys

A private or secret key is improperly disclosed.

T.Modification of private/secret keys

A secret/private key is modified.

T.Sender denies sending information

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

3.2.4 External Attacks

T.Hacker gains access

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

T.Hacker physical access

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

T.Social engineering

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

3.3 Organization Security Policies

P.Authorized use of information

Information shall be used only for its authorized purpose(s).

P.Cryptography

FIPS-approved or NIST[2]-recommended cryptographic functions shall be used to perform all cryptographic operations.

4. Security Objectives

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

4.1 Security Objectives for the TOE

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

[2] National Institute of Standards and Technology (NIST)

4.1.1 Authorized Users

O.Certificates

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

4.1.2 System

O.Preservation/trusted recovery of secure state

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

O.Sufficient backup storage and effective restoration

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

4.1.3 Cryptography

O.Non-repudiation

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

4.1.4 External Attacks

O.Control unknown source communication traffic

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

4.2 Security Objectives for the Environment

This section specifies the security objectives for the environment.

4.2.1 Non-IT security objectives for the environment

O.Administrators, 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 on a frequency sufficient to address level of risk.

O.Authentication Data Management

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

O.Communications Protection

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

O.Competent Administrators, 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 CP and the 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 nonbypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology.

O.Periodically check integrity

Provide periodic integrity checks on both system and software.

O.Security roles

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

O.Validation of security function

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

O.Trusted Path

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

O.Time stamps

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

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.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.

4.3 Security Objectives for both the TOE and the Environment

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

O.Configuration Management

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

O.Data import/export

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

O.Detect modifications of firmware, software, and backup data

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

O.Individual accountability and audit records

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

O.Integrity protection of user data and software

Provide appropriate integrity protection for user data and software.

O.Limitation of administrative access

Design administrative functions so that Administrators, 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.Require inspection for downloads

Require inspection of downloads/transfers.

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.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. IT Security Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class.

Requirement Operations:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - For operations performed while incorporating requirements from the CIMC PP the following conventions were used:
        - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
        - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that in cases where a selection operation is combined with an assignment operation and the assignment is null, the assignment operation is simply deleted leaving on the completed selection to identify the combination of operations.
        - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
        - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").

- For operations already performed in the CIMC PP the conventions from the PP have been used:
  - Assignment, Selection, and Refinement: indicated with underlined text.
  - Iteration: the title is followed by an iteration number (e.g., iteration 1).

Interpreted Requirements:

- Requirements that have been modified based upon an International Interpretation are identified by an italicized parenthetic comment following the requirement element that has been modified (e.g. *(per International Interpretation #51)*).

5.1 Security Requirements for the IT Environment

This section specifies the SFRs that are applicable to the IT environment.

Table 1 IT Environment Functional Security Requirements

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation (iteration 1)
	FAU_GEN.2 User Identity Association (iteration 1)
	FAU_SAR.1 Audit Review
	FAU_SAR.3 Selectable Audit Review
	FAU_SEL.1 Selective Audit (iteration 1)
	FAU_STG.1 Protected Audit Trail Storage (iteration 1)
	FAU_STG.4 Prevention of Audit Data Loss (iteration 1)
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic Key Generation
	FCS_CKM.4 Cryptographic Key Destruction
	FCS_COP.1 Cryptographic Operation
User Data Protection (FDP)	FDP_ACC.1 Subset Access Control (iteration 1)
	FDP_ACF.1 Security Attribute Based Access Control (iteration 1)
	FDP_ITT.1 Basic Internal Transfer Protection (iterations 1 and 2)
	FDP_UCT.1 Basic Data Exchange Confidentiality (iteration 1)
Identification and Authentication (FIA)	FIA_AFL.1 Authentication Failure Handling
	FIA_ATD.1 User Attribute Definition
	FIA_UAU.2 User Authentication Before any Action (iteration 1)
	FIA_UID.2 User Identification Before any Action (iteration 1)
	FIA_USB.1 User-subject Binding (iteration 1)
Security Management (FMT)	FMT_MOF.1 Management of Security Functions Behavior (iteration 1)
	FMT_MSA.1 Management of Security Attributes
	FMT_MSA.2 Secure Security Attributes
	FMT_MSA.3 Static Attribute Initialization
	FMT_MTD.1 Management of TSF Data
	FMT_SMR.2 Restrictions on Security Roles
Protection of the TSF (FPT)	FPT_AMT.1 Abstract Machine Testing
	FPT_ITC.1 Inter-TSF Confidentiality During Transmission (iteration 1)
	FPT_ITT.1 Basic Internal TSF Data Transfer Protection (iterations 1 and 2)
	FPT_RVM.1 Non-bypassability of the TSP (iteration 1)
	FPT_SEP.1 TSF Domain Separation
	FPT_STM.1 Reliable Time Stamps (iteration 1)
	FPT_TST_CIMC.2 Software/Firmware Integrity Test
	FPT_TST_CIMC.3 Software/Firmware Load Test
Trusted Path/Channels (FTP)	FTP_TRP.1 Trusted Path

5.1.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation (iteration 1)

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, 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.

Table 2 Auditable Events and Audit Data

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

FAU_GEN.2 User identity Association (iteration 1)

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.

FAU_SAR.1 Audit Review

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.

FAU_SAR.3 Selectable Audit Review

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.

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)

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) [**none**].

FAU_STG.1 Protected Audit Trail Storage (iteration 1)

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 **prevent** ~~detect~~ ~~unauthorized~~ modifications to the audit records. *(per International Interpretation #104).*

FAU_STG.4 Prevention of Audit Data Loss (iteration 1)

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

5.1.2 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The FIPS 140-1 validated cryptographic module shall generate cryptographic keys in accordance with [**DES, TDES, and DSS**] that meet the following: [**FIPS 46-3 for DES and TDES, and FIPS 186-2 for DSA and RSA**].

FCS_CKM.4 Cryptographic Key Destruction

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

FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 **The FIPS 140-1 validated cryptographic module shall perform [encryption, decryption, signing, verifying, hashing, random number generation] in accordance with [the following standards: FIPS 46-3 DES and 3DES (encryption and decryption); FIPS 186-2 RSA and DSA with SHA-1 (signing and verifying); FIPS 180-2 (hashing); FIPS 186-2 DSA (random number generation)]**

5.1.3 User Data Protection (FDP)

FDP_ACC.1 Subset Access Control (iteration 1)

FDP_ACC.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section **9.1** on [**subjects: users; objects: files; operations: access to files**].

FDP_ACF.1 Security Attribute Based Access Control (iteration 1)

FDP_ACF.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section **9.1** to objects based on the following: the identity of the subject and the set of roles that the subject is authorized to assume. *(per International Interpretation #103)*

FDP_ACF.1.2 The IT environment shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: The capability to zeroize plaintext private and secret keys shall be restricted to Administrators, Auditors, 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**].

FDP_ITT.1 Basic Internal Transfer Protection (iteration 1)

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

FDP_ITT.1 Basic Internal Transfer Protection (iteration 2)

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

FDP_UCT.1 Basic Data Exchange Confidentiality (iteration 1)

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

5.1.4 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the IT environment shall [**disable the user account for an authorized administrator specified duration**].

FIA_ATD.1 User Attribute Definition

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, [**User Identifier and Group Memberships**].

FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The IT environment shall require each user to be successfully authenticated before allowing any other IT environment-mediated actions on behalf of that user.

FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The IT environment shall require each user to identify itself before allowing any other IT environment-mediated actions on behalf of that user**.**

FIA_USB.1 User-subject Binding (iteration 1)

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

5.1.5 Security Management (FMT)

FMT_MOF.1 Management of Security Functions Behavior (iteration 1)

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**.

Table 4 Authorized Roles for Management of Security Functions Behavior

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

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section **9.1** to restrict the ability to modify the security attributes [**user definitions and role assignments**] to Administrators.

FMT_MSA.2 Secure Security Attributes

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

FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in section **9.1** to provide [***restrictive***] 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.

FMT_MTD.1 Management of TSF Data

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

FMT_SMF.1 Specification of Management Functions (iteration 1)

FMT_SMF.1 The **IT environment** ~~TSF~~ shall be capable of performing the following security management functions: [**Security Audit, Identification and Authentication, Account Administration**]. *(per International Interpretation #065)*

FMT_SMR.2 Restrictions on Security Roles

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:

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.

Note: 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.

5.1.6 Protection of the TSF (FPT)

FPT_AMT.1 Abstract Machine Testing

FPT_AMT.1.1 The IT environment shall run a suite of tests [***other conditions*: during Windows Server 2003 Common Criteria evaluation**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the IT environment.

FPT_ITC.1 Inter-TSF Confidentiality During Transmission (iteration 1)

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.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection (iteration 1)

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.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection (iteration 2)

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.

FPT_RVM.1 Non-bypassability of the TSP (iteration 1)

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.

FPT_SEP.1 TSF Domain Separation

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.

FPT_STM.1 Reliable Time Stamps (iteration 1)

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

FPT_TST_CIMC.2 Software/Firmware Integrity Test

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 [**not enable the TOE**].

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC. It satisfies the security objective O.Integrity protection of user data and software and O.Periodically check integrity.

FPT_TST_CIMC.3 Software/Firmware Load Test

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 [**not enable the TOE**].

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by the CC. It satisfies the security objective O.Integrity protection of user data and software and O.Periodically check integrity.

5.1.7 Trusted Path/Channels (FTP)

FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The IT environment shall provide a communication path between itself and [***local***] 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 [***local 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 no other services**].

5.2 TOE SFRs

This section specifies the security requirements that are applicable to CIMC functionality, such as key management, certificate registration, and CIMC configuration and management functions.

Table 5 CIMC TOE Functional Security Requirements

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_GEN.1 Audit Data Generation (iteration 2)
	FAU_GEN.2 User Identity Association (iteration 2)
	FAU_SEL.1 Selective audit (iteration 2)
Communication (FCO)	FCO_NRO_CIMC.3 Enforced Proof of Origin and Verification of Origin
	FCO_NRO_CIMC.4 Advanced Verification of Origin
Cryptographic Support (FCS)	FCS_CKM_CIMC.5 CIMC Private and Secret Key Zeroization
User Data Protection (FDP)	FDP_ACC.1 Subset Access Control (iteration 2)
	FDP_ACF.1 Security Attribute Based Access Control (iteration 2)
	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 Status Export
	FDP_ETC_CIMC.5 Extended User Private and Secret Key Export
	FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action
Identification and Authentication (FIA)	FIA_UID.2 User Identification Before any Action (iteration 2)
	FIA_USB.1 User-subject Binding (iteration 2)
Security Management (FMT)	FMT_MOF.1 Management of Security Functions Behavior (iteration 2)FIA_USB.1 User-subject Binding (iteration 2)
	FMT_MOF_CIMC.3 Extended Certificate Profile Management
	FMT_MOF_CIMC.5 Extended Certificate Revocation List 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
Protection of the TSF (FPT)	FPT_RVM.1 Non-bypassability of the TSP (iteration 2)

5.2.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation (iteration 2)

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the minimum level of audit; and
c) The events listed in **Table 6** below.

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, the information specified in the Additional Details column in **Table 6** below.

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

Table 6 Auditable Events and Audit Data

Section/Function	Component	Event	Additional Details
Security Audit	FAU_GEN.1 Audit Data Generation (iteration 2)	Any changes to the audit parameters, e.g., audit frequency, type of event audited Any attempt to delete the audit log	
Local Data Entry		All security-relevant data that is entered in the system	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an “accept” button). This shall be included with the accepted data.
Remote Data Entry		All security-relevant messages that are received by the system	
Data Export and Output		All successful and unsuccessful requests for confidential and security-relevant information	
Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
Private Key Load		The loading of Component private keys	
Private Key Storage		All access to certificate subject private keys retained within the TOE for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
Secret Key Storage		The manual entry of secret keys used for authentication	
Private and Secret Key Export	FDP_ETC_CIMC.4 User private and secret key export;	The export of private and secret keys (keys used for a single session or message are excluded)	
Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).

Section/Function	Component	Event	Additional Details
Certificate Status Change Approval		All requests to change the status of a certificate	Whether the request was Accepted or rejected.
CIMC Configuration		Any security-relevant changes to the configuration of the TSF.	
Certificate Profile Management	FMT_MOF_CIMC.2 Certificate profile management; FMT_MOF_CIMC.3 Extended certificate profile management	All changes to the certificate Profile	The changes made to the Profile
Revocation Profile Management		All changes to the revocation profile	The changes made to the Profile
Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile

FAU_GEN.2 User identity Association (iteration 2)

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

FAU_SEL.1 Selective Audit (iteration 2)

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) [**none**].

5.2.2 Communication (FCO)

FCO_NRO_CIMC.3 Enforced Proof of Origin and Verification of Origin

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

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity and [**no other attributes**] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

FCO_NRO_CIMC.4 Advanced Verification of Origin

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

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

5.2.3 Cryptographic Support (FCS)

FCS_CKM_CIMC.5 CIMC Private and Secret Key Zeroization

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.

5.2.4 User Data Protection (FDP)

FDP_ACC.1 Subset Access Control (iteration 2)

FDP_ACC.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 on [subjects**: users; objects: certificate services; operations: access to certificate services**].

FDP_ACF.1 Security Attribute Based Access Control (iteration 2)

FDP_ACF.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section 9.2 to objects based on the following: the identity of the subject and the set of roles that the subject is authorized to assume. *(per International Interpretation #103)*

FDP_ACF.1.2 The TSF shall enforce the rules specified in **Table 7** to determine if an operation among controlled subjects and controlled objects is allowed.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [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**].

Table 7 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.
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.

Section/Function	Component	Event
Private Key Storage		The capability to request the decryption of certificate subject private keys shall be restricted to Officers. The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. At least two Officers or one Officer and an Administrator, **or** Auditor~~, 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, **or** 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, **or** Auditor~~, or Operator~~.
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.

FDP_ACF_CIMC.2 User private Key Confidentiality Protection

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.

FDP_ACF_CIMC.3 User Secret Key Confidentiality Protection

FDP_ACF_CIMC.3.1 User secret keys stored within the CIMC, but not within a FIPS 140-1 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-1 validated cryptographic module.

FDP_CIMC_BKP.1 CIMC Backup and Recovery

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.

FDP_CIMC_BKP.2 Extended CIMC Backup and Recovery

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.

FDP_CIMC_CER.1 Certificate Generation

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**.[3]
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**.

[3] The version of the TOE certificate standard is "3" which is compatible with 2, 1, and 0.

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.

FDP_CIMC_CRL.1 Certificate Revocation List Validation

FDP_CIMC_CRL.1.1 A TSF that issues CRLs shall verify that the following fields and extensions in any CRL issued contain values in accordance with RFC3280:

1. The **version** field shall contain the integer **2**.
2. The **issuer** field shall contain the issuing certificate authority's distinguished name (DN) represented using an X.500 DN.
3. The **signature** and **signatureAlgorithm** fields shall contain the OID for a FIPS-approved digital signature algorithm.
4. The **thisUpdate** field shall indicate the issue date of the CRL.
5. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.
6. The CRL Number extension shall indicate a monotonically increasing sequence number for each CRL being issued.
7. The authority key identifier extension shall contain a numeric representation of the issuer name and serial number from the CRL issuer's certificate as a means to identify the public key corresponding to the private key used to sign a CRL.
8. The freshest CRL extension shall contain the URLs to fetch the delta CRL.
9. There shall be a sequence of zero or more revoked certificates with the following fields represented for each revoked certificate.

9.a The certificate serial number field shall contain the serial number assigned by the issuing certificate authority for each revoked certificate.
9.b The revocation date field shall contain the date at which the revocation took place.
9.c The reason code field shall identify the reason for the certificate revocation, which may be Unspecified, KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation, CertificateHold, and RemoveFromCRL.

Application Note

The X.509 states that "if the distributionPoint field is absent, the CRL MUST contain entries for all revoked unexpired certificates issued by the CRL issuer, if any, within the scope of the CRL." The TSF does not use the IssuingDistributionPoint field. It does not have a concept of "scope of CRL", and it does not follow the CRL issuing logic of X.509 due to the absence of IssuingDistributionPoint. Instead, the TSF issues (at a specific time interval) a CRL for all its current revoked, not-yet-expired, certificates previously issued using the same key. The key used to sign the CRL is the same key previously used to sign the certificates residing in the CRL. The applicable CRL for a certificate can be obtained from the location pointed to by the CRL DP of the certificate.

FDP_CIMC_CSE.1 Certificate Status Export

FDP_CIMC_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with [**the X.509 standard for CRLs specified in RFC3280, except that the critical Issuing Distribution extension is not asserted in specific circumstances when the CRL does not cover certificates where the CA key signing the certificates is different from the CA key signing the CRL**].

FDP_ETC_CIMC.5 Extended User Private and Secret Key Export

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

FDP_SDI_CIMC.2 Stored Public Key Integrity Monitoring and Action

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 [**take no action**].

5.2.5 Identification and Authentication (FIA)

FIA_UID.2 User Identification Before any Action (iteration 2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject Binding (iteration 2)

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

5.2.6 Security Management (FMT)

FMT_MOF.1 Management of Security Functions Behavior (iteration 2)

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**.

Table 8 Authorized Roles for Management of Security Functions Behavior

Section/Function	Component Function	Authorized Role
Security Audit		The capability to configure the audit parameters shall be restricted to Administrators. The capability to change the frequency of the audit log signing event shall be restricted to Administrators.
Backup and Recovery		The capability to configure the backup parameters shall be restricted to Administrators. The capability to initiate the backup or recovery function shall be restricted to [**Administrators**].
Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers. If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Officers.

Section/Function	Component Function	Authorized Role
Data Export and Output		The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer, or Auditor~~, 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.2 Certificate profile management; FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administrators.
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.

FMT_MOF_CIMC.3 Extended Certificate Profile Management

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

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

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

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

- **keyUsage**;
- **basicConstraints**;
- **certificatePolicies**

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

FMT_MOF_CIMC.5 Extended Certificate Revocation List Profile Management

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

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

- **issuer;**
- **issuerAltName** (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within 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.

FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection

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.

FMT_MTD_CIMC.5 TSF Secret Key Confidentiality Protection

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.

FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export

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

FMT_SMF.1 Specification of Management Functions (iteration 2)

FMT_SMF.1 The TSF shall be capable of performing the following security management functions: [**Certificate registration, Certificate profile management, Certificate revocation list profile management, Revocation profile management**]. *(per International Interpretation #065)*

5.2.7 Protection of the TSF (FPT)

FPT_RVM.1 Non-bypassability of the TSP (iteration 2)

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.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 components as specified in Part 3 of the CC, augmented with ALC_FLR.3 and AVA_VLA.4 as indicated in bold in the following table. Note also that the EAL 4 requirements that exceed EAL 3 as augmented by the CIMC PP SL3 are indicated in italics in the following table. No operations are applied to the assurance components.

Table 9 Assurance Requirements (EAL 4 augmented)

Assurance Class	Assurance Components
Configuration Management (ACM)	*ACM_AUT.1 Partial CM Automation*
	ACM_CAP.4 Generation Support and Acceptance Procedures

Assurance Class	Assurance Components
	ACM_SCP.2 Problem Tracking CM Coverage
Delivery and Operation (ADO)	ADO_DEL.2 Detection of Modification
	ADO_IGS.1 Installation, Generation, and Start-up Procedures
Development (ADV)	ADV_FSP.2 Fully Defined External Interfaces
	ADV_HLD.2 Security Enforcing High-level Design
	ADV_IMP.1 Subset of the Implementation of the TSF
	ADV_LLD.1 Descriptive Low-level Design
	ADV_RCR.1 Informal Correspondence Demonstration
	ADV_SPM.1 Informal TOE Security Policy Model
Guidance Documents (AGD)	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Life Cycle Support (ALC)	ALC_DVS.1 Identification of Security Measures
	ALC_FLR.3 Systematic Flaw Remediation
	ALC_LCD.1 Developer Defined Life-cycle Model
	ALC_TAT.1 Well-defined Development Tools
Tests (ATE)	ATE_COV.2 Analysis of Coverage
	ATE_DPT.1 Testing: High-level Design
	ATE_FUN.1 Functional Testing
	ATE_IND.2 Independent Testing - Sample
Vulnerability Assessment (AVA)	AVA_MSU.2 Validation of Analysis
	AVA_SOF.1 Strength of TOE Security Function Evaluation
	AVA_VLA.4 Highly Resistent Vulnerability Analysis

5.3.1 Configuration Management (ACM)

ACM_AUT.1 Partial CM Automation

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_CAP.4 Generation Support and Acceptance Procedures

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labeled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4NewC The configuration list shall uniquely identify all configuration items that comprise the TOE. *(per International Interpretation #3)*

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem Tracking CM Coverage

ACM_SCP.2.1D The developer shall provide list of configuration items for the TOE. *(per International Interpretation #4).*

ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST. *(per International Interpretation #4).*

ACM_SCP.2.2C *(this element has been deleted per International Interpretation #4)*

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

ADO_DEL.2 Detection of Modification

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, Generation, and Start-up Procedures

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE. *(per International Interpretation # 51)*

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

ADV_FSP.2 Fully Defined External Interfaces

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security Enforcing High-level Design

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_IMP.1 Subset of the Implementation of the TSF

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

ADV_IMP.1.3C The implementation representation shall describe the relationships between all portions of the implementation.

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

ADV_LLD.1 Descriptive Low-level Design

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP enforcing and other modules.

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal Correspondence Demonstration

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM.1 Informal TOE Security Policy Model

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

AGD_ADM.1 Administrator Guidance

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User Guidance

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life Cycle Support (ALC)

ALC_DVS.1 Identification of Security Measures

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_FLR.3 Systematic Flaw Remediation

ALC_FLR.3.1D The developer shall provide flaw remediation procedures addressed to TOE developers. *(per International Interpretation #094)*

ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws. *(per International Interpretation #062)*

ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users. *(per International Interpretation #094)*

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquires of suspected security flaws in the TOE. *(per International Interpretation #094)*

ALC_FLR.3.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE. *(per International Interpretation #094)*

ALC_FLR.3.9C The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

ALC_FLR.3.10C The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections. *(per International Interpretation #094)*

ALC_FLR.3.11C The flaw remediation guidance shall identify the specific points of contact for all reports and enquires about security issues involving the TOE. *(per International Interpretation #094)*

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_LCD.1 Developer Defined Life-cycle Model

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_TAT.1 Well-defined Development Tools

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Security Testing (ATE)

ATE_COV.2 Analysis of Coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: High-level Design

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional Testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent Testing – Sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

AVA_MSU.2 Validation of Analysis

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE Security Function Evaluation

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.3.7.1 Highly Resistant Vulnerability Analysis (AVA_VLA.4)

AVA_VLA.4.1d The developer shall perform a vulnerability analysis.

AVA_VLA.4.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.4.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.4.2c The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.4.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.4c The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.5c The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.6c The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

AVA_VLA.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.4.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.4.3e The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.4.4e The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.4.5e The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

5.4 Strength of Function Requirements

The minimum Strength of Function (SOF) level for the TOE and IT environment functional security requirements is SOF-basic. The specific SOF is stated in this section for specific requirements.

5.4.1 Authentication Mechanisms

The authentication mechanisms specified in FIA_UAU.2 iterations 1 meets the following SOF requirements:

1. For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or Personal Identification Number (PIN), false acceptance error rate of a biometric device, or some combination of authentication methods.)

2. For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

5.4.2 Cryptographic Modules

FIPS 140-1 validated cryptographic modules perform all cryptographic functions performed by the CIMC. FIPS 140-1 validated cryptographic modules are used to generate cryptographic keys and store plaintext private and secret keys.

5.4.2.1 Encryption and FIPS 140-1 Validated Modules

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

5.4.2.1.1 Encryption Algorithms

The encryption specified for:

- FAU_STG.1 Protected Audit Trail Storage
- FCO_NRO_CIMC.4 Advanced Verification of Origin
- FDP_ACF_CIMC.2 User Private Key Confidentiality Protection
- FDP_ACF_CIMC.3 User Secret Key Confidentiality Protection
- FDP_CIMC_BKP.2 Extended CIMC Backup and Recovery
- FDP_ETC_CIMC.5 Extended User Private and Secret Key Export
- FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action
- FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection
- FMT_MTD_CIMC.5 TSF Secret Key Confidentiality Protection
- FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export
- FPT_TST_CIMC.2 Software/Firmware Integrity Test (TOE environment)
- FPT_TST_CIMC.3 Software/Firmware Load Test (TOE environment)

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

5.4.2.1.2 FIPS 140-1 Validated Cryptographic Modules

Cryptographic modules specified for:

- FCS_CKM.1 Cryptographic Key Generation (TOE environment)
- FDP_ACF_CIMC.2 User Private Key Confidentiality Protection
- FDP_ACF_CIMC.3 User Secret Key Confidentiality Protection
- FDP_ETC_CIMC.5 Extended User Private and Secret Key Export
- FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action
- FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection
- FMT_MTD_CIMC.5 TSF Secret Key Confidentiality Protection
- FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export

shall be validated against FIPS 140-1.

5.4.2.1.3 Split Knowledge Procedures

Split-knowledge procedures specified in:

- FDP_ETC_CIMC.5 Extended User Private and Secret Key Export
- FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export

shall be implemented and validated as specified in FIPS 140-1.

5.4.2.1.4 Authentication Codes

The authentication code specified in:

- FAU_STG.1 Protected Audit Trail Storage
- FCO_NRO_CIMC.4 Advanced Verification of Origin
- FDP_CIMC_BKP.2 Extended CIMC Backup and Recovery
- FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action
- FPT_TST_CIMC.2 Software/Firmware Integrity Test (TOE environment)
- FPT_TST_CIMC.3 Software/Firmware Load Test (TOE environment)

shall be a FIPS-approved or recommended authentication code.

5.4.2.2 Cryptographic Module Levels for Cryptographic Functions that Involve Private or Secret Keys

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

Table 10 specifies for each category of use for a private or secret key, the overall FIPS 140-1 level for the validated cryptographic module. The TOE does not generate subject certificate private keys, therefore, the *Long Term Private Key Protection* keys does not apply.

Table 10 FIPS 140-1 Level for Validated Cryptographic Module

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	N/A
Long Term Confidentiality	2
Short Term Private key Protection	2
Short Term Confidentiality	1

5.4.2.3 Cryptographic Functions That Do Not Involve Private or Secret Keys

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

1. *Hash Generation*: A one-way hash functions is used in the process of signature generation and verification (a signature is typically generated by applying a private key to the hash of the message). The generation of

a hash does not require a key. Therefore, hash generation does not have the same confidentiality requirements of other cryptographic functions.

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

The cryptographic modules that only perform signature verification and/or keyless hash generation functions are validated to FIPS 140-1 Level 1.

6. TOE Summary Specification

This chapter describes the Microsoft Certificate Services security functions and associated assurance measures. The Microsoft Certificate Server security functions and SAMs satisfy the security functional requirements of the CIMC Security Level 3 PP and exceeds the security assurance requirements of the CIMC Security Level 3 PP. The SFs and SAMs performed by the Microsoft Certificate Server are described in the following sections, as well as a mapping to the security functional and assurance requirement satisfied by the TOE.

6.1 TOE Security Functions

The section presents the TOE Security Functions (TSFs) and a mapping of SFs to SFRs. The TOE performs the following SFs:

- Identification,
- Roles,
- Access Control,
- Security Audit,
- Backup & Recovery,
- Remote Data Entry & Export,
- Key Management, and
- Certificate Management.

6.1.1 Identification

The TOE requires each user to be identified and authenticated prior to performing TSF-mediated functions on behalf of that user. The TOE requires any interaction with the TOE to be performed via the interfaces implemented over the IT environment provided secure DCOM. Enrolling for a certificate using the TOE's Certificate Server MMC snap-in GUI tool will only allow the user to request a new certificate from a CA in the user's own domain. Therefore, the user must be known to the domain which requires the user to be identified and authenticated before the CA will service the user's request. Upon a successful logon in the IT Environment, a process is created and assigned a token that defines a security context based on the attributes collected during the logon process (e.g. user identity and group identities). Each process, or thread within a process, in the IT environment has an associated token.

The TOE obtains the identification of the user (security identification or Security Identifier (SID)) from the calling process or thread that is requesting a service, referred to as the caller. The TOE uses the caller identification to perform its security checks to ensure the caller has the appropriate privilege or access permission to perform the requested service. For certificate requests, the TOE ensures the caller is the same as the certificate subject. Additionally, when a new certificate is requested or a certificate is requested to be renewed, the TOE verifies the digital signature included in the service request to ensure the caller has the private key associated with the public key included in the certificate request.

The TOE offers an auto-enrollment feature that will allow for the automatic submission of certificate request upon user logon. Additionally, the auto-enrollment feature allows for the TOE to be configured such that certificate request that are a result of the auto-enrollment are automatically approved and certificates issued instead of waiting for a certificate request to be approved.

SFR Mapping:

The **Identification** security function satisfies the following SFRs:

FIA_UID.2 (iteration 2) – The Microsoft Windows Server 2003 Certificate Server must be installed in *Enterprise Mode*. The TOE implements its only external interfaces via the IT environment provided DCOM. All users interacting with the TOE must be identified and authenticated by the TOE and the IT environment respectively. As a result, there will be no situations in which a non-identified and non-authenticated user can perform any action since all users must be authenticated to the domain during the network logon to the IT Environment on which the TOE resides.

- FIA_UID.2 (iteration 2) – The Microsoft Windows Server 2003 Certificate Server must be installed in *Enterprise Mode*. The TOE implements its only external interfaces via the IT environment provided DCOM. All users interacting with the TOE must be identified and authenticated by the TOE and the IT environment respectively.
- FIA_USB.1 (iteration 2) – Each process and thread has a token that identifies the responsible user (used for audit and access), associated groups (used for access), privileges, and logon rights held by that process or thread on behalf of the user. For each service request to the TOE, the TOE obtains the identification of the user from the calling process or thread (the SID). The TOE uses the caller identification which is then used by the TOE to obtain the user's privileges, associated groups, and, performs its access checks to determine if the requested service can be provided.

6.1.2 Roles

Security Management functions are supported by the TOE by providing functions to manage the various features provided by the TOE and restricting certain capabilities to specific roles of users. Additionally, the TOE relies on the IT Environment to create users and assign group and policy information to those users. The notion of a role within the TOE is generally realized by assigning group accounts and privileges to a given user account or by assigning specific permissions to user accounts. Whenever that user account is used to logon, the user will assume the role that corresponds with the combination of groups, privileges, or permissions that it holds. The TOE recognizes the following roles:

- **Certificate Administrator**: Certificate Administrators manage the Certificate Server. They can configure and maintain the Certificate Server. This includes the ability to assign all other Certificate Server roles and renew the CA certificate. Certificate Administrators are designated by assigning the Manage CA permission in the TOE's CA MMC snap-in.
- **Officer**: Officers (called Certificate Managers in the GUI) are responsible for the certificates in the Certificate Server. Officers are designated by assigning the Issue and Manage Certificates permission in the TOE's CA MMC snap-in. They can approve certificate enrollment and revocation requests. Officers can also submit certificate requests on behalf of users.
- **Auditor**: Auditors are responsible to view and interpret the Certificate Server audit records. This role is not assigned directly through the Certificate Server interface. Instead, Certificate Server will treat any user that has the IT Environment policy *Manage Auditing and Security Log* privilege as an Auditor
- **Backup Operators**: Backup Operators are responsible for backup and restoration of Certificate Server. Like the Auditor role, this role is not assigned directly through the Certificate Server interface. Instead, Certificate Server will treat any user that has the IT Environment policy *Backup Files and Directories* privilege as a Backup Operator.

- **Enrollee:** The Enrollee is any identified and authenticated user who is authorized to make requests to the Certificate Server. In the security descriptor maintained by the Certificate Server (further details in the next section), users must be granted the ENROLL permission using the TOE's Certificate Server MMC management snap-in.

The Auditor and Backup Operator roles are designated by the assignment of privileges in the IT environment. The Certificate Administrator, Officer, and Enrollee roles are designated by the internal security descriptor maintained by the TOE that defines what services users have access to.

The separation of the above roles can be enforced using a feature called *Role Separation*. Once activated, role separation allows a user to be assigned to only a single role. If a user is assigned to more than one role and attempts to perform an operation on the Certificate Server, the operation is denied. For this reason, before role separation is enabled the configuration should be verified so each user is assigned only one role.

Only the Certificate Administrator can enable and disable role separation via the TOE. Once role separation is enabled, any assigned roles are in effect until the Certificate Administrator disables role separation via the TOE.

Roles can be assigned and changed by the Certificate Administrator while role separation is enabled or disabled. It is possible for a user assigned a role to become locked out of administering a Certificate Server when role separation is enabled if the user is also assigned to a second role. If the Certificate Administrator assigns himself or another role holder to a second role, then the Certificate Administrator violates the rules of role separation by allowing a user to have two roles. Once the user is assigned to two roles, role separation will not allow that user to perform any activity on the Certificate Server, including, in the case of the Certificate Administrator, the activity of removing himself from one of the roles.

The following table (based on the FMT_MOF.1 requirement Table 8 (Authorization Roles for Management of Security Functions Behavior) defines the set of management functions that can be performed within the TOE and the Role that is allowed to perform that operation.

NOTE: The terms Certificate Administrator and IT Environment Administrator are used as below:

- Certificate Administrator – users in the Certificate Administrator role as defined earlier in this section.
- IT Environment Administrator – users acting as administrators in the environment (i.e., users in the Windows 2003 administrators group.

Table 11 Role Restrictions

Section/Function	Authorized Role	Not Applicable
Security Audit	The capability to configure the audit parameters is restricted to Administrators. The capability to change the frequency of the audit log signing event is restricted to Administrators.	Audit log signing is not performed by the TOE – see Section 7 for details
Backup and Recovery	The capability to configure the backup parameters is restricted to Certificate Administrators. The capability to initiate the backup or recovery function is restricted to *Backup Operators*.	The TOE does not offer the capability to configure the backup parameters.

Section/Function	Authorized Role	Not Applicable
Certificate Registration	The capability to approve fields or extensions to be included in a certificate is 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.	This is not applicable to Officers as the Cert Administrator configures the profiles, and the Officer does not modify this configuration.
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.	This action is not applicable to the TOE, as the TOE does not support the export of CIMC private keys.
Certificate Status Change Approval	Only Officers can configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Officers can configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.	This action is not applicable to the TOE as there is no automated process to approve certificate revocation. This is not applicable to Officers as it is addressed in the profile which is configured by the Cert Administrator. The Officer does not modify this configuration.
CIMC Configuration	Except as stated elsewhere, the capability to configure any TSF functionality is restricted to Certificate Administrators.	
Certificate Profile Management	The capability to modify the certificate profile is restricted to Certificate Administrators.[4]	
Revocation Profile Management	The capability to modify the revocation profile is restricted to Certificate Administrators.	The TOE does not support profiles or templates for the revocation of certificates.
Certificate Revocation List Profile Management	The capability to modify the certificate revocation list profile is restricted to Certificate Administrators.	

SFR Mapping:

The **Roles** security function satisfies the following SFRs:

[4] The TOE should be configured such that only Certificate Administrators have the permission to change the templates.

- FMT_MOF.1 (iteration 2) – The TOE enforces Certificate Server roles that are implemented in conjunction with the IT Environment. The TOE restricts the ability to modify management functionality to a specific role. The TOE ensures the user is a member of the appropriate role before the management behavior is modified. Table 11 demonstrates that the Roles function is sufficient to enforce the FMT_MOF.1 requirement. Columns 1 in Table 11 is consistent with column 1 in Table 8 (included in the FMT_MOF.1 requirement in section 5) identifying the security functions the requirement restricts management of. Column 3 in Table 11 denotes management functionality that the TOE does not provide and, therefore, restrictions associated with them are not applicable to the TOE. Column 2 in Table 11 describes the restrictions to management functions enforced by the Roles security function. Column 2 is consistent with column 3 in Table 8, with one exception: The TOE restricts the capability to initiate the backup or recovery function to the Backup Operator role and the requirement restricts this capability to the Administrator role (which is referred to as the Certificate Administrator). The TOE's restriction is acceptable because the change in restriction of management functionality is not to one of the roles mandated in the TOE's IT environment FMT_SMR.2 requirement but the change is to an additional role offered by the TOE. Also, the Backup Operator can only perform backup related management functions. Therefore, restricting administrative functionality to the Backup Operator role rather than the Certificate Administrative role satisfies the FMT_MOF.1 requirement.

6.1.3 Access Control

The TOE supports controlling access to services it provides by defining access control to services based on user roles. These roles map users to the functions they can perform. Users must be authenticated to the IT environment Windows domain in which the TOE resides. Users request an operation to be performed on the Certificate Server with the MMC Certificates snap-in or command line tools. These client tools communicate with the server using the IT environment provided DCOM service. This DCOM service supports the ability of the TOE to identify the user as an authenticated user in the domain with all the rights and privileges associated with that user.

The TOE maintains an internal security descriptor that defines what services users have access to. This security descriptor is virtual in that when the TOE starts, the data for the descriptor is initialized by reading from the IT environment registry. When changes are made to the security descriptor during runtime, the data is written to the registry as well as in memory. The descriptor is the Global Certificate Server descriptor. The purpose of the global descriptor is to identify access to resources and to define the members of the roles that are not maintained by the IT Environment (Certificate Administrator, Officer, Enrollee). The Global Certificate Server descriptor maintains the following permissions that define who can perform the following operations:

- **Read Certificates:** Allows a user with this permission to connect to the TOE and read certificates including the CA Certificate and CRLs.
- **Issue and Manage Certificates (Officer role):** This permission identifies a user as being in the Officer role.
- **Manage Certificate Authority (Certificate Administrator role):** This permission identifies a user as being in the Certificate Administrator role.
- **Enroll (Request Certificates) (Enrollee role):** This permission identifies a user as being in the ENROLLEE role which will allow the user to submit a new certificate request.

The TOE services provided and what roles can access each service is provided in the table below (based on Table 7 -the FDP_ACF requirement):

Table 12 Authorizations

Services	Authorized Role	Applicability
Required by FDP_ACF		
Certificate Request Remote and Local Data Entry	The entry of certificate request data is restricted to Officers and the subject of the requested certificate.	
Certificate Revocation Request Remote and Local Data Entry	The entry of certificate revocation request data is restricted to Officers. and the subject of the certificate to be revoked.[5]	
Data Export and Output	The export or output of confidential and security-relevant data is performed only at the request of authorized users.	The TOE does not allow for the export of confidential and security-relevant data. The TOE does store critical data such as its own private key in a hardware cryptographic service module.
Key Generation	The capability to request the generation of Component keys (used to protect data in more than a single session or message) is restricted to Certificate Administrators.	The TOE does not allow for the generation of Component keys.
Private Key Load	The capability to request the loading of Component private keys into cryptographic modules is restricted to Certificate Administrators[6].	The TOE does not allow for the loading of Component private keys. The TOE's private key is stored in the hardware cryptographic service module.
Private Key Storage	The capability to request the decryption of certificate subject private keys is restricted to Officers.	The TOE does not provide a capability to decrypt certificate subject private keys.
Trusted Public Key Entry, Deletion, and Storage	The capability to change (add, revise, delete) the trusted public keys is restricted to Certificate Administrators.	The TOE does not provide a capability to change the trusted public keys.

[5] The request to revoke a certificate is rejected if the requestor is not an Officer.
[6] The CA private key resides in the hardware crypto module.

Services	Authorized Role	Applicability
Secret Key Storage	The capability to request the loading of CIMC secret keys into cryptographic modules is restricted to Certificate Administrators.	The TOE does not implement key management for CIMC secret keys. The hardware cryptographic service module used by the TOE provides its own key management service.
Private and Secret Key Destruction	The capability to zeroize CIMC plaintext private and secret keys is restricted to Certificate Administrators, Auditors, Officers, and Operators.	The TOE does not implement key management for CIMC secret keys. The hardware cryptographic service module used by the TOE provides its own key management service.
Private and Secret Key Export	The capability to export a component private key is restricted to Backup Operators. The capability to export certificate subject private keys is restricted to Officers.	The TOE does not support the export of a certificate subject private keys
Certificate Status Change Approval	Only Officers *and the subject of the certificate* are capable of requesting that a certificate be placed on hold. Only Officers are capable of removing a certificate from on hold status. Only Officers are capable of approving the placing of a certificate on hold. Only Officers *and the subject of the certificate* are capable of requesting the revocation of a certificate. [7] Only Officers are capable of approving the revocation of a certificate and all information about the revocation of a certificate.	

The table above (Table 12) demonstrates the sufficiency of the access control function to meet the access control related requirements. Table 12 above is based upon Table 7 in the FDP_ACF.1 requirement in that column 1 of Table 12 is the same as Table 7; column 2 of Table 12 is the same as column 3 of Table 7, with the exceptions as noted below.

SFR Mapping:

The **Access Control** security function satisfies the following SFRs:

[7] Only Officers are allowed to request the revocation of a certificate.

- FDP_ACC.1 (iteration 2) – To enforce the security policy, the TOE relies on the IT Environment to maintain the Auditor and Backup Operator roles. Additionally, the Certificate Server maintains a Global Security Descriptor (SD) which maintains which users are in the Officer role, Certificate Administrator, who can read certificates and who can enroll for certificates.
- FDP_ACF.1 (iteration 2) – The TOE enforces the access control policy by using the following items:
    - Role: Users are identified as a member of the Certificate Administrator, Backup Operator or Auditor role through the rights the user has been granted in the IT Environment or through the permissions or rights assigned using the TOE's MMCs snap-ins. A user is identified to be in the Officer role by being granted *Issue and Manage Certificates* in the Global SD. A user must be mapped into one of these roles or be allowed *Read Certificate* or *Enroll permission* before access to any service is allowed.
    - ACL: The TOE maintains the Global SD. The Global descriptor identifies users in the Certificate Administrator or Officer role as well as identifying users that are granted the Certificate Server services: *Read Certificate* and *Enroll*.
    - The table above in the Access Control function describes
    - The TOE access control requirements for "Private Key Storage", "Private Key Load", and "Private and Secret Key Destruction" do not apply for the Microsoft Windows Server 2003 Certificate Server. The Microsoft Windows Server 2003 Certificate Server 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.
    - Additionally, only an Officer can request a certificate to be revoked, whereas the FDP_ACF requirement allows subjects to request certificate data regarding their own certificates. This change does not violate the FDP_ACF requirement because the restriction is reduced from two roles to one.
- FPT_RVM.1 (iteration 2) – The TOE enforces the Access Control Policy at the entry point of every DCOM interface that it implements. The TOE does not provide interfaces to its services other than those implemented based on IT environment provided DCOM. When a user requests access to a TOE service, the TOE first maps the user to a Role and ensures that the user is in the appropriate role to complete the operation.

6.1.4 Security Audit

The TOE collects audit data for internal actions and user actions and works in conjunction with the IT Environment audit infrastructure to securely record and store this information. When a TOE related security relevant event occurs, the TOE generates the corresponding audit log event and calls upon the IT Environment audit infrastructure to record the event. These events are collected with other IT environment audit log events and are stored in the Security log under the control of the IT environment.

Each audit log record includes:

- Date: The date the event occurred.
- Time: The time the event occurred.
- User: The SID of the user on whose behalf the event occurred that represents the user. SIDs are described in more detail in Section 6 under Identification.
- Event ID: A unique number identifying the particular event class.
- Outcome: Success or Failure of event.
- Description: Contains additional information associated with the specific event.

Note: the audit records do not include plaintext private or secret keys or other critical security parameters.

The TOE provides a mechanism for the Certificate Administrator Role to specify which categories of TOE related events when detected are to be generated for the security log. This is done by mapping each event to an Event Category. The Auditor using the Certificate Server MMC snap-in can choose which event categories should be generated for the security log.

The following table lists the required set of auditable events (and additional audit record details when applicable) included in the FAU_GEN.1.1 requirement in section 5. The "How Addressed" identifies how the auditable event is addressed. This column identifies if the auditable event is addressed by the TOE itself, the environment, or is not applicable to the TOE functionality. For auditable events that are addressed by the environment, the TOE relies upon the IT environment to record these events and these events relate to functionality that exists in the IT Environment that the TOE depends upon. For example, the TOE relies on the I&A mechanism for user validation. In turn, it is the IT Environment's responsibility to record these events if they occur. If the TOE addresses the auditable event, the column specifies the event category and event Identification (ID) which includes the relevant audit information. This column also identifies any events that are not applicable to the TOE. An event ID is associated with each possible audit record type (e.g. Event ID 789); therefore, the event ID identifies the type of event that is audited. The event IDs are categorized into classes (e.g. AUDIT_FILTER_CASECURITY) and each event ID belongs to a class (e.g. Event 789 belongs to class AUIDT_FILTER_CASECURITY). Classes can be selected by the Certificate Administrator to be audited or not audited by the TOE.

All audit events when detected are delivered to the IT Environment which is responsible for ensuring the records are recorded in the Security log (or sometimes referred to as the event log. The IT Environment provides Event Logger controls and protects access and modification to the Security log. The Security log is an IT Environment system resource. The IT Environment is responsible for ensuring that only users in the Auditor role have access to the security log. Additionally, the IT environment security log is opened exclusively by the IT environment (i.e. underlying OS) during boot time and there is no interface to delete or modify the security log entries by any user.

If the Security log becomes full, the TOE relies on the IT Environment to prevent auditable events from occurring except actions taken by IT Environment Administrator.

Additionally, the TOE relies on the IT Environment and its ability to provide reliable time stamps.

Table 13 TOE Auditable Events

How Addressed[8]	Event	Additional Details
AUDIT_FILTER_CASECURITY	Startup and shutdown of the audit function	
AUDIT_FILTER_CASECURITY	Any changes to the audit parameters, e.g., audit frequency, type of event audited. Any attempt to delete the audit log	
AUDIT_FILTER_CASECURITY	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.
AUDIT_FILTER_CASECURITY	All security-relevant messages (i.e., requests) that are received by the system	
AUDIT_FILTER_CASECURITY [9]	All Successful and unsuccessful requests for confidential and security-relevant information	

[8] The categories are not identified in the audit log, only the audit ID is identified (e.g. SE_AUDITID_XXX) is identified in the audit log.

How Addressed[8]	Event	Additional Details
Not Applicable: The TSF does not request key generation.	Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
Not Applicable: The TSF does not store user private keys	The Loading of Component private keys	
Not Applicable – Key recovery functionality is not considered within the scope of the TOE.	All access to certificate subject private keys retained within the TOE for key recovery purposes	
AUDIT_FILTER_CASECURITY	All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
Not Applicable: The TOE does not store user secret keys	The manual entry of secret keys used for authentication	
Not Applicable – Private and Secret keys are not exported.	The export of private and secret keys (keys used for a single session or message are excluded)	
AUDIT_FILTER_CERTIFICATE	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.).
AUDIT_FILTER_CERTIFICATE	All requests to change the status of a certificate	Whether the request was accepted or rejected.
AUDIT_FILTER_CACONFIG	Any security-relevant changes to the configuration of the TSF.	
AUDIT_FILTER_CERTIFICATE Additionally, the environment audits the changes to certificate templates as they are Directory Service (DS) objects and the auditing of these objects are included in the security audit log on the Active Directory machine in the environment.	All changes to the certificate Profile	The changes made to the Profile
Not Applicable – The TOE does not support the automation of revocation and therefore, there is no revocation profile.	All changes to the revocation profile	The changes made to the Profile
AUDIT_FILTER_CERTREVOCATION Note that the NextUpdate value is included in this audit record and it is the only required field that can be set by the cert admin	All changes to the certificate revocation list profile	The changes made to the profile

In addition to the audit events listed in Table 12, which map to the events listed in the table included in the FAU_GEN.1.1 requirement the audit events required to meet the minimum level of audit are also addressed by the TOE. Several of these are already addressed in Table 12 and the environment addresses others. Table 13 (TOE Minimum Auditable Events) identifies the events required to meet the minimum level of audit and how the TOE

[9] The only security-related information are certificates, therefore, this audit event is applicable to requests for certificates.

addresses them. The following auditable events are also required by the minimum level of audit, however, they are not applicable to the TOE because a request for certificate service will always be associated with a user identify. As described in the Identification function a user must be known to the domain before a certificate request is submitted to the TOE. Therefore, the certificate request will always have a user identity associated with it that can be obtained by the TOE.

- Unsuccessful use of the user identification mechanism, including the user identity provided (associated with FIA_UID.2)
- Unsuccessful binding of user security attributes to a subject (e.g. creation of subject) (associated with FIA_USB.1).

Table 13 TOE Minimum Auditable Events

How Addressed	Related Security Functional Components	Minimum Audit Event
Addressed in Table 12 (Event: Changes to audit parameters)	FAU_SEL.1 Selective audit (iteration 2)	All modifications to the audit configuration that occur while the audit collection functions are operating.
Addressed in Table 12 (Events associated with certificate access)	FDP_ACF.1 Security attribute based access control (iteration 2)	Successful request to perform an operation on a n object covered by the SFP

SFR Mapping:

The **Security Audit** security function satisfies the following SFRs:

- FAU_GEN.1 (iteration 2) – The TOE audit collection is capable of generating audit records for the events identified in Table 12 (Auditable Events) and Table 13 (TOE Minimum Audit Events). Additionally, the TOE audit collection is capable of generating audit records for the additional events identified in section 6.1.4 which satisfy the minimum level of auditing specified in FAU_GEN.1. The following information is recorded for each audit event: date, time, user SID or name, event ID and outcome.
- FAU_GEN.2 (iteration 2) – The Microsoft Windows Server 2003 Certificate Server must be installed in *Enterprise Mode*. The TOE implements its only external interfaces via the IT environment provided DCOM. All users interacting with the TOE will be able to be identified and authenticated by the TOE and the IT environment respectively. As a result, there will be no situations in which a non-identified and non-authenticated user can perform any action since all users must be authenticated to the domain during the network logon to the IT Environment on which the TOE resides. Therefore, each user that attempts an action will have their identity associated with that action and available for being included in the audit record.
- FAU_SEL.1 (iteration 2) – The Certificate Server MMC snap-in provides the Certificate Administrator role the ability to select categories, or types, of audit events to be included in the security log, assuming that the Object Access Auditing Policy in the IT environment has been turned on by the IT environment Administrator. There are seven (7) categories that are defined and all TOE auditable events are mapped to one of these categories.

6.1.5 Backup & Recovery

The TOE provides methods for performing secure backups and recovery of data specific to the TOE. Only members of the Backup Operator role can perform the backup and recovery operations. The TOE provides the ability to backup and restore the Certificate database both in a full and incremental form and the CA certificate with public key. The CA private key is maintained in the hardware cryptographic service module. The CERTUTIL.EXE command line application and the Certificate Server MMC snap-in make available these operations.

The Certificate database is the set of user public keys, associated certificates and CRL information. There are no private keys stored in this database. The certificate database is used to store operational information on certificates and their status including all certificate requests in any status, all issued certificates, and all revoked certificates. The state of the TOE can be re-created from backup of the certificate database. This database is implemented as a Jet database. The information stored in this database is considered public information since it only includes signed public key certificates and CRL information. It is protected from unauthorized alteration, however, it can be backed up and restored without the need for a password because the backup operator would have logged on to his/her account maintained by the IT Environment using his/her own account password.

The TOE provides information to allow an Auditor to ensure the integrity of the certificate database. When the TOE is started, and when it is stopped, hashes of the certificate database, the CA public key and the CA certificate are created. These three hash values (the hashes are calculated with a cryptographic means) and a Certificate Service private key usage count are included with the start and stop event when it is recorded in the IT Environment security event log. The hash values from the most recent Certificate Service start and stop events can be compared to ensure the database was not altered when the service was not running.

The CA Certificate is the certificate issuing server's public key-private key pair and associated signed certificate. This information is considered to be private since compromise of the CA Certificate private key would breach the overall PKI security of all issued certificates. The CA private key is resides in the hardware cryptographic service modules.

SFR Mapping:

The **Backup & Recovery** security function satisfies the following SFRs:

- FDP_CIMC_BKP.1 – The TOE provides a GUI and command line method for performing backup and recovery operations on the certificate database and the TOE CA Certificate. The recovery functions will restore the certificate database, the CA Certificate or both to the state where they were last backed up.
- FDP_CIMC_BKP.2 – The Certificate database is considered public information, it does not include any private keys. The CA private key is maintained in the hardware cryptographic service module. The TOE provides information to allow an Auditor to ensure the integrity of the certificate database by including three hash values (related to the certificate database) and a Certificate Service usage count in the event log when the TOE starts and stops. The presentation of these values allow the Auditor the ability to compare these values upon startup to those that were included upon the previous stopping of the TOE to determine if there have been any changes when the service was not running. A hash of the event log is as sufficient as a keyed hash because the event log is protected from modification by all users.

6.1.6 Remote Certificate Request Data Entry & Certificate and Certificate Status Export

The TOE processes certificate requests formatted according to the following standards which, in conjunction with the Identification security function and I&A performed in the IT Environment, provide the verification of origin framework for the TOE to follow:

PKCS #7 (Cryptographic Message Syntax Standard),

PKCS #10 (Certification Request Syntax Standard),

RFC 2797 CMC (Certificate Management Messages over Cryptographic Message Syntax).

The TOE generates certificates and certificate revocation lists according to the following standard which provides a verification of origin framework for users of certificates and CRLs to follow:

RFC 3280 Internet X.509 PKI Certificate and CRL Profile (which is consistent with ITU-T Recommendation X.509.

In servicing certificate request or renewal of certificates, the TOE ensures that the certificate request is digitally signed and that the caller is the subject of the certificate request. The TOE will not accept a certificate request or certificate renewal request if it is not signed. Furthermore, the TOE will not issue a certificate if the user submitting the request is different from the certificate subject specified in the request. It should be noted that network communications in the IT Environment are also protected by IPSec.

SFR Mapping:

The **Remote Data Entry & Export** security function satisfies the following SFRs:

- FCO_NRO_CIMC.3 – The TOE generates certificates and CRLs according to the RFC 3280 standard which provides a verification of origin framework. Therefore, the TOE provides the ability to prove the origin of status information it generates. Additionally, the TOE requires that the IT environment provided DCOM authentication based protocols are used to communicate with the TOE. When certificate requests are received the identity of the requesting user is impersonated and the request is completed in the context of that user. Additionally, the request is parsed and the data is analyzed to ensure that the certificate subject name matches the authenticated user that submitted the request. The TOE processes certificate requests formatted according to the PKCS #7, PKCS #10, and RFC 2797 standards. The TOE Identification security function and I&A performed in the IT Environment provide the verification of origin. Note that the active directory is queried for the authenticated user identity to obtain at least the subject Common Name. The TOE can be configured to use the rest of the RDN prefix. Alternatively, the TOE can be configured to obtain the full subject DN from the Active Directory using the authenticated subject identity.

  When certificate revocation requests are received, the role/authorization of the requesting user is verified. The TOE Identification security function and I&A performed in the IT Environment, provide the verification of origin of revocation request.

- FCO_NRO_CIMC.4 – Certificate requests made by a Certificates MMC snap-in or CERTREQ.EXE command line tool must be encoded using PKCS #10 or CMC formats. These formats inherently support the request being signed using the private key corresponding to the public key in the certificate request. This provides proof of possession of the private key. The TOE does not accept any other security relevant information outside of certificate requests. When certificate requests are received the identity of the requesting user is impersonated and the request is completed in the context of that user. Additionally, the request is parsed and the data is analyzed to ensure that the certificate subject name matches the user who was authenticated by the IT environment and submitted the request. The IT Environment authentication is considered to have met the authentication code aspects of the initial registration. Also, see the previous section as to how the TOE obtains the subject DN from the subject identity authenticated by the IT Environment. For certificate renewal, the subject must send a PKCS#7 request signed using a current valid signature key.

- FDP_CIMC_CSE.1 – The TOE provides certificate status information by following means: CRLs (X.509 7/ RFC 3280 format except that the critical Issuing Distribution extension is not asserted in specific circumstances when the CRL does not cover certificates where the CA key signing the certificates is different from the CA key signing the CRL): The TOE provides the ability to configure the specific details of the CRLs for each CA to the Certificate 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, this Update Date, Revoked Certificate and a Signature. The format of the exported CRL conforms to the X.509 standard for CRLs specified in RFC3280, except that the critical Issuing Distribution extension is not asserted in specific circumstances when the CRL does not cover certificates where the CA key signing the certificates is different from the CA key signing the CRL.

6.1.7 Key Management

The key management function is concerned with the management of keys that are used to support the TOE's security functions such as the TOE's private and public key, and the public keys associated with the certificates it provides to users. Digital signatures included in the certificates to ensure the integrity of key management related information.

The TOE relies on FIPS 140-1 Level 3 validated cryptographic security modules for key generation for certificates, key storage and key destruction through zeroization.

The TOE uses its underlying operating system's file system to store certificates which include public keys (the certificate database). There are no private keys stored in this database.

The Certificate Service provides information to allow an Auditor to ensure the integrity of the certificate database. When the TOE is started, and when it is stopped, hashes of the certificate database, the CA public key and the CA certificate are created. These three hash values and a Certificate Service private key usage count are included with the start and stop event when it is recorded in the IT Environment security event log. The hash values from the most recent Certificate Service start and stop events can be compared to ensure the database was not altered when the service was not running. The Administrative Guidance for the TOE includes procedures to perform the comparison.

The TOE does not store user private keys, and does not support the export of private keys.

SFR Mapping:

The **Key Management** security function satisfies the following SFRs:

- FDP_ACF_CIMC.2 – The Certificate Authority private key is stored by the TOE in the hardware Cryptographic Service Module (HSM). No other private keys are collected or stored.
- FMT_MTD.CIMC.4 – No subject private keys are stored in the TOE. The CA private key is stored in the HSM. All encryption is performed using FIPS 140-1 validated cryptographic modules. The only private key that is stored is CA private key. No other private keys are collected or stored.
- FDP_SDI_CIMC.3 – The entire certificate database, the Certificate Server signed certificate and the Certificate Server public key are protected from unauthorized modification through the use of hash calculations. The TOE generates a hash for these items during TOE startup and shutdown and dumps this information to the event log and the Administrative Guidance document provides procedures on how to perform a comparison between the current start hash values and the previous stop hash values. If the values are the same the integrity of the certificate database has been maintained. This procedure is sufficient to ensure the integrity of the public keys that are stored in the certificate database because during operation the TOE prevents modification of the public keys. In addition, the signed CA certificate hash is written to the registry for verification during operations. A hash of the event log is as sufficient as a keyed hash because the event log is protected from modification by all users.
- FDP_ACF_CIMC.3 – the TOE does not collect or store user secret keys.
- FMT_MTD_CIMC.5 – The TOE stores the CA private key in a hardware cryptographic service module.
- FCS_CKM_CIMC.5 – the TOE stores no secret keys. Private keys are destroyed inside a FIPS 140-1 validated cryptographic module.
- FDP_ETC_CIMC.5 – The TOE does not support the export of user private or secret keys. The TOE stores the Certificate Authority private key in a hardware cryptographic service module.
- FMT_MTD_CIMC.7 – The TOE stores the Certificate Authority private key in a hardware cryptographic service module. The TOE does not support the export of any other private or secret keys.

6.1.8 Certificate Management

The TOE provides the ability to issue certificates and publish CRLs. The Microsoft Certificate Server manages and securely stores certificate templates (or profiles). Templates contain attributes and information that must be included in the request or will be automatically used in the request if it is not present in the request. Every certificate request is based on a template. If it is not based on a template, the certificate request will be rejected. During the certificate request, the Certificate Server validates that all required attributes are provided or the certificate request will be denied.

The TOE allows for qualified subordination which can place certificate issuance constraints on subordinate CAs and can place usage constraints on the certificates they issue. With qualified subordination, a subordinate CAs can be focused according to specific certification needs allowing for more efficient administration. Qualified subordination also allows for the establishment of trust between CAs in separate trust hierarchies. This type of trust relationship is also called *cross-certification*. With this trust relationship, qualified subordination is not limited to subordinate CAs.

Trust between hierarchies may be established using a subordinate CA in one hierarchy and the root CA in another hierarchy.

Qualified subordination extends the trust hierarchy by allowing the ability to place additional trust conditions within and between the domains in the PKI. With qualified subordination, the qualified subordinate CAs in the trust hierarchy can each have different rules governing how they will issue certificates and how their certificates may be used. All constraints that are placed on a qualified subordinate CA are defined upon the installation of the CA.

The TOE publishes CRLs that identifies certificates in the certificate database that have been revoked by the TOE. The TOE can publish two types of CRLs: Base CRLs and Delta CRLs. A Base CRL identifies all the certificates that have been revoked and a Delta CRLs identifies the certificates that have been revoked since the last published Base CRL. The TOE can publish CRLs automatically based upon a configured time period or upon the manual invocation by the CA Administrator.

SFR Mapping:

The **Certificate Management** security function satisfies the following SFRs:

- FMT_MOF_CIMC.3 – The TOE provides standard templates for certificates and ensures that certificates it creates are consistent with the currently selected template. These templates conform to the X.509 standard. Certificate templates are stored as directory objects in the AD in the IT Environment. A default set of X.509-compliant templates is assigned to each Certificate Server when it is created, and the template selection may be modified by the Certificate Administrator through the Certificate Template MMC snap-in. Certificates issued by a Certificate Server must conform to one of its assigned templates. The TOE provides the ability to configure the specific details of the certificates (i.e., Domain Name (DN) Attributes or Extensions) for each Certificate Server to the Administrator. The Certificate Administrator can specify acceptable values for the following fields and extensions: 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; keyUsage; basicContraints; certificatePolicies, and certificate extensions.
- FMT_MOF_CIMC.5 – The TOE generates CRLs according to a template implemented directly in code, to ensure CRLs are always consistent with the standard certificate revocation list template. The value of the Issuer field is determined by the name of the issuing Certificate Server and the value of the nextUpdate field is controlled by the Certificate Administrator. The configurable values are stored in the IT Environment registry. The TOE does not support the issuerAltName field within the CRL.
- FDP_CIMC_CER.1 – As previously described by the Remote Data Entry & Export security function, the TOE, working in conjunction with the IT environment, verifies the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, whenever the private key may be used to generate digital signatures. The TOE provides standard templates for the certificates and ensures that certificates are consistent with the currently selected template and shall only generates 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.

- FDP_CIMC_CRL.1 – The TOE provides standard templates for the CRLs to ensure that CRLs are consistent. The TOE ensures that the following fields and extensions in any CRL issued contain values in accordance with RFC3280:
  1. The **version** field shall contain the integer **2**.
  2. The **issuer** field shall contain the issuing certificate authority's distinguished name (DN) represented using an X.500 DN.
  3. The **signature** and **signatureAlgorithm** fields shall contain the OID for a FIPS-approved digital signature algorithm.
  4. The **thisUpdate** field shall indicate the issue date of the CRL.
  5. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.
  6. The CRL Number extension shall indicate a monotonically increasing sequence number for each CRL being issued.
  7. The authority key identifier extension shall contain a numeric representation of the issuer name and serial number from the CRL issuer's certificate as a means to identify the public key corresponding to the private key used to sign a CRL.
  8. The freshest CRL extension shall contain the URLs to fetch the delta CRL.
  9. There shall be a sequence of zero or more revoked certificates with the following fields represented for each revoked certificate.
  - 9.a The certificate serial number field shall contain the serial number assigned by the issuing certificate authority for each revoked certificate.
  - 9.b The revocation date field shall contain the date at which the revocation took place.
  - 9.c The reason code field shall identify the reason for the certificate revocation, which may be Unspecified, KeyCompromise, CACompromise, AffiliationChanged, Superseded, CessationOfOperation, CertificateHold, and RemoveFromCRL.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the CC EAL 4 augmented assurance requirements:

- Process Assurance,
- Delivery and Guidance,
- Design Documentation,
- Tests, and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by Microsoft ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Microsoft ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. Microsoft performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, the CM documentation, and security flaws.

Microsoft applies procedures to accept and act upon reported security flaws and requests to correct security flaws. Microsoft designates specific points of contact for user reports and security related inquiries. The procedures are documented and describe how security flaws are tracked, that for each security flaw a description and status of the correction of the security flaw is provided, that corrective actions are identified for each security flaw, how flaw

information is provided (corrective actions and guidance on corrective actions). The procedures ensure that all reported flaws are corrected and that corrections are issues to TOE users, and that the flaws do not introduce new flaws. The procedures also ensure a timely response to reported flaws and the automatic distribution of security flaw reports to the affected users. These activities are documented in:

Document	Version	Date
Windows Cert Server Management (CM) Manual	1.9	2 Aug 2005

6.2.1.2 Life Cycle Support

Microsoft ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan. Microsoft includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE. Microsoft achieves this through the use of a documented model of the TOE life cycle and well-defined development tools that yield consistent and predictable results. Additionally, Microsoft documents the implementation dependent options and the meaning of all statements used in the implementation. This information and these procedures are documented in:

Document	Version	Date
Assurance Life Cycle (ALC) for Windows Certificate Server	0.2	2 Aug 2005

SAR Mapping:
The **Process Assurance** measures satisfy the following SARs:

- ACM_AUT.1
- ACM_CAP.4,
- ACM_SCP.2,
- ALC_DVS.1,
- ALC_FLR.3,
- ALC_LCD.1, and
- ALC_TAT.1.

6.2.2 Delivery and Guidance

Microsoft provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Microsoft's delivery procedures describe the electronic and non-electronic procedures to be used to detect modification to the TOE. These procedures are documented in:

Document	Version	Date
Windows XP and Windows Server 2003 Delivery Procedures	0.2	3 Aug 2005

Microsoft provides administrator and user guidance on how to utilize the TOE SFs and warnings to authorized administrators and users about actions that can compromise the security of the TOE. The installation and generation

procedures, included in the administrator guidance, describe the steps necessary to install the TOE in accordance with the evaluated configuration. Administrator and user guidance is documented in:

Document	Version	Date
Windows Server 2003 Certificate Server Evaluated Configuration Administrator's Guide	1.0	16 Sep 2005
Windows Server 2003 Certificate Server Security Configuration Guide	1.0	22 Sep 2005
Windows Server 2003 Certificate Server Evaluated Configuration User's Guide	1.0	19 Aug 2005

SAR Mapping:

The **Delivery and Guidance** assurance measure satisfies the following SARs:

- ADO_DEL.2,
- ADO_IGS.1,
- AGD_ADM.1, and
- AGD_USR.1.

6.2.3 Development

The Windows Server 20003 Certificate Server "Security Design Documentation" is an extensive set of documents describing all aspects of the TOE security design, architecture, mechanisms, and interfaces. The Security Design Documentation includes the following information:

- Describes the form, content, and organization of the System Design documentation.
- Provides an informal description and model of the access control policy for the system.
- Describes the decomposition of the system and identifies the subsystems in terms of components.
- Description of the components and identifies the modules within the component in terms of subcomponents.
- Description of the subcomponents presenting the following:
  - Summary identifying the subcomponent's name, implementation location, and execution environment.
  - A description of the design of the subcomponent and a summary of its SFs and mechanisms.
  - A specification of each TSF interface implemented by the subcomponent. The following is provided for each TSF interface: purpose, parameters, security checks, and security effects.
  - A correspondence matrix that identifies for each TSF interface, which security functions the interface's checks and effects help implement. The matrix includes a rationale for this correspondence.
  - A test family summary that describes test cases implemented in the security tests for each Application Programming Interface (API).

The Security Design Documentation includes the following documents:

Document	Version	Date
Certificate Server Component Design Specification	4	27 Jul 2005
Certificate Service Subcomponent Design Specification	44	15 Nov 2005
Certificate Service Default Policy Module Subcomponent Design Specification	16	1 Sep 2005

Certificate Service Default Exit Module Subcomponent Design Specification	8	16 Nov 2004
Certification Authority GUI Subcomponent Design Specification	0.6	8 Jul 2005
Certificate Server Component Correspondence Matrix		16 Nov 2004
Informal TOE Security Policy Model Design Specification	6	28 Sep 2005
Functional Specification Completeness Rationale	4	2 Sep 2005

SAR Mapping:

The **Development** security assurance measure satisfies the following SARs:

- ADV_FSP.2: The Windows Server 2003 Certificate Server Functional Specification consists of many Subcomponent Design documents that fully describes all interfaces to the TSF.
- ADV_HLD.2: The Windows Server 2003 Certificate Server High-level Design consists of the System Decomposition Summary document and the Component Descriptions document which satisfies the requirement for decomposing the TOE into subsystems and fully describes each subsystem, including inter-subsystem interfaces.
- ADV_LLD.1: The Windows Server 2003 Certificate Server Low-level Design consists of many Subcomponent Design documents that satisfies the requirement to decompose each subsystem into modules and fully describes each module. Note that the Subcomponent Design documents support both the low level design and the functional specification requirements.
- ADV_IMP.1: A subset of the source code used to generate the TOE satisfies this requirement.
- ADV_RCR.1: Most of the correspondence between the various design documentation is implicit to the way in which the documentation is structured. The way that this correspondence is evident within the design documentation is:
    - ST-TSS to FSP: The Windows Server 2003 Certificate Server Functional Specification describes how the interfaces correspond with the security functions in the ST.
    - FSP to HLD: The Windows Server 2003 Certificate Server High-level Design describes how the various security behaviors in the MS Functional Specification are further refined.
    - HLD to LLD: The Windows Server 2003 Certificate Server Low-level Design describes how the various security behaviors in the MS High-level Design are further refined.
    - LLD to IMP: The Windows Server 2003 Certificate Server Low-level Design also serves to provide a correspondence between modules and their specific implementations.
- ADV_SPM.1: The Windows Server 2003 Certificate Server Security Model models the entities and rules related to the policies for identification, audit, and all of the information flow policies. Additionally, correspondence with the Windows Server 2003 Certificate Server Functional Specification is described.

6.2.4 Tests

The TOE test documentation has been created to demonstrate appropriate breadth and depth of coverage. The test documentation describes how all security relevant APIs are tested, specifically describing all test cases and variations necessary to demonstrate that all security checks and effects related to the API are correctly implemented. The test documentation provides correspondence between the security-relevant APIs and applicable tests and test variations. The test documentation describes the actual tests, procedures to successfully execute the tests, and expected results of the tests. The test documentation also includes results in the form of logs resulting from completely exercising all of the security test procedures.

The Test Documentation includes the following information:

- The test plan describes the form, content, and organization of test documentation. It also summarizes each of the test suites and includes high-level procedures for exercising the tests.
- The test families described the set of security-relevant test cases on a per-subcomponent basis. These descriptions include references to the corresponding test suites that implement those test cases. Note that every test case corresponds to at least one test suite.
- The test suites include both documentation and an actual implemented test (if applicable). Test suites are organized around tests that share a common theme, such as handle enforcement, privilege enforcement, auditing, etc. The test suite documentation describes the purpose and "theme" for the test suite, the set of test variations that are exercised for each of its corresponding test cases, procedures to successfully exercise the test suite, and the expected results. The test suite documentation also implicitly includes the actual tests that provide specific details regarding test variations and expected results.
- The test results are essentially the set of logs resulting from completely exercising all of the security test procedures. These logs include summaries of the results in terms of total test variations, counts of variations that passed, failed, or blocked (i.e., were unable to run), and detailed information about each variation that was attempted, including more detailed results and expected results.

The Test Documentation includes the following documents:

Document	Version	Date
Test Plan	0.1	10 May 2005
Certificate Server Test Suite	1.7	21 Sep 2005
Test Plan for Certification GUI	1.2	23 Sep 2005

SAR Mapping:

The **Tests** assurance measure satisfies the following SARs:

- ATE_COV.2: The test case descriptions (in the Windows Server 2003 Certificate Server Functional Specification) describe the test cases for each of the security-relevant interfaces of the TOE. The descriptions indicate which tests are used to satisfy the test cases identified for each interface.
- ATE_DPT.1: The test case descriptions (in the Windows Server 2003 Certificate Server High-level Design) include more detailed test case descriptions that demonstrate that all of the corresponding interfaces are appropriately exercised.
- ATE_FUN.1: The Windows Server 2003 Certificate Server Test Plan describes the security functions to be tested, how to successfully test all of them, the expected results, and the actual test results after exercising all of the tests.
- ATE_IND.2: The TOE and test documentation will be available for independent testing.

6.2.5 Vulnerability Assessment

6.2.5.1 Evaluation of Misuse

The Windows Server 2003 Certificate Server Common Criteria Administration Guide and Windows Server 2003 Certificate Server Common Criteria User Guide describe the operation of the TOE and how to maintain a secure state. These guides also describe all operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. These guides are documented in:

Document	Version	Date
Windows Server 2003 Certificate Server Evaluated Configuration	1.0	16 Sep 2005

Administrator's Guide		
Windows Server 2003 Certificate Server Evaluated Configuration User's Guide	1.0	19 Aug 2005

The misuse analysis shows that the administrative and user guidance completely addresses managing the TOE in a secure configuration.

Document	Version	Date
Windows 2003 Certificate Server Misuse Analysis	0.2	22 Aug 2005

6.2.5.2 Strength of TOE SFs

All of the SOF claims related to the TOE are based on cryptographic functions. An analysis of cryptographic functions in relation to the SOF requirements is not applicable as the CC strength of analysis requirement is not applicable to cryptographic measures.

6.2.5.3 Vulnerability Analysis

Microsoft performed a vulnerability analysis of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE within the TOE's IT environment. The vulnerability analysis is documented in:

Document	Version	Date
Windows Server 2003 Certificate Server Vulnerability Analysis	1.0	15 Sep 2005

SAR Mapping

The **Vulnerability Assessment** assurance measure satisfies the following SARs:

- AVA_MSU.2,
- AVA_SOF.1, and
- AVA_VLA.4.

7. PP Claims

As documented in this ST, Microsoft Windows Server 2003 Certificate Server complies with CIMC Security Level 3 (SL3) PP, Version 1.0, October 31, 2001.

The Security Environment, Objectives, and Requirements in this ST have been reproduced[10] from the CIMC SL3 PP, as indicated below:

[10] Note that reproduction of material from the CIMC PP includes elimination of materials not relative to the selected Security Level. This extra step is necessary because the CIMC PP intermixes material from four PPs into a single document.

- The Assumptions, Threats, and Policies have been reordered to group the SL3 specific environment statements with the statements that apply to all Security Levels. All of the CIMC SL3 PP assumptions, threats, and policies have been included and no new assumptions, threats, or policies have been introduced.
- The Security Objectives have been reordered to group the SL3 specific security objectives with the objectives that apply to all Security Levels. All of the CIMC SL3 PP security objectives have been included and no new objectives have been introduced.
- The Requirements for the IT environment and the TOE have been reordered to be presented alphabetically. All operations have been completed on the requirements in compliance with the PP as indicated using bold and bold-italic text in Section 5.1 and 5.2.
- References to Table headings numbers and section headings numbers within the requirement statements have been changed as the sections and tables in the ST do not have the same exact heading numbers as in the CIMC PP. These changes are identified as refinements.
- Tables 7 (Access Controls) and Table 8 (Authorized Roles for Management of Security Function Behavior) have been refined to remove the Operator role, which is not defined in FMT_SMR.2.
- The TOE SARs have been identified as presented in the CIMC SL3 PP, but the requirements have also been reproduced into this ST from the CC Part 3. All of the CIMC SL3 PP SARs have been included with the exception of ACM_CAP.3. ACM_CAP.3 has been replaced with ACM_CAP.4. Furthermore, ACM_AUT.1 and ALC_LCD.1 have been added to raise the overall assurance level from EAL 3 augmented to EAL 4 augmented. To further augment EAL4, ALC_FLR.3 replaced ALC_FLR.2 and AVA.VLA.4 replaced AVA.VLA.2. These additional requirements serve only to increase the overall assurance in the TOE without impacting compliance with CIMC PP SL3. These requirements are presented in Section 5.3.
- The SOF Requirements has been entirely copied from the CIMC SL3 PP. These requirements are presented in Section 5.4.
- FAU_STG.1 (iteration 1) is refined to mandate additionally secure functionality.
- All of the CIMC SL3 PP TOE SFRs have been included (not including those described which are replaced as described below), with the exceptions noted below for the following reasons:
    - FMT_MOC_CIMC.6 and FDP_CIMC_OCSP.1 are only applicable if the TOE implements OSCP. The TOE does not implement Online Certificate Status Protocol (OSCP) and, therefore, these requirements are not included in this ST. Subsequently the audit events associated with these requirements were removed from FAU_GEN.1 and the management aspects of this function were removed from FMT_MOF.1.
    - FDP_ITT.1 and FPT_ITT.1 (iteration 3) are only applicable if the TOE contains physically separated parts, which is not the case with respect to the TOE.
    - FDP_ITT.1 and FPT_ITT.1 (iteration 4) are only applicable if the TOE transmits confidential data, which is not the case with respect to the TOE.
        - As a result of the non-applicability of FDP_ITT.1 (iteration 3 and 4) and FPT_ITT.1 (iteration 3 and 4), the following objective is only supported by the environment and not supported by both the TOE and the environment as stated in the PP: O.Protect user and TSF data during internal transfer.
    - FPT_ITC.1 (iteration 2) is not applicable because the TOE does not possess or transmit confidential TSF data.
    - FDP_UCT.1 (iteration 2) is not applicable because the TOE does not transmit data across an external channel to another part of the TOE.
    - FPT_STM.1, FAU_STG.1, FAU_STG.4 (iterations 2), and FIA_UAU.1 are removed as TOE requirements (remain on the environment) because they are completely enforced by the

environment. As a result, the following objectives are only supported by the environment and not supported by both the TOE and the environment as stated in the PP: O.Time stamps; O.Respond to possible loss of stored audit records; O.Restrict actions before authentication; O.Protect stored audit records. These requirements can be allocated to the Certificate Server environment and remain conformant with the CIMC PP because the following conditions are met:

A. The underlying operating system (Windows Server 2003) has completed a formal Common Criteria Evaluation and Validation Scheme (CCEVS) evaluation that demonstrated compliance with the requirements allocated to the environment;

B. The Certificate Server evaluation team has tested the functionality provided by the environment as part of the Certificate Server evaluation;

C. Windows Server 2003 has been evaluated to, at least, against the same assurance requirements as the Certificate Server; and

D. The ST and Validation Report (VR) explicitly state that these requirements are satisfied by in the environment, specifically by Windows Server 2003.

- The following CIMC SL3 PP TOE SFRs have been replaced with requirements that encompass those that are replaced:

  - The PP FPT_CIMC_TSP.1 requirement is concerned with the protection and integrity of the audit records. In this ST, FPT_CIMC_TSP.1 is replaced with IT environment requirement FAU_STG.1 (iteration 1), as additionally operated upon beyond the operation included in the CIMC PP. This ST FAU_STG.1 (iteration 1) refines the requirement from the CIMC PP changing it from mandating that the TSF be able to "detect" modification to the audit log to mandating that the TSF be able to "prevent" modification to the audit log. The objective of the FPT_CIMC_TSP.1 requirement is to detect modification to the audit log. However, the refinement of FAU_STG.1 requires that the TOE prevent audit log modification. Therefore, the PP FPT_CIMC_TSP.1 requirement is not applicable to the TOE and it is considered to be replaced with by the refined FAU_STG.1 (iteration 1). FAU_STG.1 (iteration 1) refined meets the objective that is mapped to FPT_CIMC_TSP.1 (O.Protect stored audit records) by preventing all modification to the audit log. Additionally, meeting FAU_STG.1 (iteration 1) as refined offers a more protected audit log than FPT_CIMC_TSP.1. Therefore, the threats that are indirectly mapped to FPT_CIMC_TSP.1 (T.Modification of private/secret keys; T.Administrators, Operators, Officers and Auditors commit errors or hostile actions) are even more countered by FAU_STG.1 (iteration 1) refined.

    Note that a TOE requirement is replaced with refining an IT environment requirement. This is acceptable given that FAU_STG.1 has been removed from the set of TOE security functional requirements as it is the TOE's IT environment that protects the audit records.

  - FIA_UAU.2 and FIA_UID.2 have been included to replace those that they are hierarchical to. FIA_UAU.2 replaces FIA_UAU.1 as an IT environment requirement and FIA_UID.2 replaces FIA_UID.1 as both an IT environment and a TOE requirement.

- The content of FDP_CIMC_CRL.1 is modified:

  - When the TOE (WS03 Cert Server) uses a new key, it has a new certificate authority certificate. The new certificate points to a unique CRL URL where the CRL associated with the certificate is found. The CRL is signed with the same key of the new certificate.

    The CRL referenced by the new certificate authority certificate can be validated successfully using only the new key and not an old key. When the TOE needs to revoke a certificate issued using an old key, it puts the revoked certificate in the CRL that can be validated using only the old key and not the new key, because the revoked certificate previously has been issued using the old key and not the new key.

For a certificate issued by the TOE using an old key, if the certificate appears in the CRL of the TOE old key, the certificate would still be confirmed as revoked in its certificate validation process, as the TOE certificate points to the CRL of the Cert Server old key. As a result, despite the difference between the ST FDP_CIMC_CRL.1 SFR and the CIMC PP FDP_CIMC_CRL.1 SFR, the TSF meets the O.CERTIFICATES security objective of the PP.

- The content of FDP_CIMC_CSE.1.1 is modified:
    - RFC2459 is replaced with RFC3280 as RFC3280 replaces RFC2459.

Note that all of the corresponding rationale elements in the CIMC PP have also been referenced in this ST in Section 8. The rationale elements have been added and modified in this ST only as necessary to support the introduction of the additional SARs, identified above, to bring the overall assurance level to EAL 4 augmented.

8. Rationale

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

8.1 Security Objectives Rationale

The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy or assumption is covered by at least one security objective. Table 12 maps security objectives for the TOE to threats, Table 13 maps security objectives for the environment to threats, and Table 14 maps security objectives for both the TOE and the environment to threats. Table 15 maps the organizational security policies to security objectives. Table 16 maps assumptions to IT security objectives, listing which objectives each assumption helps to cover. The items in the tables are ordered alphabetically, sorted on the first column.

Table 12 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 13 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
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,

Non-IT Security Objective	Threat
	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
O.Time stamps	T.Critical system component fails, 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.Respond to possible loss of stored audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

Table 14 Relationship of Security Objectives for Both the TOE and the Environment to Threats

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

Non-IT Security Objective	Threat
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
O.Security-relevant configuration management	T.Administrative errors of omission

Table 15 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 16 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, O.Installation, O.Security-relevant configuration management, O.User authorization management, O.Configuration Management
A.Cooperative Users	O.Cooperative Users
A.CPS	O.CPS, O.Security-relevant configuration management, O.User authorization management, O.Configuration Management
A.Disposal of Authentication Data	O.Disposal of Authentication Data
A.Malicious Code Not Signed	O.Procedures for preventing malicious code, O.Require inspection for downloads, O.Malicious Code Not Signed
A.Notify Authorities of Security Issues	O.Notify Authorities of Security Issues
A.Operating System	O.Operating System
A.Physical Protection	O.Physical Protection
A.Social Engineering Training	O.Social Engineering Training

8.1.1 Security Objectives Sufficiency

The following discussions provide information regarding:

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

8.1.1.1 Threats and Objectives Sufficiency

8.1.1.1.1 Authorized Users

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

It is countered by:

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

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

It is countered by:

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

T.User error makes data inaccessible addresses a user accidentally deleting user data. Consequently, the user data is inaccessible. Examples include the following:

- User accidentally deletes data by striking the wrong key on the keyboard or by striking the enter key as an automatic response.
- User does not understand the implications of the prompt at hand and inadvertently gives a response that deletes user data.
- User misunderstands a system command and issues a command that unintentionally deletes user data.

It is countered by:

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

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

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

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

It is countered by:

O.Competent Administrators, 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.

8.1.1.1.2 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.

8.1.1.1.3 Cryptography

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

It is countered by:

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

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

O.Limitation of administrative access. The administrative functions are designed in such a way that administrative personnel do not automatically have access to user objects, except for necessary exceptions. In general, the exceptions tend to be role specific. Limiting the number of users who have access to cryptographic keys reducing the likelihood of unauthorized disclosure.

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

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

It is countered by:

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

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

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

O.Protect stored audit records ensures that audit records are protected against unauthorized access, modification, or deletion to provide for traceability of user actions. This objective ensures that modifications to private and secret keys can be detected through the audit trail.

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

It is countered by:

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

8.1.1.1.4 External Attacks

T.Hacker gains access addresses:

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

It is countered by:

> **O.Restrict actions before authentication** ensures that only a limited set of actions may be performed before a user is authenticated. This prevents a hacker who is unable to circumvent the access control mechanisms from performing security-relevant operations.
>
> **O.Control unknown source communication traffic** ensures that communication traffic from an unknown source is controlled (e.g., rerouted or discarded) to prevent potential damage. Various kinds of hacker attacks can be detected or prevented by rerouting or discarding suspected hacker traffic.
>
> **O.Individual accountability and audit records** provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This allows for the detection of unauthorized activity. Once detected, the damage resulting from such activity can be eliminated or mitigated.
>
> **O.Notify Authorities of Security Issues** ensures that proper authorities are notified regarding any security issues that impact their systems. This minimizes the potential for the loss or compromise of data.
>
> **O.React to detected attacks** ensures that automated notification or other reactions to the TSF discovered attacks is implemented in an effort to identify attacks and to create an attack deterrent. This objective is relevant if actions that the organization deems essential also pose a potential attack that could be exploited.
>
> **O.Trusted path** ensures that a trusted path is established between the user and the system. The trusted path is used to protect authentication data, thus reducing the likelihood that a hacker can masquerade as an authorized user.

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

It is countered by:

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

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

It is countered by:

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

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

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

8.1.1.2 Policies and Objectives Sufficiency

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

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

8.1.1.3 Assumptions and Objectives Sufficiency

8.1.1.3.1 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.

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.

8.1.1.3.2 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.

8.1.1.3.3 Physical

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

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

8.2 Security Requirements Rationale

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

8.2.1 Security Requirements Coverage

The following tables provide a mapping of the relationships of security requirements to objectives, illustrating that each security requirement covers at least one objective and that each objective is covered by at least one security requirement. The first table in this section, Table 17, addresses the mapping of security functional requirements to security objectives. The second table, Table 18, addresses the mapping of security assurance requirements to security objectives.

Table 17 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
FAU_STG.1 Protected Audit Trail Storage (iteration 1)	O.Protect stored audit records
FAU_STG.4 Prevention of Audit Data Loss (iteration 1)	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

Functional Requirement	Objective
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_ETC_CIMC.5 Extended User Private and Secret Key Export	O.Data import/export
FDP_UCT.1 Basic Data Exchange Confidentiality (iterations 1)	O.Data import/export
FPT_ITT.1 Basic Internal Transfer Protection (iteration 1)	O.Integrity protection of user data and software, O.Protect user and TSF data during internal transfer
FPT_ITT.1 Basic Internal Transfer Protection (iteration 2)	O.Integrity protection of user data and software
FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action	O.Integrity protection of user data and software
FIA_AFL.1 Authentication Failure Handling	O.React to detected attacks
FIA_ATD.1 User Attribute Definition	O.Maintain user attributes
FIA_UAU.2 User Authentication Before any Action (iteration 1)	O.Limitation of administrative access, O.Restrict actions before authentication
FIA_UID.2 User Identification Before any Action (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_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 Initialization	O.Security-relevant configuration management
FMT_MTD.1 Management of TSF Data	O.Individual accountability and audit records, O.Protect stored audit records

Functional Requirement	Objective
FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.5 TSF Secret Key Confidentiality Protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export	O.Data import/export
FMT_SMR.2 Restrictions on Security Roles	O.Security roles
FPT_AMT.1 Abstract Machine Testing	O.Periodically check integrity, O.Validation of security function
FPT_ITC.1 Inter-TSF Confidentiality During Transmission (iteration 1)	O.Data import/export
FPT_ITT.1 Basic Internal TSF Data Transfer Protection (iteration 1 and 2)	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 (iteration 1)	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 18 Security Assurance Requirements Related to Security Objectives

Assurance Requirement	Objective
ACM_AUT.1 Partial CM Automation	selection of EAL 4, O.Configuration management
ACM_CAP.4 Generation Support and Acceptance Procedures	selection of EAL 4, O.Configuration management
ACM_SCP.2 Problem Tracking CM Coverage	selection of EAL-CSPP, EAL 4, O.Configuration management
ADO_DEL.2 Detection of Modification	selection of EAL 4
ADO_IGS.1 Installation, Generation, and Start-up Procedures	selection of EAL 1, EAL-CSPP, EAL 3,EAL 4, O.Installation
ADV_FSP.2 Fully defined External Interfaces	selection of EAL 4, O.Lifecycle security
ADV_HLD.2 Security Enforcing High-level Design	selection of EAL 3, EAL 4, O.Lifecycle security
ADV_IMP.1 Subset of the Implementation of the TSF	selection of EAL 4, O.Lifecycle security
ADV_LLD.1 Descriptive Low-level Design	selection of EAL 4, O.Lifecycle security
ADV_RCR.1 Informal Correspondence Demonstration	O.Lifecycle security, selection of EAL 1, EAL-CSPP, EAL 3, EAL 4
ADV_SPM.1 Informal TOE Security Policy Model	selection of EAL-CSPP, EAL 4, O.Lifecycle security
AGD_ADM.1 Administrator Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.Auditors Review Audit

Assurance Requirement	Objective
	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 EAL 1, EAL-CSPP, EAL 3, EAL 4
AGD_USR.1 User Guidance	O.Administrators, Operators, Officers and Auditors guidance documentation, O.Malicious Code Not Signed, O.Procedures for preventing malicious code, O.Require inspection for downloads, selection of EAL 1, EAL-CSPP, EAL 3, EAL 4
ALC_DVS.1 Identification of Security Measures	selection of EAL-CSPP, EAL 3, EAL 4
ALC_FLR.3 Systematic Flaw Remediation	O.Lifecycle security, O.Repair identified security flaws, selection of EAL-CSPP, EAL4 augmented
ALC_LCD.1 Developer Defined Life-cycle Model	selection of EAL 4
ALC_TAT.1 Well-defined Development Tools	selection of EAL 4
ATE_COV.2 Analysis of Coverage	selection of EAL-CSPP, EAL 3, EAL 4
ATE_DPT.1 Testing – High-Level Design	selection of EAL-CSPP, EAL 3
ATE_FUN.1 Functional Testing	selection of EAL-CSPP, EAL 3, EAL 4
ATE_IND.2 Independent Testing – Sample	selection of EAL-CSPP, EAL 3, EAL 4
AVA_MSU.2 Validation of Analysis	selection of EAL-CSPP, EAL 4
AVA_SOF.1 Strength of TOE Security Function Evaluation	selection of EAL-CSPP, EAL 3, EAL 4
AVA_VLA.4 Highly Resistant Vulnerability Analysis	selection of EAL-CSPP, EAL 3, EAL 4

8.2.2 Security Requirements Sufficiency

8.2.2.1 Security Objectives for the TOE

8.2.2.1.1 Authorized Users

O.Certificates is provided by **FDP_CIMC_CER.1 (Certificate Generation)** which ensures that certificates are valid, **FDP_CIMC_CRL.1 (Certificate revocation list validation)**, and **FDP_CIMC_CSE.1 (Certificate status export)** 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 cannot obtain a bad certificate by obtaining a user's authenticator from the TOE and then using that authenticator to obtain a bad certificate.

8.2.2.1.2 System

O.Preservation/trusted recovery of secure state is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)** which covers the requirement that the state of the system be preserved so that it can be recovered in the event of a secure component failure.

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

8.2.2.1.3 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.

8.2.2.1.4 Cryptography

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

8.2.2.2 Non-IT Security Objectives for the Environment

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.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_LLD.1 (Descriptive low-level design), ADV_RCR.1 (Informal correspondence demonstration), and ADV_SPM.1 (Information TOE security policy model) which cover the requirement that security is designed into the CIMC. ALC_FLR.2 (Flaw reporting procedures) covers the requirement that flaws are detected and resolved during the operational phase.

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

8.2.2.3 IT Security Objectives for the Environment

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

O.Respond to possible loss of stored audit records is provided by **FAU_STG.4 (Prevention of audit data loss) (iterations 1)** 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.2 (User authentication before any action) (iterations 1)** which covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.

8.2.2.4 Security Objectives for the TOE and Environment

O.Configuration Management is provided by **FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2)** which covers the requirement that only authorized users can change the configuration of the system. **FMT_MOF_CIMC.3 (Extended certificate profile management)** covers the requirement that Administrators be able to control the types of information that are included in generated certificates. **FMT_MOF_CIMC.5 (Extended certificate revocation list profile management)** covers the requirement that Administrators be able to control to the types of information that are included in generated certificate revocation lists. **O.Configuration Management** is supported by **AGD_ADM.1 (Administrator Guidance)** which covers the requirement that Administrators be provided with documentation describing the configuration management features of the TOE and by **A.Competent Administrators, 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_ETC_CIMC.5 (Extended user private and secret key export)** and **FMT_MTD_CIMC.7 (Extended TSF private and secret key export)** that cover the requirement that private and secret keys be protected when they are transmitted to and from the TOE. **O.Data import/export** is also supported by **FDP_UCT.1 (Basic data exchange confidentiality) (iteration 1)** which covers the requirement that data other than private and secret keys be protected when they are transmitted to and from the CIMC.

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.2 (User identification before any action) (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)** cover the requirement that the date and time of audited events are recorded in the audit records along with the identities of the entities responsible for the actions. **FMT_MTD.1 (Management of TSF data)** covers the requirement that audit data be available for review by ensuring that users, other than Auditors, cannot delete audit logs. Finally, **FAU_SAR.1 (Audit review)** and **FAU_SAR.3 (Selectable audit review)** cover the requirement that the audit records are made available for review so that individuals can be held accountable for their actions.

O.Integrity protection of user data and software is provided by FDP**_ITT.1 (Basic internal transfer protection) (iteration 1)** 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.2 (User authentication before any action) (iterations 1)**, and **FIA_UID.2 (User identification before any action) (iterations 1 and 2)**.

FIA_UAU.2 (User authentication before any action) (iteration 1) and **FIA_UID.2 (User identification before any action) (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 cannot 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)** covers the requirement to be able to recover to a viable state.

O.Procedures for preventing malicious code is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** which ensures that only signed code can be executed and **AGD_ADM.1 (Administrator Guidance), AGD_USR.1 (User Guidance)** and **A.Malicious Code Not Signed** which ensure that those who are capable of signing code do not to sign malicious code. It is also supported by **FDP_ACF_CIMC.2 (User private key confidentiality protection), FDP_ACF_CIMC.3 (User secret key confidentiality protection), FCS_CKM.4 (Cryptographic key destruction) and FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** which ensure that an untrusted entity cannot 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)** 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. At Security Level 3, where the threat of malicious activity is greater, **FAU_STG.1 (Protected audit trail storage) is** required so that modifications to the audit log is prevented.

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

8.3 Assurance Requirements Rationale

CIMCs designed to meet SL3 may be appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. SL3 requires additional integrity controls to ensure data is not modified. A CIMC at SL3 includes protections to protect against someone with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

The assurance level for SL3 is EAL 3 augmented. Augmentation results from the selection of:

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

ADO_DEL.2 Detection of Modification
A vendor can be expected to use a signature or other method to ensure that the code has not been tampered with prior to installation. Since the product is security related, this type of precaution should be expected.

ADV_FSP.2 Fully Defined External Interfaces
It is not a difficult task to fully define all external interfaces to the product. Indeed, this is necessary to correctly develop the product for interaction with other products. This will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ADV_IMP.1 Subset of the Implementation of the TSF
This high a level of assurance requires that additional documentation regarding the implementation of the product be provided. It is through examination of this portion of the implementation that the product can be adequately evaluated with regard to the requirements.

ADV_LLD.1 Descriptive Low-level Design
This high a level of assurance requires that additional documentation regarding the design of the product be provided. It is through examination of this design that the product can be adequately evaluated with regard to the requirements.

ADV_SPM.1 Informal TOE Security Policy Model
While the generation of a security policy does require security expertise, this can be performed by a consultant (if necessary) and does not otherwise impact the vendor's existing development process at SL 3.

ALC_FLR.2 Flaw Report Procedures
EAL 3 and EAL 4 do not have the ALC_FLR component. It is within best commercial practices for a vendor of security products to have flaw reporting procedures covering: - Addressing user reported problems - Correcting flaws - Notifying users and - Revising procedures to reduce the potential for introducing new and/or additional flaws. Specific procedures are not defined in the assurance requirement; therefore this should have minimal impact on vendors who have already implemented a flaw-reporting program.

ALC_TAT.1 Well-defined Development Tools
It is important that very secure products be unambiguous.

AVA_MSU.2 Validation of Analysis Components
A security vendor implementing standard, best commercial practices will not be impacted by this component. AVA_MSU.2 requires that the vendor produce user and administrator documentation that is adequate for understanding the operating modes of the TOE and the required external security controls necessary for secure operation. The vendor is required to analyze this documentation for conformance to the requirements.

AVA_VLA.2 Independent Vulnerability Analysis
Penetration attacks are very likely given the threat model for SL 3. As a result, it is important that some penetration analysis and testing be performed.

8.3.1 Rationale for EAL 4 Augmented

With the exception of ALC_FLR.2, the EAL 3 augmentations in the CIMC SL3 PP bring the assurance level nearly to EAL 4. As a result, EAL 4 augmented has been selected as the overall assurance level for the TOE.

The ST increases the amount of assurance the TOE evaluation results will provide compared to the amount of assurance that is mandated by the SL3 in the CIMC PP. Assurance is increased by either adding new assurance requirements or by replacing those in the CIMC SL3 PP with requirements that are hierarchical to them. Given that the statement of objectives have not changed while the assurance has increased, it is clear that the resulting set of assurance requirements are sufficient and appropriate.

The additional requirements necessary to bring the assurance level to EAL 4 augmented are rationalized below:

ACM_AUT.1 Partial CM Automation
Automation in the configuration management system can help reduce the risk of human error or negligence.

ACM_CAP.4 Generation Support and Acceptance Procedures
It is important that changes to the TOE be appropriately controlled. This requirement helps to ensure that when changes are made, they are appropriate and correctly applied to the resulting TOE.

ALC_LCD.1 Developer Defined Life-cycle Model
A life-cycle definition establishes engineering practices throughout the development and maintenance of the TOE that increase confidence that the resulting TOE correctly implements the desired functionality.

To further augment EAL 4, the following assurance requirements have also been added. Several of them, as noted below, replace requirements that they are hierarchical to resulting in providing additional assurance.

ALC_FLR.3 replaced ALC_FLR.2 and provides additional assurance that flaws in the TOE will be corrected and that TOE users will receive the corrections.

AVA_VLA.4 replaced AVA_VLA.2 and provides additional assurance that exploitable vulnerabilities in the TOE are minimized.

8.4 Requirement Dependency Rationale

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

8.4.1 Rationale that Dependencies are Satisfied

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

8.4.1.1 SFR Dependencies

The following table provides a summary of the SFR dependency analysis.

Table 19 Summary of Security Functional Requirements Dependencies for Security Level 3

Component	Dependencies	Which is:
FAU_GEN.1 Audit Data Generation	FPT_STM.1 Reliable Time Stamps	Included
FAU_GEN.2 User Identity Association	FAU_GEN.1 Audit Data Generation	Included
	FIA_UID.1 Timing of Identification	Included (FIA_UID.2 which is hierarchical to FIA_UID.1)
FAU_SAR.1 Audit Review	FAU_GEN.1 Audit Data Generation	Included
FAU_SAR.3 Selectable Audit Review	FAU_SAR.1 Audit Review	Included
FAU_SEL.1 Selective Audit	FAU_GEN.1 Audit Data Generation	Included
	FMT_MTD.1 Management of TSF Data	Included
FCO_NRO_CIMC.3 Enforced Proof of Origin and Verification of Origin	FIA_UID.1 Timing of Identification	Included (FIA_UID.2 which is hierarchical to FIA_UID.1)
FCO_NRO_CIMC.4 Advanced Verification of Origin	FCO_NRO_CIMC.3 Enforced Proof of Origin and Verification of Origin	Included
FCS_CKM.1 Cryptographic Key Generation	FCS_CKM.2 Cryptographic Key Distribution or FCS_COP.1 Cryptographic Operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic Key Destruction	Included
	FMT_MSA.2 Secure Security Attributes	Included
FCS_CKM.4 Cryptographic Key Destruction	FDP_ITC.1 Import of User Data without Security Attributes or FCS_CKM.1 Cryptographic Key Generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure Security Attributes	Included
FCS_CKM_CIMC.5 CIMC Private and Secret Key Zeroization	FCS_CKM.4 Cryptographic Key Destruction	Included
	FDP_ACF.1 Security Attribute Based Access Control	Included
FCS_COP.1 Cryptographic Operation	FCS_CKM.4 Cryptographic Key Destruction	Included
	FDP_ITC.1 Import of User Data without Security Attributes or FCS_CKM.1 Cryptographic Key Generation	FCS_CKM.1 Included

Component	Dependencies	Which is:
	FMT_MSA.2 Secure Security Attributes	Included
FDP_ACC.1 Subset Access Control	FDP_ACF.1 Security Attribute Based Access Control	Included
FDP_ACF.1 Security Attribute Based Access Control	FDP_ACC.1 Subset Access Control	Included
	FMT_MSA.3 Static Attribute Initialization	Included
FDP_ACF_CIMC.2 User Private Key Confidentiality Protection	None	
FDP_ACF_CIMC.3 User Secret Key Confidentiality Protection	None	
FDP_CIMC_BKP.1 CIMC Backup and Recovery	FMT_MOF.1 Management of Security Functions Behavior	Included
FDP_CIMC_BKP.2 Extended CIMC Backup and Recovery	FDP_CIMC_BKP.1 CIMC Backup and Recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate Revocation List Validation	None	
FDP_CIMC_CSE.1 Certificate Status Export	None	
FDP_ETC_CIMC.5 Extended User Private and Secret Key Export	None	
FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action	None	
FIA_AFL.1 Authentication Failure Handling	FIA_UAU.1 Timing of Authentication	Included (FIA_UAU.2 which is hierarchical to FIA UAU.1)
FIA_ATD.1 User Attribute Definition	None	
FIA_UAU.2 User Authentication Before any Action	FIA_UID.1 Timing of Identification	Included (FIA_UID.2 which is hierarchical to FIA_UID.1)
FIA_UID.2 User Identification Before any Action	None	
FIA_USB.1 User-subject Binding	FIA_ATD.1 User Attribute Definition	Included
FMT_MOF.1 Management of Security Functions Behavior	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
	FMT_SMF.1 Specification of Management Functions	Included
FMT_MOF_CIMC.3 Extended Certificate Profile Management	FMT_MOF.1 Management of Security Functions Behavior	Included
	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
FMT_MOF_CIMC.5 Extended Certificate Revocation List Profile Management	FMT_MOF.1 Management of Security Functions Behavior	Included
	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
FMT_MSA.1 Management of Security Attributes	FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control	Included
	FMT_SMF.1 Specification of Management Functions	Included

Component	Dependencies	Which is:
	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
FMT_MSA.2 Secure Security Attributes	ADV_SPM.1 Informal TOE Security Policy Model	Included
	FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control	FDP_ACC.1 Included
	FMT_MSA.1 Management of Security Attributes	Included
	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
FMT_MSA.3 Static Attribute Initialization	FMT_MSA.1 Management of Security Attributes	Included
	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
FMT_MTD.1 Management of TSF Data	FMT_SMR.1 Security Roles	Included (FMT_SMR.2 which is hierarchical to FMT_SMR.1)
	FMT_SMF.1 Specification of Management Functions	Included
FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection	None	
FMT_MTD_CIMC.5 TSF Secret Key Confidentiality Protection	None	
FMT_MTD_CIMC.6 TSF Private and Secret Key Export	None	
FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export	FMT_MTD_CIMC.6 TSF Private and Secret Key Export	Included
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.2 Restrictions on Security Roles	FIA_UID.1 Timing of Identification	Included (FIA_UID.2 which is hierarchical to FIA_UID.1)
FPT_AMT.1 Abstract Machine Testing	None	
FPT_TST_CIMC.2 Software/Firmware Integrity Test	FPT_AMT.1 Abstract Machine Testing	Included
FPT_TST_CIMC.3 Software/Firmware Load Test	FPT_AMT.1 Abstract Machine Testing	Included
FTP_TRP.1 Trusted Path	None	

8.4.1.2 SAR Dependencies

The following table provides a summary of the SARs dependency analysis.

Table 20 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)
ACM_CAP.4	ACM_SCP.1	Included (hierarchical to ACM_SCP.2)
	ALC_DVS.1	Included

Component	Depends On:	Which is:
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
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.3	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

Component	Depends On:	Which is:
	(indirect) ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	Included
ATE_FUN.1	no dependencies	not applicable
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.4	ADV_FSP.1	Included (hierarchical to ADV_FSP.2)
	ADV_HLD.2	Included
	ADV_IMP.1	Included
	ADV_LLD.1	Included
	AGD_ADM.1	Included
	AGD_USR.1	Included
	(indirect) ADV_RCR.1	Included
	(indirect) ALC_TAT.1	Included

8.4.2 Rationale that Requirements are Mutually Supportive

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

8.4.2.1 Bypass

Prevention of bypass is derived as described below:

FIA_UID.2 and FIA_UAU.2 support other functions' allowing user access to data by not allowing the user to take any actions prior to identification and authentication.

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

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

8.4.2.2 Tamper

Prevention of tamper is derived as described below:

FAU_STG.1 protects the integrity of the audit trail.

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

FIA_UID.2 and FIA_UAU.2 support other functions by not allowing a user to take any actions prior to identification and authentication.

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

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

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

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.

8.4.2.3 Deactivation

Prevention of deactivation is derived as described below:

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

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

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

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

8.4.2.4 Detection

Detection is derived as described below:

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

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

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

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

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

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

8.5 Explicitly Stated Requirements Rationale

This ST includes a number of explicitly stated requirements. Each of the explicitly stated requirements is defined in the CIMC PP and rationale immediately follows the statement of each such requirement. The explicitly stated requirements can be identified by the use of the keyword “CIMC” in the requirement component and element identifiers.

This ST includes additional SARs that are not included in CIMC PP SL3. These requirements serve to require some automated tools to be used in configuration management (ACM_AUT.1), require the configuration management system to include an acceptance plan and support generation of the TOE (ACM_CAP.4), require a life-cycle model and with provisions for controlling the development and maintenance of the TOE (ALC_LCD.1), and a systematic approach to address security flaws (ALC_FLR.3). As such, these requirements are generally applicable to the management, generation and control of the development of the TOE and are therefore applicable to the TOE regardless of its security functional requirements (including those explicitly defined in CIMC PP SL3).

8.6 TOE Summary Specification Rationale

The following table describes the association between the TSF and the TOE SFRs. This table in conjunction with rationale provided in Section 6.1 demonstrates that the TOE SFRs are satisfied.

Table 21 Security Function to TOE SFR Mapping

Security Function	Security Functional Components
Identification	FIA_UID.2 User Timing of Identification Before any Action (iteration 2)
	FIA_USB.1 User-subject Binding (iteration 2)
Access Control	FDP_ACC.1 Subset Access Control (iteration 2)
	FDP_ACF.1 Security Attribute Based Access Control (iteration 2)
	FPT_RVM.1 Non-bypassability of the TSP (iteration 2)
Roles	FMT_MOF.1 Management of Security Functions Behavior (iteration 2)
Security Audit	FAU_GEN.1 Audit Data Generation (iteration 2)
	FAU_GEN.2 User Identity Association (iteration 2)
	FAU_SEL.1 Selective Audit (iteration 2)
Backup & Recovery	FDP_CIMC_BKP.1 CIMC Backup and Recovery
	FDP_CIMC_BKP.2 Extended CIMC Backup and Recovery
Remote Data Entry & Export	FCO_NRO_CIMC.3 Enforced Proof of Origin and Verification of Origin
	FCO_NRO_CIMC.4 Advanced Verification of Origin
	FDP_CIMC_CSE.1 Certificate Status Export
Key Management	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_ETC_CIMC.5 Extended User Private and Secret Key Export

Security Function	Security Functional Components
	FDP_SDI_CIMC.3 Stored Public Key Integrity Monitoring and Action
	FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection
	FMT_MTD_CIMC.5 TSF Secret Key Confidentiality Protection
	FMT_MTD_CIMC.7 Extended TSF Private and Secret Key Export
Certificate Management	FDP_CIMC_CER.1 Certificate Generation
	FDP_CIMC_CRL.1 Certificate Revocation
	FMT_MOF_CIMC.3 Extended Certificate Profile Management
	FMT_MOF_CIMC.5 Extended Certificate Revocation List Profile Management

Section 6.2 provides descriptions of how the TOE Security Assurance requirements are satisfied.

8.7 Strength of Function (SOF) Rationale

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

8.8 PP Claims Rationale

As indicated in Section 7, Microsoft Certificate Services complies with CIMC SL3 PP, Version 1.0, October 31, 2001. All of the security objectives and security requirements defined in the CIMC SL3 PP have been reproduced in this ST with the following exceptions: ACM_CAP.4 replaced ACM_CAP.3; ALC_FLR.3 replaced ALC_FLR.2. All applicable operations left uncompleted in the CIMC SL3 PP have been completed in this ST in accordance with the bounds set forth by the CIMC SL3 PP. This ST has introduced no additional security objectives or security requirements, with the following exceptions: ACM_AUT.1, ACM_CAP.4, ALC_LCD.1, ALC_FLR.3. These security assurance requirements have been introduced to raise the overall assurance level from EAL 3 augmented to EAL 4 augmented. These security assurance requirements correspond to existing security objectives and serve to increase the overall assurance of the TOE without impacting CIMC PP SL3 compliance.

9. Access Control Policies

9.1 CIMC IT Environment Access Control Policy

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

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

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

Subject identification includes:

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

Access type, with explicit allow or deny:

- Read
- Write
- Execute

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

9.2 CIMC TOE Access Control Policy

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

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

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

Subject identification includes:

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

Access type, with explicit allow or deny:

- Read
- Write
- Execute

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

10. Glossary of Terms

The following definitions are used throughout this standard:

Authentication code: a cryptographic checksum, based on a FIPS-approved or recommended security method; also known as a Message Authentication Code (MAC) in ANSI standards.

CIMC: the set of hardware, software, firmware, or some combination thereof, that issues, revokes, and manages public key certificates and certificate status information, and is contained within the CIMC boundary.

CIMC boundary: an explicitly defined contiguous perimeter that establishes the physical bounds of a CIMC.

Compromise: the unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: the property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a CIMC or the security of the information protected by the CIMC.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- a keyed hash computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic key component (key component): a parameter used in conjunction with other key components in a FIPS-approved or recommended security method to form a plaintext cryptographic key or perform a cryptographic function.

Digital signature: a non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.

Encrypted key: a cryptographic key that has been encrypted with a key encrypting key, a PIN or a password in order to disguise the value of the underlying plaintext key.

Error detection code (EDC): a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

FIPS-Approved or recommended mode of operation: a mode that employs only the operation of FIPS-approved or recommended security methods.

FIPS-approved or recommended security method: a security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, authentication technique, or evaluation criteria) that is either a) specified in a FIPS or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

Firmware: the programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. *Hardware*: the physical equipment used to process programs and data in a CIMC.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, passwords) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal Identification Number (PIN): a 4 or more character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

Physical protection: the safeguarding of a CIMC, cryptographic keys, or other CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Private key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Protection Profile: an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. (Public keys are not considered CSPs.)

Public key certificate: a set of data that unambiguously identifies an entity, contains the entity's public key, is digitally signed by a trusted party, and binds the public key to the entity.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does not imply a classification level rather the term implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Security policy: a precise specification of the security rules under which a CIMC shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.

Software: the programs and associated data that can be dynamically written and modified.

Split knowledge: a condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Trusted path: a means by which an operator and a TSF can communicate with the necessary confidence to support the TSP.

User: an individual, or a process (subject) operating on behalf of the individual, accessing CIMC.

Zeroization: a method of erasing electronically stored data by altering or deleting the contents of the data storage so as to prevent the recovery of the data.

11. Acronyms

ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
CA	Certificate Authority
CC	Common Criteria
CCEVS	CC Evaluation and Validation Scheme
CIMC	Certificate Issuing and Management Component
CMC	Certificate Management protocol using CMS
CMS	Content Management System
COM	Component Object Model
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
DCOM	Distributed COM
DLL	Dynamic Link Library
DN	Domain Name
DoS	Denial of Service
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HSM	Hardware Cryptographic Security Module
I&A	Identification and Authentication
ID	Identification
IEC	International Electro-technical Commission

IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OS	Operating System
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Request for Comment
SAM	Security Assurance Measure
SAR	Security Assurance Requirement
SD	Security Descriptor
SID	Security Identifier
SF	Security Functions
SFR	Security Functional Requirement
SL3	Security Level 3
SMB	Server Message Block
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report