Netscape Certificate Management System 6.1 Service Pack 1 Security Target

Revision 1.0
March 12, 2003

Prepared for:
America Online, Inc.

466 Ellis Street
Mountain View, CA, 94043-4042

Prepared By:

Science Applications International Corporation

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. SECURITY TARGET INTRODUCTION 6

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 6
1.2 CONFORMANCE CLAIMS 6
1.3 STRENGTH OF ENVIRONMENT 6
1.4 CONVENTIONS, TERMINOLOGY, ACRONYMS 7
1.4.1 Conventions 7
1.4.2 Terminology and Acronyms 7
1.5 SECURITY TARGET OVERVIEW AND ORGANIZATION 8

2. TOE DESCRIPTION 9

2.1 PRODUCT TYPE 13
2.2 PRODUCT DESCRIPTION 13
2.3 PRODUCT FEATURES 13
2.3.1 Security Functions 13
2.3.1.1 Identification & Authentication 13
2.3.1.2 Access Control 14
2.3.1.3 Security Management 14
2.3.1.4 Security Audit 14
2.3.1.5 Backup & Recovery 14
2.3.1.6 Remote Data Entry & Export 14
2.3.1.7 Key Management 14
2.3.1.8 Certificate Management 14
2.4 SECURITY ENVIRONMENT TOE BOUNDARY 14
2.4.1 Physical Boundaries 14
2.4.2 Logical Boundaries 15

3. SECURITY ENVIRONMENT 16

3.1 SECURE USAGE ASSUMPTIONS 16
3.1.1 Personnel Assumptions 16
3.1.2 Physical Assumptions 17
3.1.3 Connectivity Assumptions 17
3.2 THREATS 17
3.2.1 Authorized Users 17
3.2.2 System 17
3.2.3 Cryptography 18
3.2.4 External Attacks 18
3.3 ORGANIZATION SECURITY POLICIES 18

4. SECURITY OBJECTIVES 19

4.1 SECURITY OBJECTIVES FOR THE TOE 19
4.1.1 Authorized Users 19
4.1.2 System 19
4.1.3 Cryptography 19
4.1.4 External Attacks 19
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 19
4.2.1 Non-IT security objectives for the environment 19
4.2.2 IT security objectives for the environment 20
4.3 SECURITY OBJECTIVES FOR BOTH THE TOE AND THE ENVIRONMENT 21

5. IT SECURITY REQUIREMENTS 23

5.1 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 23
5.1.1 Security Audit (FAU) 23
5.1.2 Cryptographic support (FCS) 25

5.1.3 User Data Protection (FDP) *25*
5.1.4 Identification and authentication (FIA) *26*
5.1.5 Security management (FMT) *27*
5.1.6 Protection of the TSF (FPT) *28*
5.1.7 Trusted path/channels (FTP) *29*
5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 30
5.2.1 Security Audit (FAU) *31*
5.2.2 Communication (FCO) *33*
5.2.3 Cryptographic support (FCS) *34*
5.2.4 User Data Protection (FDP) *34*
5.2.5 Identification and authentication (FIA) *39*
5.2.6 Security management (FMT) *39*
5.2.7 Protection of the TSF (FPT) *42*
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 43
5.3.1 Configuration Management (ACM) *44*
5.3.2 Delivery and Operation (ADO) *45*
5.3.3 Development (ADV) *46*
5.3.4 Guidance Documents (AGD) *49*
5.3.5 Life Cycle Support (ALC) *50*
5.3.6 Security Testing (ATE) *51*
5.3.7 Vulnerability Assessment (AVA) *52*
5.4 STRENGTH OF FUNCTION REQUIREMENTS 54
5.4.1 Authentication Mechanisms *54*
5.4.2 Cryptographic Modules *54*
5.4.2.1 Encryption and FIPS 140-1 Validated Modules 54
5.4.2.2 Cryptographic module levels for cryptographic functions that involve private or secret keys 55
5.4.2.3 Cryptographic Functions That Do Not Involve Private or Secret Keys 56

6. TOE SUMMARY SPECIFICATION 57

6.1 TOE SECURITY FUNCTIONS 57
6.1.1 Identification & Authentication *57*
6.1.2 Access Control *58*
6.1.3 Security Management *58*
6.1.3.1 CMS Privileged Users and Groups (Roles) 58
6.1.3.2 About Roles 61
6.1.3.3 Access Rules: 61
6.1.4 Security Audit *63*
6.1.5 Backup & Recovery *65*
6.1.6 Remote Data Entry & Export *65*
6.1.7 Key Management *66*
6.1.8 Certificate Registration, Certificate Revocation, OCSP Basic Response Validation and Their Profile Management *67*
6.2 TOE SECURITY ASSURANCE MEASURES 68
6.2.1 Process Assurance *68*
6.2.1.1 Configuration Management 68
6.2.1.2 Life cycle support 69
6.2.2 Delivery and Guidance *69*
6.2.3 Development *69*
6.2.4 Tests *70*
6.2.5 Vulnerability Assessment *70*
6.2.5.1 Evaluation of Misuse 70
6.2.5.2 Strength of TOE Security Functions 71
6.2.5.3 Vulnerability Analysis 71

7. PROTECTION PROFILE CLAIMS 72

8. RATIONALE 73

8.1 SECURITY OBJECTIVES RATIONALE 73
8.1.1 Security Objectives Sufficiency 75
8.1.1.1 Threats and Objectives Sufficiency 75
8.1.1.2 Policies and Objectives Sufficiency 81
8.1.1.3 Assumptions and Objectives Sufficiency 82
8.2 SECURITY REQUIREMENTS RATIONALE 83
8.2.1 Security Requirements Coverage 83
8.2.2 Security Requirements Sufficiency 86
8.2.2.1 Security Objectives for the TOE 86
8.2.2.2 Non-IT Security Objectives for the Environment 86
8.2.2.3 IT Security Objectives for the Environment 87
8.2.2.4 Security Objectives for the TOE and Environment 88
8.3 ASSURANCE REQUIREMENTS RATIONALE 90
8.3.1 Rationale for EAL 4 92
8.4 REQUIREMENT DEPENDENCY RATIONALE 92
8.4.1 Rationale that Dependencies are Satisfied 92
8.4.1.1 Security Functional Requirements Dependencies 92
8.4.1.2 Security Assurance Requirements Dependencies 95
8.4.2 Rationale that Requirements are Mutually Supportive 97
8.4.2.1 Bypass 97
8.4.2.2 Tamper 97
8.4.2.3 Deactivation 98
8.4.2.4 Detection 98
8.5 EXPLICITLY STATED REQUIREMENTS RATIONALE 99
8.6 TOE SUMMARY SPECIFICATION RATIONALE 99
8.7 STRENGTH OF FUNCTION (SOF) RATIONALE 100
8.8 PP CLAIMS RATIONALE 100

9. ACCESS CONTROL POLICIES 101

9.1 CIMC IT ENVIRONMENT ACCESS CONTROL POLICY 101
9.2 CIMC TOE ACCESS CONTROL POLICY 101

10. GLOSSARY OF TERMS 102

11. ACRONYMS 105

LIST OF TABLES

Table 1 IT Environment Functional Security Requirements 23
Table 2 Auditable Events and Audit Data 24
Table 3 Audit Search Criteria 25
Table 4 Authorized Roles for Management of Security Functions Behavior 27
Table 5 CIMC TOE Functional Security Requirements 30
Table 6 Auditable Events and Audit Data 31
Table 7 Access Controls 34
Table 8 Authorized Roles for Management of Security Functions Behavior 39
Table 9 Assurance Requirements (EAL 4 augmented) 43
Table 10 FIPS 140-1 Level for Validated Cryptographic Module 55
Table 11 Role Restrictions 61
Table 12 Auditable Events 63
Table 13 Relationship of Security Objectives for the TOE to Threats 73
Table 14 Relationship of Security Objectives for the Environment to Threats 73
Table 15 Relationship of Security Objectives for Both the TOE and the Environment to Threats 74

Table 16 Relationship of Organizational Security Policies to Security Objectives 74
Table 17 Relationship of Assumptions to IT Security Objectives 75
Table 18 Security Functional Requirements Related to Security Objectives 83
Table 19 Security Assurance Requirements Related to Security Objectives 85
Table 20 Summary of Security Functional Requirements Dependencies for Security Level 3 92
Table 21 Summary of Security Assurance Requirements Dependencies for Security Level 3 95
Table 22 Security Function to TOE SFR Mapping 99

LIST OF FIGURES

Figure 1 CMS6.1 System Overview 12

1. Security Target Introduction

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

1.1 Security Target, TOE and CC Identification

ST Title – Netscape Certificate Management System 6.1 Service Pack 1 Security Target

ST Version – Revision 1.0

ST Date – March 12, 2003

TOE Identification – Netscape Certificate Management System 6.1 Service Pack 1

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

1.2 Conformance Claims

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
    - Part 2 extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 conformant
    - Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2
- Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001.

1.3 Strength of Environment

Netscape Certificate Management System 6.1 Service Pack 1 (CMS6.1) is appropriate for environments where risks and consequences of data disclosure and loss of data integrity are moderate. Certificate Issuing and Management Component (CIMC) Security Level 3 (SL3) requires integrity controls to ensure data is not modified. A CIMC at SL3, such as CMS6.1, includes protections to protect against someone with physical access to the components and includes assurance requirements to ensure the CIMC is functioning securely.

SL3 provides some protection against malicious authorized users by requiring at least distinct roles. One role will be responsible for account administration, key generation, and audit configuration; a second role will be responsible for issuing and revoking certificates; and a third role responsible for maintaining the audit logs. SL3 requires two-party control of private key export and additional auditing of import and export of secret and private keys and requests for information. Cryptographic modules responsible for long-term private key protection or for signing certificates or certificate status information must be validated to FIPS 140-1 Level 3. Finally, there is increased public key protection and digital signatures are required on all messages.

At SL3, the applicable CC assurance level is EAL 3 (methodically tested and checked) augmented by selected requirements from EAL 4 (methodically designed, tested and reviewed). However, since the SL3 augmentations to EAL 3 bring the overall assurance nearly to EAL 4, EAL 4 (augmented with ALC_FLR.2) has been adopted as the overall assurance level for CMS6.1. An EAL 4 evaluation includes an analysis supported by “gray box” testing,

selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. EAL 4 also includes an analysis supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities.

To ensure that the risks of the target environment are adequately countered, SL3 requires a minimum strength of function (SOF) level of basic, with the exception of specific SOF requirements for authentication and encryption functions. The specific SOF requirements can be found in Section 5.4.1 (Authentication Mechanisms) and Section 5.4.2 (Cryptographic Modules).

1.4 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.4.1 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.
- 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).
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4.2 Terminology and Acronyms

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

1.5 Security Target Overview and Organization

The Netscape Certificate Management System 6.1 Service Pack 1 (CMS6.1) Target of Evaluation (TOE) is a Certificate Management System offering a wide range of certificate related services. This Security Target describes the CMS6.1 TOE, intended environments, security objectives, security requirements (for the TOE and IT environment), security functions, Protection Profile claims, and all necessary rationale. This information is organized the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8)
- Access control policies (Section 9)
- Glossary of terms (Section 10)
- Acronyms (Section 11)

2. TOE Description

The Netscape Certificate Management System 6.1 Service Pack 1 (CMS6.1) provides a powerful security framework to guarantee the identity of users and ensure privacy of communications. CMS6.1 issues and manages X.509v3 certificates needed to handle strong authentication, single sign-on and secure communications. CMS6.1 handles all the major functions around the certificate lifecycle simplifying enterprise-wide deployment and adoption. Customizable registration allows CMS6.1 to adapt to virtually any enterprise security policy.

Features Overview

- Helps enterprises build a Public Key Infrastructure to issue, renew, suspend, revoke and manage single and dual-key certificates
- Integrates easily with third-party security software and existing applications through published application programming interfaces
- Allows administrators to request and install certificates onto smart cards, in real time, with minimal interaction from end users
- Scales to manage millions of digital certificates
- Supports extranet-facing security
- Supports key recovery for retrieval in the case of corrupted encryption keys
- Supports Online Certificate Status Protocol (OCSP) to give users up-to-date certificate revocation status

Strong Authentication

Unlike passwords, certificates cannot be easily reproduced. Issued by a trusted authority, digitally signed certificates provide a reliable method of verifying user identity and preventing identity theft.

Enables Single Sign-On

Single sign-on has immediate benefits for both the end user -- who only needs to remember a single password to access resources, and the administrator -- who enjoys simplified maintenance across multiple servers. Single sign-on can also lower enterprise help desk costs by reducing the volume of calls concerning lost passwords.

Digital certificates, issued by CMS6.1 and tied to users stored in Netscape® Directory Server, provide the safest way to authenticate users quickly and transparently.

Enables Secure Communications

Protecting mission-critical information is an important requirement for today's security-conscious companies. CMS6.1 issues X.509v3 certificates that allow an enterprise to encrypt critical network-based information, ensuring information privacy.

Flexible Deployment

CMS6.1 allows for flexible deployment adapting to enterprise security policies and existing investments in security solutions. Easy configuration and installation allow enterprises to tailor deployment for use with a variety of extranet and intranet applications through integration with several third-party products and customize using published application programming interfaces (APIs) for authentication, policy modules and custom extensions.

High Scalability & Manageability

CMS6.1 provides a distributed, high-performance architecture that is designed to support large deployments across employees, partners and customers and includes a centralized, Web-based

administration tool that helps administrators manage roles, logs, users and groups. A command-line interface is also available for easy automation of common tasks.

Advanced Security Features

CMS6.1 can be used with FIPS 140-1 Level 3-validated hardware. Hardware signing protects the highly sensitive CIMC component keys such as CA signing key, DRM storage key, OCSP signing key, etc., keeping them off any easily accessible desktop machine.

Integrated Applications

CMS6.1 enables enterprises to deploy Web-based authentication, form signing, Virtual Private Networks, routers, and S/MIME. CMS6.1 is fully integrated with Netscape Directory Server as well as other security solutions such as SecurID, allowing enterprises to easily leverage existing investments in security solutions.

A CMS6.1 system is composed of the following key components:

- CMS

  CMS can be configured into four different subsystems working together to provide the entire set of features. The four subsystems are:

  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Data Recovery Manager (DRM) or Key Archival and Recovery Manager (KRA)
  - Online Certificate Status Protocol (OCSP) Responder

  The CMS (CA, RA, DRM, OCSP Responder) component is the main component in CMS6.1, and is a set of pure Java classes. This component can be portable to other J2EE containers such as Netscape's Application Server that provides excellent application deployment capability, reliability, and scalability.

  The CMS component provides a secure application (service) platform where services (i.e. Certificate Authority Service, Registration Authority Service, OCSP Service, Key Archival and Recovery Service, and other Customer specific services) can be tightly integrated with a PKI infrastructure. A service that is developed on top of CMS can communicate to its users, and other CMS services securely.

- HTTP Engine (e.g., Netscape Enterprise Server)

  The web engine provides the HTML-based UI (presentation) and HTTP-based protocol handling. It does not perform authentication and authorization other than providing and/or enforcing SSL. The web engine provides the HTML-based UI (presentation) and HTTP-based protocol handling. It performs basic certificate validation and delegates all the application-specific authentication and authorization to CMS via a callback mechanism.

- Internal Database (e.g., Netscape Directory Server)

  The internal database stores information such as certificates, requests, officers/administrator information, and other information such as access control information.

The following architectural diagram shows the interactions between various CMS configurations and various internal and external systems. Internally, CMS communicates with an internal database (CMS's Internal Database) where certificate records, request records, system user records are stored. CMS also accesses the cryptographic operations via the HTTP engine. Externally, the HTTP engine manages the presentation-level interaction between CMS and users including end-users, security officers, and administrators. CMS may optionally publish certificates to a corporate LDAP directory.

In addition to the HTTP Engine and Internal Database, CMS also relies on access to processing capabilities, file storage, as well as hardware cryptographic modules provided by its IT environment.

The Non-TOE IT environments are similar among all CIMC boundaries. Please refer to CIMC Boundary 1 in Figure 1 to see complete details for all other Non-TOE IT within other CIMC boundaries.

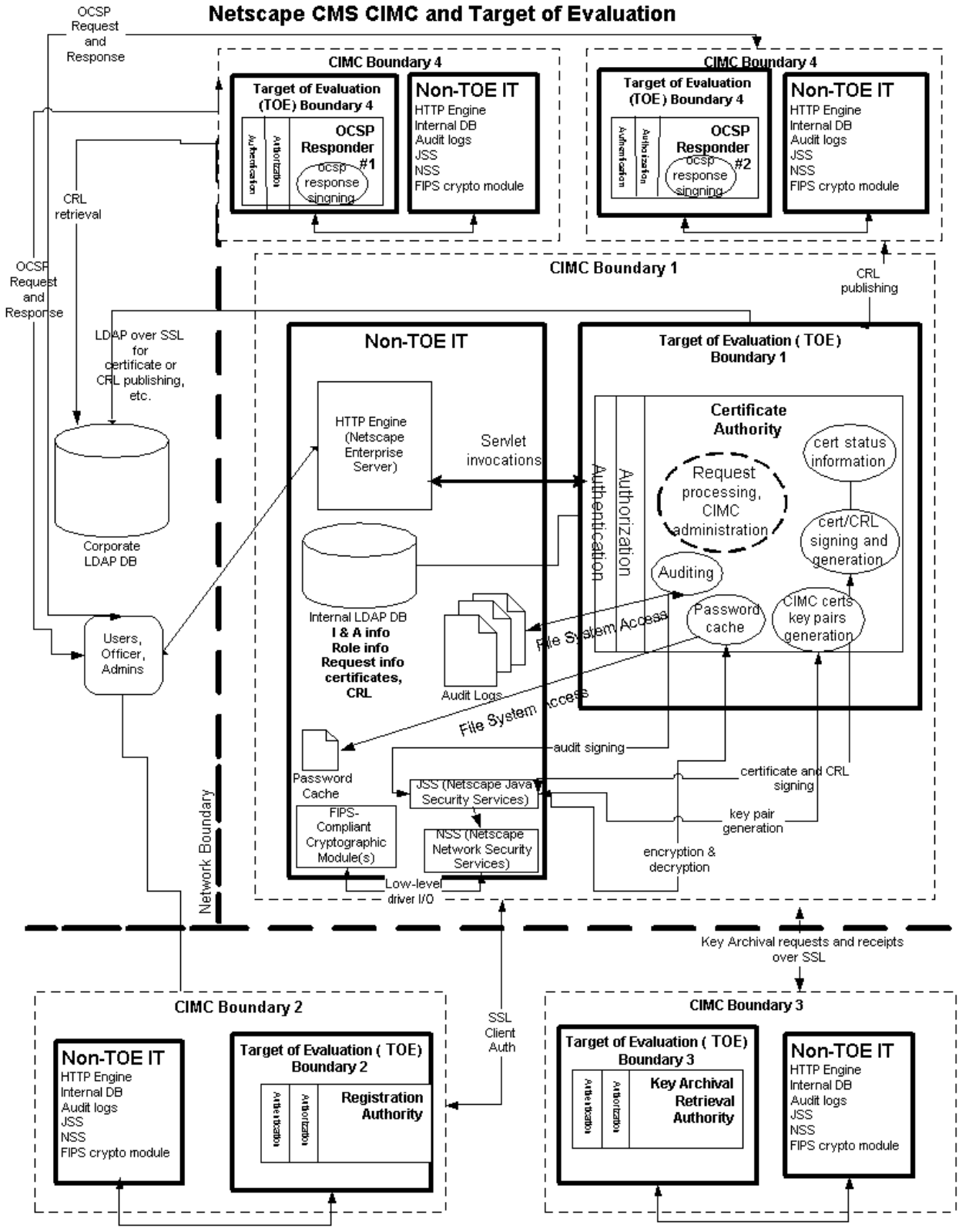

Figure 1 CMS6.1 System Overview

While a complete CMS6.1 *system* includes all of the components within the CIMC boundaries indicated in Figure 1, the CMS6.1 *TOE* includes the components within the labeled TOE Boundaries. Specifically, the CA, RA, OCSP Responder, or DRM (or KRA). The CMS6.1 TOE also includes a backup/restore utility, a single-signon password management tool, and an audit log signature verification tool. A JAVA console application is bundled with CMS6.1 that interacts securely with CMS using HTTP/S to allow administrators to manage CMS6.1. The backup/restore utility runs in the IT environment and allows an Administrator to backup or restore the CMS6.1 configuration.

2.1 Product Type

CMS6.1 is a certificate issuing and management product. As such, it offers the following general services to users and/or administrators:

- Certificate Enrollment
- Certificate Renewal
- Certificate Revocation
- Certificate Retrieval
- Request Queue Management
- Certification and Certificate Revocation List (CRL) Management
- Remote Server Request Handling
- Configuration Management
- Key Archival and Retrieval Service
- Online Certificate Status Protocol (OCSP) Responder Service

2.2 Product Description

The CMS6.1 TOE is an operating system application written in Java using associated network (Netscape Network Security Services; NSS) and java (Netscape Java Security Services; JSS) security service libraries. The CMS6.1 TOE is designed to integrate with a directory server such as Netscape Directory Server and a HTTP engine such as Netscape Enterprise server to provide an internal data store and a network interface, respectively. JSS/NSS are designed to support the use of hardware devices that perform standards-oriented cryptographic operations. All of the components represent a CMS6.1 system. A CMS6.1 system is designed to be hosted within Solaris 8.0 and to be connected to networks, including the Internet, and to offer these services using standard HTTP/SSL protocols.

CMS6.1 is designed to be installed in one of four configurations: CA, RA, OCSP Responder, or DRM. The primary difference between these configurations is the set of services offered to users.

2.3 Product Features

The CMS6.1 TOE offers the following security functions:

2.3.1 Security Functions

2.3.1.1 Identification & Authentication

CMS6.1 ensures that users are identified and authenticated before they can access any other security relevant services.

2.3.1.2 Access Control

CMS6.1 provides the ability to define an access control list for each service it provides. These access control lists are used to ensure that users can only access services they have been authorized to use.

2.3.1.3 Security Management

CMS6.1 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.

2.3.1.4 Security Audit

CMS6.1 has the capability to audit security relevant events. Audit records are generated when audit events occur, including the responsible user, date, time, and other details. Audit records are collected into audit buffers that are signed, to protect against possible tampering of the audit records, and then copied into non-volatile audit logs.

2.3.1.5 Backup & Recovery

CMS6.1 has a backup/restore utility that can be used to save a snapshot of a CMS6.1 configuration and then restore that configuration at a later date. The integrity of the backup data is protected using digital signatures.

2.3.1.6 Remote Data Entry & Export

CMS6.1 protects data import and export operations using SSL sessions.

2.3.1.7 Key Management

CMS6.1 includes a number of key management functions. In particular, CMS6.1 protects security critical keys and other information by either encrypting it or storing it within a hardware cryptographic module. CMS6.1 also uses digital signatures when appropriate to ensure the integrity of key management related information.

2.3.1.8 Certificate Management

CMS6.1 includes a number of certificate management functions. In particular, CMS6.1 allows administrators to control, limit, or mandate values in certificates, certificate revocation lists (CRLs), and online certificate status protocol (OCSP) responses that are generated.

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 HTTP-based interfaces to access the security functions of the TOE.

As depicted in Figure 1, the TOE exists as an application program interacting with other components to implement its security functions. The TOE application runs within an IT environment consisting of a Java runtime environment and is integrated with a Netscape Enterprise Server. The java runtime environment is provided by a trusted host operating system (e.g., Solaris 8). The Netscape Enterprise Server serves to offer a HTTP-based interface to users of CMS6.1.

The TOE application supports LDAP interfaces and also HTTP-based interfaces via Netscape Enterprise Server. The LDAP interfaces are used to connect to the internal LDAP Server (e.g., Netscape Directory Server) used by CMS6.1 exclusively as a private data store, and also to connect to a Corporate LDAP server for publishing purposes, if configured. The HTTP-based interfaces allow users and administrators to connect to CMS6.1 to access its security functions and to manage CMS6.1.

2.4.2 Logical Boundaries

Since the TOE is an application, its logical and physical boundaries largely coincide. The TOE requires basic execution, data storage support, and network connectivity services from its IT environment. The external interfaces are limited to LDAP and HTTP/SSL. LDAP connections are supported only when initiated by CMS6.1. The HTTP/SSL interfaces are used to offer functions via service-oriented web pages to CMS6.1 users, officers, and administrators.

Note that administrative functions are performed using a console application included with CMS6.1. This application interacts with CMS using HTTP/SSL, but instead of using HTML it uses a proprietary language to better facilitate the administrator functions available.

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 security functional requirements for the TOE and environment specified in Sections 5.1 and 5.2, and the TOE Security Assurance Requirements specified in Section 5.3.

3.1 Secure Usage Assumptions

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

3.1.1 Personnel Assumptions

A.Auditors Review Audit Logs

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

A.Authentication Data Management

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

A.Competent Administrators, 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 operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the appropriate Security Level identified in this family of PPs.[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

[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 hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.

T.Flawed code

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

3.2.3 Cryptography

T.Disclosure of private and secret keys

A private or secret key is improperly disclosed.

T.Modification of private/secret keys

A secret/private key is modified.

T.Sender denies sending information

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

3.2.4 External Attacks

T.Hacker gains access

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

T.Hacker physical access

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

T.Social engineering

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

3.3 Organization Security Policies

P.Authorized use of information

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

P.Cryptography

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

4. Security Objectives

This section includes the security objectives 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.

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 certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.

O.Disposal of Authentication Data

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

O.Installation

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

O.Malicious Code Not Signed

Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.

O.Notify Authorities of Security Issues

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

O.Physical Protection

Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.

O.Social Engineering Training

Provide training for general users, Administrators, Operators, Officers and Auditors in techniques to thwart social engineering attacks.

O.Cooperative Users

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

O.Lifecycle security

Provide tools and techniques used during the development phase to ensure security is designed into the CIMC. Detect and resolve flaws during the operational phase.

O.Repair identified security flaws

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

4.2.2 IT security objectives for the environment

O.Cryptographic functions

The TOE must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. (Validated is defined as FIPS 140-1 validated.)

O.Operating System

The operating system used is validated to provide adequate security, including domain separation and nonbypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology.

O.Periodically check integrity

Provide periodic integrity checks on both system and software.

O.Security roles

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

O.Validation of security function

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

O.Trusted Path

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

4.3 Security Objectives for both the TOE and the Environment

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

O.Configuration Management

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

O.Data import/export

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

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

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

O.Individual accountability and audit records

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

O.Integrity protection of user data and software

Provide appropriate integrity protection for user data and software.

O.Limitation of administrative access

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

O.Maintain user attributes

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

O.Manage behavior of security functions

Provide management functions to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code

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

O.Procedures for preventing malicious code

Incorporate malicious code prevention procedures and mechanisms.

O.Protect stored audit records

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

O.Protect user and TSF data during internal transfer

Ensure the integrity of user and TSF data transferred internally within the system.

O.Require inspection for downloads

Require inspection of downloads/transfers.

O.Respond to possible loss of stored audit records

Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.

O.Restrict actions before authentication

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

O.Security-relevant configuration management

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

O.Time stamps

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

O.User authorization management

Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.

O.React to detected attacks

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

5. IT Security Requirements

5.1 Security Requirements for the IT Environment

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

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.1 Timing of authentication (iteration 1)
	FIA_UID.1 Timing of identification (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) [***no additional attributes***].

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 detect modifications to the audit records.

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 [**any FIPS-approved or recommended cryptographic key generation algorithm**] that meet the following: [**FIPS 140-1**].

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 [**any FIPS-approved or recommended key destruction method**] 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 [**all cryptographic operations**] in accordance with [**FIPS-approved or recommended algorithms**].

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 [**users, files, and 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 identity of the subject and the set of roles that the subject is authorized to assume.

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

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, [**and no other security attributes**].

FIA_UAU.1 Timing of authentication (iteration 1)

FIA_UAU.1.1 The IT environment shall allow [**HTTP and LDAP based services**[2]] on behalf of the user to be performed before the user is authenticated.

[2] These are the services that are controlled by CMS6.1 and are not subject to mediation by the IT environment.

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

FIA_UID.1 Timing of identification (iteration 1)

FIA_UID.1.1 The IT environment shall allow [**HTTP and LDAP based services**] on behalf of the user to be performed before the user is identified.

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

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_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 initial start-up, periodically during normal operation, or at the request of an authorized user**] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the IT environment.

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 Security Functional Requirements

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)
	FAU_STG.1 Protected audit trail storage (iteration 2)
	FAU_STG.4 Prevention of audit data loss (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_CIMC_OCSP.1 Basic Response Validation
	FDP_ETC_CIMC.5 Extended user private and secret key export
	FDP_ITT.1 Basic internal transfer protection (iterations 3 and 4)
	FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
	FDP_UCT.1 Basic data exchange confidentiality (iteration 2)
Identification and authentication (FIA)	FIA_UAU.1 Timing of authentication (iteration 2)
	FIA_UID.1 Timing of identification (iteration 2)
	FIA_USB.1 User-subject binding (iteration 2)
Security management (FMT)	FMT_MOF.1 Management of security functions behavior (iteration 2)
	FMT_MOF_CIMC.3 Extended certificate profile management
	FMT_MOF_CIMC.5 Extended certificate revocation list profile management
	FMT_MOF_CIMC.6 OCSP Profile Management

Security Functional Class	Security Functional Components
	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_CIMC_TSP.1 Audit log signing event
	FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 2)
	FPT_ITT.1 Basic internal TSF data transfer protection (iterations 3 and 4)
	FPT_RVM.1 Non-bypassability of the TSP (iteration 2)
	FPT_STM.1 Reliable time stamps (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	
	FPT_CIMC_TSP.1 Audit log signing event	Audit log signing event	Digital signature, keyed hash, or authentication code shall be included in the audit log.
Local Data Entry		All security-relevant data that is entered in the system	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an “accept” button). This shall be included with the accepted data.
Remote Data Entry		All security-relevant messages that are received by the system	

Section/Function	Component	Event	Additional Details
Data Export and Output		All successful and unsuccessful requests for confidential and security-relevant information	
Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
Private Key Load		The loading of Component private keys	
Private Key Storage		All access to certificate subject private keys retained within the TOE for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
Secret Key Storage		The manual entry of secret keys used for authentication	
Private and Secret Key Export	FDP_ETC_CIMC.4 User private and secret key export; FMT_MTD_CIMC.6 TSF private and secret key export	The export of private and secret keys (keys used for a single session or message are excluded)	
Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
Certificate Status Change Approval		All requests to change the status of a certificate	Whether the request was Accepted or rejected.
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
Online Certificate Status Protocol (OCSP) Profile	FMT_MOF_CIMC.6 OCSP Profile	All changes to the OCSP profile	The changes made to the Profile

Section/Function	Component	Event	Additional Details
Management	Management		

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) [***no additional attributes***].

FAU_STG.1 Protected audit trail storage (iteration 2)

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

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

FAU_STG.4 Prevention of audit data loss (iteration 2)

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the Auditor, if the audit trail is full.[3]

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 [**the identity of the certificate issuer**] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

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

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.

[3] U.S. National interpretation indicates that this requirement should include the phrase "and take no other actions" after the operation that is identified as having already been performed in the CIMC PP. Since, the CIMC PP has already completed the operation, the requirement was copied verbatim from the CIMC PP, and the additional phrase does not serve to change the requirement, the requirement has been left in the original form provided by the CIMC PP.

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

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

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.

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

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 [**users, services, and access to 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 identity of the subject and the set of roles that the subject is authorized to assume.

FDP_ACF.1.2 The TSF shall enforce the rules specified in **Table 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 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

Section/Function	Component	Event
		private keys into cryptographic modules shall be restricted to Administrators.
Private Key Storage		The capability to request the decryption of certificate subject private keys shall be restricted to Officers. The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. At least two Officers or one Officer and an Administrator, Auditor, or Operator shall be required to request the decryption of a certificate subject private key.
Trusted Public Key Entry, Deletion, and Storage		The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators.
Secret Key Storage		The capability to request the loading of CIMC secret keys into cryptographic modules shall be restricted to Administrators.
Private and Secret Key Destruction		The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators, Auditors, Officers, and Operators.
Private and Secret Key Export		The capability to export a component private key shall be restricted to Administrators. The capability to export certificate subject private keys shall be restricted to Officers. The export of a certificate subject private key shall require the authorization of at least two Officers or one Officer and an Administrator, Auditor, or Operator.
Certificate Status Change Approval		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.

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

FDP_ACF_CIMC.3 User secret key confidentiality protection

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

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

FDP_CIMC_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.

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the CC. It supports the security objectives O.Object and data recovery free from malicious code and O.Preservation/trusted recovery of secure state.

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.

Rationale: This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the CC. It supports the security objectives O.Object and data recovery free from malicious code and O.Preservation/trusted recovery of secure state.

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**.
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.

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

FDP_CIMC_CRL.1 Certificate revocation list validation

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

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

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

FDP_CIMC_CSE.1 Certificate status export

FDP_CIMC_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with [**the X.509 standard for CRLs (RFC2459) and, the OCSP standard as defined by RFC 2560**].

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

FDP_CIMC_OCSP.1 OCSP basic response validation

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

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

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

FDP_ETC_CIMC.5 Extended user private and secret key export

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

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

FDP_ITT.1 Basic internal transfer protection (iteration 3)

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

FDP_ITT.1 Basic internal transfer protection (iteration 4)

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

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

FDP_SDI_CIMC.3.1 Public keys stored within the CIMC, but not within a FIPS 140-1 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 [**audit the failure**].

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

FDP_UCT.1 Basic data exchange confidentiality (iteration 2)

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

5.2.5 Identification and authentication (FIA)

FIA_UAU.1 Timing of authentication (iteration 2)

FIA_UAU.1.1 The TSF shall allow [**Certificate Enrollment Requests**[4] **and Certificate Retrieval**[5]] on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1 Timing of identification (iteration 2)

FIA_UID.1.1 The TSF shall allow [**Certificate Enrollment Requests and Certificate Retrieval**] on behalf of the user to be performed before the user is identified.

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

FIA_USB.1 User-subject binding (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

[4] Certificate Enrollment allows users to request various types of certificates. However, in order for a request to be fulfill the user must either be authenticated or an Officer must approve the request.
[5] Certificate Retrieval allows users to search, list and view certificates as well as download certificates and CRLs.

Section/Function	Component Function	Authorized Role
		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.
Data Export and Output		The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer, Auditor, or Operator.
Certificate Status Change Approval		Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.
CIMC Configuration		The capability to configure any TSF functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)
Certificate Profile Management	FMT_MOF_CIMC.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	The capability to modify the certificate revocation list profile shall be restricted to Administrators.

Section/Function	Component Function	Authorized Role
	revocation list profile management	
Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.

FMT_MOF_CIMC.3 Extended certificate profile management

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

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

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

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

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

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

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

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

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

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

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

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

FMT_MOF_CIMC.6 OCSP profile management

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

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

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

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

FMT_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.

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

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

FMT_MTD_CIMC.5.1 TSF secret keys stored 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.

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

FMT_MTD_CIMC.7 Extended TSF private and secret key export

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

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

5.2.7 Protection of the TSF (FPT)

FPT_CIMC_TSP.1 Audit log signing event

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

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

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

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

Rationale: This component is necessary to specify a unique requirement for certificate issuing and management components that is not addressed by existing CC requirements. It supports the security objective O.Protect stored audit records, by providing additional protection for stored audit records at Security Levels 2 and 3.

FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 2)

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

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 3)

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

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 4)

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

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.

FPT_STM.1 Reliable time stamps (iteration 2)

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.2 as indicated in bold 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
	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

Assurance Class	Assurance Components
	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.2 Flaw reporting procedures
	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.2 Independent 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 labelled with its reference.

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

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 CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

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 documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

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 TSPenforcing 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.1.1E 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.2 Flaw reporting procedures

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C 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.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C 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.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.6C 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.2.1E 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.

AVA_VLA.2 Independent vulnerability analysis

AVA_VLA.2.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.2.2D The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.2.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

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

AVA_VLA.2.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4E 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.2.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

5.4 Strength of Function Requirements

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

5.4.1 Authentication Mechanisms

The authentication mechanisms specified in FIA_UAU.1 iterations 1 and 2 shall meet the following strength of function 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 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 must perform all cryptographic functions performed by CIMCs. FIPS 140-1 validated cryptographic modules are also required to generate cryptographic keys and to store plaintext private and secret keys.

5.4.2.1 Encryption and FIPS 140-1 Validated Modules

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

5.4.2.1.1 Encryption Algorithms

The encryption specified for:

FAU_STG.1	Protected audit trail storage
FCO_NRO_CIMC.4	Advanced verification of origin
FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_CIMC_BKP.2	Extended CIMC backup and recovery
FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export
FPT_CIMC_TSP.1	Audit log signing event
FPT_CIMC_TSP.2	Audit log time stamp event
FPT_TST_CIMC.2	Software/firmware integrity test
FPT_TST_CIMC.3	Software/firmware load test

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

5.4.2.1.2 FIPS 140-1 Validated Cryptographic Modules

Cryptographic modules specified for:

FCS_CKM.1	Cryptographic key generation
FDP_ACF_CIMC.2	User private key confidentiality protection
FDP_ACF_CIMC.3	User secret key confidentiality protection
FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action
FMT_MTD_CIMC.4	TSF private key confidentiality protection
FMT_MTD_CIMC.5	TSF secret key confidentiality protection
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export
FPT_CIMC_TSP.1	Audit log signing event

shall be validated against FIPS 140-1.

5.4.2.1.3 Split Knowledge Procedures

Split-knowledge procedures specified in:

FDP_ETC_CIMC.4	User private and secret key export
FDP_ETC_CIMC.5	Extended user private and secret key export
FMT_MTD_CIMC.6	TSF private and secret key export
FMT_MTD_CIMC.7	Extended TSF private and secret key export

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

5.4.2.1.4 Authentication Codes

The authentication code specified in:

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

shall be a FIPS-approved or recommended authentication code.

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

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

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

Table 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	3
Long Term Confidentiality	2
Short Term Private key Protection	2
Short Term Confidentiality	1

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

5.4.2.3 Cryptographic Functions That Do Not Involve Private or Secret Keys

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

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

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

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

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Identification & Authentication

Users are identified using certificates. The certificates are originally verified by the Netscape Enterprise Server using SSL. The certificates are passed to CMS6.1 which attempts to match the certificate with a user in its internal database. If this is successful, an authentication token is created with the user attributes associated with the certificate (e.g., user roles). Subsequent requests from the same SSL session are associated with this authentication token.

If a certificate is invalid, a failure will occur in establishing the SSL session and no services will be available. If a certificate is valid, but not recognized by CMS6.1, identification and authentication will fail and applicable services will not be available.

There are a number of services that are available from the TOE that do not require authentication. These services include:

- Enrollment Requests
  - A user can request various types of certificates (note that the request will not be granted unless the user is authenticated or an Officer approves the request)
- Retrieval
  - Check request status
  - List certificates
  - Search certificates
  - Import CA certificate chain
  - Import certificate revocation list

Note that only these services are available without using SSL (default port 80). When using SSL (default port 443), additional features are provided. These features are Renewal and Revocation services, which require client certificates for authentication. Authentication is required for these services to ensure that users can renew or revoke only their own certificates. Officer functions are available (default port 8100) using SSL client authentication. Other administrative functions are available using the console application. The console application uses port 8200, by default, where SSL client authentication is enforced in the TOE configuration. Note that all of these ports are configured by default and can be changed by an Administrator.

The Identification & Authentication security function satisfies the following security requirements:

> FIA_UAU.1 (iteration 2) – CMS6.1 only allows enrollment requests and certificate related retrieval requests without being authenticated. The identification and authentication requires a valid certificate, known to CMS6.1.
>
> FIA_UID.1 (iteration 2) – CMS6.1 only allows enrollment requests and certificate related retrieval requests without being identified. The identification and authentication requires a valid certificate, known to CMS6.1.
>
> FIA_USB.1 (iteration 2) – CMS6.1 ensures that users are associated with their actions by creating an authentication token when a user is identified and authenticated, and then associating that authentication token with every request made in the context of the corresponding SSL session.

6.1.2 Access Control

Each servlet (i.e., service) has an access control list that defines which users and groups can use the services of that servlet. These access control lists simply list the users and/or groups that are permitted to invoke the servlet. When a request comes in to access a servlet, the user (and associated groups) is checked against the access control list on the servlet and the servlet will execute only if the user is allowed.

Users can access the TOE only using the HTTP-based interfaces (including the console application). The only accesses not subject to access control are those accessible outside a SSL session (i.e., those that do not require identification or authentication). By enforcing an access control check on all other accesses, CMS6.1 ensures that its access control mechanism cannot be bypassed.

The Access Control security function satisfies the following security requirements:

> FDP_ACC.1 (iteration 2) – CMS6.1 includes a number of services and each is assigned an access control list defining who can access the service. Users are defined internally in CMS6.1 and once authenticated, their user identity and associated roles are used to make access decisions.
>
> FDP_ACF.1 (iteration 2) – CMS6.1 uses its access control mechanism primarily to enforce user access and role restrictions define in Table 11. Note that there are some operations where the subject of the certificate is allowed to request an operation on the certificate – in these cases a Proof of Possession (POP) check is performed to ensure the certificate belongs to the requesting subject.
>
> FPT_RVM.1 (iteration 2) – CMS6.1 offers only limited, well-defined interfaces and ensures that users are authenticated (except for a limited set of unmediated functions) and appropriate access control checks are made and enforced prior to allowing a service to be used.

6.1.3 Security Management

CMS6.1 can be configured to define specific groups (or role). Each group can be assigned one or more users. The Access Control mechanism is used to restrict functions to specific administrator roles by configuring necessary access control lists.

6.1.3.1 CMS Privileged Users and Groups (Roles)

Each CMS subsystem has four roles set up by default. The roles that are created are specific to the CMS subsystem, and depend on which CMS subsystem has been installed. All of the privileged roles (see About Roles for more information about privileges) require SSL client-authentication by presenting a certificate that maps to the user with the corresponding role (i.e., authorization). The following sections show the default roles that are created with each subsystem and the main privileges of each.

6.1.3.1.1 CA

- Administrators
    - Can start/stop the server (from the command-line).
    - Can perform all configuration management for CA (unless assigned otherwise), including the configuration of certificate profiles (specifying the set of acceptable values for fields and extensions) for certificate enrollment requests (via the CMS Console).
    - Can backup (CMSBackup) and restore (CMSRestore) the subsystem from the command-line.
- Certificate Manager Agents

- Can approve fields/extensions (to be included in a certificate) of certificate profiles that have been enabled and configured by the Administrator (via SSL-capable browsers to the CA Agent interface).
- Can run tools (CMCEnroll and CMCRevoke) to pre-approve certificate enrollment and revocation requests.

- Auditors
  - Can view signed audit logs (from the IT environment). This is the only role allowed this privilege.
  - Can verify audit log signatures by running the AuditVerify tool (from the IT environment).

- Trusted Manager
  - The Trusted Manager role is a special role that is not for privileged users. It is created for inter-CIMC_boundary communication. The trust of this communication is established using the role authentication/authorization mechanism. Conceptually, this role is not an actual privileged role that a user can be assigned to. Rather, the Trusted Manager role is a means of establishing trust between two CMS subsystems. To have the RA communicate with the CA securely, the CA administrator needs to create an "RA user" on the CA with the Trusted Manager role when setting up the RA. All communications between the RA and CA are then made through this special user with the RA's certificate over SSL client-authentication and the Trusted Manager role authorization (via Inter-CIMC_boundary interface connectors).

6.1.3.1.2 RA

- Administrators
  - Can start/stop server (from the command-line).
  - Can perform all configuration management for the RA (unless assigned otherwise), including the configuration of certificate profiles (specifying the set of acceptable values for fields and extensions) for certificate enrollment requests (via CMS Console).
  - Can backup (CMSBackup) and restore (CMSRestore) the subsystem from the command-line.

- Registration Manager Agents
  - Can approve fields/extensions (to be included in a certificate) of certificate profiles that have been enabled and configured by the Administrator (via SSL-capable browsers to the RA Agent interface).

- Auditors
  - Can view signed audit logs (from the IT environment). This is the only role allowed this privilege.
  - Can verify audit log signatures by running the AuditVerify tool (from the IT environment).

6.1.3.1.3 DRM

- Administrators
    - Can start/stop server (from the command-line).
    - Can perform all configuration management for the DRM (via the CMS Console).
    - Can backup (CMSBackup) and restore (CMSRestore) the subsystem from the command-line
- Data Recovery Manager Agents
    - Can approve recovery of subject private keys (via SSL-capable browsers to the DRM Agent interface).
    - Can export recovered subject private keys (via SSL-capable browsers to the DRM Agent interface).
- Auditors
    - Can view signed audit logs (from the IT environment). This is only role allowed this privilege.
    - Can verify audit log signatures by running the AuditVerify tool (from the IT environment).
- Trusted Manager
    - The Trusted Manager role is a special role that is not for privileged users. It is created for inter-CIMC_boundary communication. The trust of this communication is established using the role authentication/authorization mechanism. Conceptually, this role is not an actual privileged role that a user can be assigned to. Rather, the Trusted Manager role is a means of establishing trust between two CMS subsystems. To have the CA communicate with the DRM securely, the DRM administrator creates a CA user in the DRM with the Trusted Manager role. All communications between the CA and DRM are then made through this special user with the CA's certificate over SSL client-authentication and Trusted Manager role authorization.

6.1.3.1.4 OCSP

- Administrators
    - Can start/stop server (from the command-line).
    - Can perform all configuration management for DRM (via the CMS Console).
    - Can backup (CMSBackup) and restore (CMSRestore) the subsystem from the command-line.
- Online Certificate Status Manager Agents
    - Can add CRLs (to the OCSP Responder Agent interface via SSL-capable browsers).
    - Can define supported CAs (via SSL-capable browsers to the OCSP Responder Agent interface).
- Auditors
    - Can view signed audit logs (via the CMS Console). This is the only role allowed this privilege.
    - Can verify audit log signatures by running the AuditVerify tool (from the IT environment).

6.1.3.2 About Roles

Of all privileged roles supported by CMS, the Certificate Manager Agents role, the Registration Manager Agents role, and the DRM Agent Role are the ones that map directly to the "Officer" role defined in the ST and the CIMC PP. The Online Certificate Status Manager Agents are a sub-group of the Administrator role defined in the CIMC PP. The following further specifies this mapping:

- Administrator

  The Administrator role is divided into finer-grained sub-roles, each bearing different responsibilities:

  - Administrators for the CA, RA, DRM, and OCSP subsystems
  - Online Certificate Status Manager Agents

- Officer
  - Certificate Manager Agents
  - Data Recovery Manager Agents
  - Registration Manager Agents

- Auditor
  - Auditors from CA, RA, DRM, and OCSP

6.1.3.3 Access Rules:

The following access rules are used to establish the default access control lists for the servlets. Note that the access control lists used only to restrict functions associated with explicitly defined users and groups (i.e., roles). Rules restricting access to subjects of certificates are enforced directly using certificate-based identification and authentication or POP.

Table 11 Role Restrictions

Section/Function	**Authorized Role**
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*.
Data Export and Output	The export or output of confidential and security-relevant data is performed only at the request of authorized users.
Key Generation	The capability to request the generation of Component keys (used to protect data in more than a single session or message) is restricted to Administrators.
Private Key Load	The capability to request the loading of Component private keys into cryptographic modules is restricted to Administrators.
Private Key Storage	The capability to request the decryption of certificate subject private keys is restricted to Officers. CMS6.1 does not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. CMS6.1 does not allow users or administrators to decrypt a certificate subject private key.

Section/Function	Authorized Role
Trusted Public Key Entry, Deletion, and Storage	The capability to change (add, revise, delete) the trusted public keys is restricted to Administrators.
Secret Key Storage	The capability to request the loading of CIMC secret keys into cryptographic modules is restricted to Administrators.
Private and Secret Key Destruction	The capability to zeroize CIMC plaintext private and secret keys is restricted to Administrators, Auditors, Officers, and Operators.
Private and Secret Key Export	The capability to export a component private key is restricted to Administrators. The capability to export certificate subject private keys is restricted to Officers. CMS6.1 does not support the export of component private keys. The export of a certificate subject private key requires the authorization of at least two Officers.
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. Only Officers are capable of approving the revocation of a certificate and all information about the revocation of a certificate.
Required by FMT_MOF	
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.
Backup and Recovery	The capability to configure the backup parameters is restricted to Administrators. The capability to initiate the backup or recovery function is restricted to *Administrators*.
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.
Data Export and Output	CMS6.1 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

Section/Function	Authorized Role
	status of a certificate.
CIMC Configuration	Except as stated elsewhere, the capability to configure any TSF functionality is restricted to Administrators.
Certificate Profile Management	The capability to modify the certificate profile is restricted to Administrators.
Revocation Profile Management	The capability to modify the revocation profile is restricted to Administrators.
Certificate Revocation List Profile Management	The capability to modify the certificate revocation list profile is restricted to Administrators.
Online Certificate Status Protocol (OCSP) Profile Management	The capability to modify the OCSP profile is restricted to Administrators.

The Security Management security function satisfies the following security requirements:

> FMT_MOF.1 (iteration 2) – CMS6.1 uses the access control mechanism to ensure that the various security roles can only perform appropriate functions as indicated in the table above.

6.1.4 Security Audit

CMS6.1 maintains all security relevant audit records in an audit log. The audit log is managed by a logging subsystem that is called upon by the CA, RA, OCSP Responder, or DRM (or KRA) whenever an event occurs that requires logging.

Each audit record includes:

- date,
- time,
- event type,
- thread ID,
- responsible user or agent,
- indication of success or failure,
- and other relevant information depending on the event type:
  - request identifier,
  - authentication source,
  - state,
  - DN,
  - Serial number,
  - Violation indicator,
  - Reason indicator

The following table lists the minimum set of auditable events (and additional audit record details when applicable):

Table 12 Auditable Events

Event	Additional Details
Changes to the audit parameters	
Attempts to delete the audit log	
Startup and shutdown of the audit function	
Audit log signing event	Digital signature

Event	Additional Details
Modifications to the audit configuration (while the audit collection functions are operating)	
Successful requests to perform an operation on an object covered by the SFP	
Successful transfers of user data	Identification of the protection method used
The identity of any user or subject using the data exchange mechanisms	
Unsuccessful use of the user identification and authentication mechanism, including the user identity provided	
Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	
Changes to the time	
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.
All security-relevant messages (i.e., requests) that are received by the system	
Successful and unsuccessful requests for confidential and security-relevant information	
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
The loading of Component private keys	
Access to certificate subject private keys retained within the TOE for key recovery purposes	
Changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
Manual entry of secret keys used for authentication	
Export of private and secret keys (keys used for a single session or message are excluded)	
Certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
Requests to change the status of a certificate	Whether the request was accepted or rejected.
Security-relevant changes to the configuration of the TSF.	
All changes to the certificate Profile	The changes made to the Profile
Changes to the revocation profile	The changes made to the Profile
Changes to the certificate revocation list profile	The changes made to the profile
Changes to the OCSP profile	The changes made to the Profile

The logging subsystem can filter audit records as they occur. The following attributes can be selected to be excluded from the audit log:

- event type

Note that all audit records are included by default and the selection rules can be used to reduce the set of audit records that are included in the audit log.

When a write to the audit log fails, CMS6.1 will shutdown to prevent additional auditable events to be generated. Subsequently, the TOE will not start until the situation is resolved by collaborative effort of the Auditor and Administrator in the IT Environment..

The audit log is stored internal to the CMS6.1 system. The only interfaces offered to delete audit records are controlled using an access control list so that no user can delete audit records or an entire audit log through the CMS TOE. Removal of an audit log must be done through the IT environment by a CMS auditor. In order to prevent undetected modification of audit records, CMS6.1 can be configured to use the RSA or DSA algorithm to sign entries in the log. Each signature is itself written as an entry in the audit log after the entries that are signed. The signature is computed over the previous log entries, starting with, and including, the previous signature. Since the

previous signature is signed along with the intervening data, the signatures form a chain reaching back to the very first signature created by the CMS instance. This chaining property can be used to detect the insertion of bogus log entries before a block of signed log entries, or the deletion of a block of log entries. The interval of flushing audit buffers (and the signing of which) to a file is configurable by the Administrator in CMS6.1.

CMS6.1 ensures that each record includes a reliable time stamp by always obtaining the current time and date from its host.

The Security Audit security function satisfies the following security requirements:

FAU_GEN.1 (iteration 2) – CMS6.1 minimally generates the events listed in the table above and includes the date, time, event type, subject, success or failure, as well as any additional content listed in the table above.

FAU_GEN.2 (iteration 2) – CMS6.1 records the responsible user in the contents of each audit record. The user identity is the target user for failed authentication attempts or the user authenticated for the session causing the event.

FAU_SEL.1 (iteration 2) – CMS6.1 includes the ability to filter audit records based on their event type as they occur.

FAU_STG.1 (iteration 2) – CMS6.1 protects audit records using access controls that allow only an Auditor to review or delete the audit log. CMS6.1 provides additional assurance that audit records are not modified by digitally signing audit record buffers as they are flushed into the non-volatile audit log storage.

FAU_STG.4 (iteration 2) – When the audit log becomes full, CMS6.1 shuts down and will not start until the condition is addressed.

FPT_STM.1 (iteration 2) – CMS6.1 ensures that reliable time stamps are included with each audit record by always obtaining the current time from its host.

FPT_CIMC_TSP.1 – CMS6.1 signs each audit buffer as it is flushed to non-volatile storage. The signature includes the keyed hash of the previous buffer to ensure a whole buffer cannot be removed, and each signature is stored along with its buffer.

6.1.5 Backup & Recovery

A backup/restore utility is available to backup or restore the CMS6.1 configuration. The utility runs in the context of the IT environment and operates on the IT environment representation of CMS6.1 (i.e., the files that back CMS6.1).

The utility can be used on demand and is capable of restoring a CMS6.1 configuration using only the applicable backup files and applicable encryption keys. The utility signs all backup files and checks the signatures for validity when restoring a CMS6.1 configuration. Since all critical security information that needs to be protected is already stored in encrypted form, disclosure is not a concern of the backup utility.

The Backup & Recovery security function satisfies the following security requirements:

FDP_CIMC_BKP.1 – The TOE includes a backup/restore utility that can be used on demand and requires only itself, the backup files, and applicable keys to restore as CMS6.1 configuration.

FDP_CIMC_BKP.2 – The backup/restore utility signs all CMS6.1 backup files to protect them from unauthorized modification. Unauthorized disclosure of backup data is addressed by the fact that any data requiring encryption is stored in encrypted form and it is that form that is stored in each backup.

6.1.6 Remote Data Entry & Export

CMS6.1 is responsible for importing and exporting certificates, keys, key components, certificate status, and other data. CMS6.1 protects these data transfers from unauthorized disclosure and modification using SSL sessions or PKCS#10 signatures in the case of certificate requests. In addition, the TOE provides certificate status information by following means: OCSP messages and CRLs.

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

FCO_NRO_CIMC.3 – CMS6.1 generates digital signatures for certificates, CRLs, and OCSPs. Inbound requests are authenticated using SSL or PKCS#10 in the case of certificate requests.

FDP_UCT.1 (iteration 2) – All communications external to the TOE and internal on remote components are performed over a SSL session. The SSL session will protect the data transmitted from unauthorized modification or disclosure.

FPT_ITC.1 (iteration 2) – All communications external to the TOE and internal on remote components are performed over a SSL session. The SSL session will protect the data transmitted from unauthorized modification or disclosure.

FCO_NRO_CIMC.4 - PKCS#10 signatures are used to verify certificate requests, all other security relevant messages are verified using SSL.

FDP_CIMC_CSE.1 - The TOE provides certificate status information by following means:

1. OCSP messages (RFC 2560 compliant)
2. CRLs (X.509 / RFC 2459 compliant)

FDP_ITT.1 (iteration 3 & 4) - All communications external to the TOE and internal on remote components are performed over a SSL session. The SSL session will protect the data transmitted from unauthorized modification or disclosure.

FPT_ITT.1 (iteration 3 & 4) - All communications external to the TOE and internal on remote components are performed over a SSL session. The SSL session will protect the data transmitted from unauthorized modification or disclosure.

6.1.7 Key Management

CMS6.1 supports key generation for certificates and encryption and import and export of public and private keys. CMS6.1 relies on a FIPS 140-1 validated module to perform critical key generation, key storage, and zeroization for key destruction. Additional details can be found in the security requirement mapping below.

The Key Management security function satisfies the following security requirements:

FDP_ACF_CIMC.2 – CMS6.1 does not support CIMS personnel private keys. Certificate private keys are encrypted using a hardware cryptographic module, but are not stored within the TOE.

FMT_MTD.CIMC.4 – CMS6.1 stores all CIMC private keys in a hardware cryptographic module.

FDP_SDI_CIMC.3 – Public keys are all stored signed with a digital signature. The signature on the digital certificate is verified each time the key is accessed. If the verification fails an audit record is generated and the certificate cannot be used.

FDP_ACF_CIMC.3 – CMS6.1 does not store user secret keys.

FMT_MTD_CIMC.5 – CMS6.1 secret keys are stored in cryptographic modules.

FCS_CKM_CIMC.5 – CMS6.1 does not store plaintext keys itself, but does invoke zeroization functions provided by the hardware cryptographic modules.

FDP_ETC_CIMC.5 – CMS6.1 only exports private/secret keys for KRA private key restoration. This export is always in encrypted form.

FMT_MTD_CIMC.7 – CMS6.1 does not export TSF private or secret keys.

CMS uses the PKCS# module provided by the cryptographic hardware venders to access the hardware cryptographic modules. These cryptographic hardware components are expected to have been successfully evaluated through the FIPS 140-1 program.

6.1.8 Certificate Registration, Certificate Revocation, OCSP Basic Response Validation and Their Profile Management

CMS6.1 provides functionality to issue, suspend, reinstate, renew, and revoke certificates, report status of certificates, and generate CRLs and OCSP responses. All these certificate services are provided in a secure manner, protecting the integrity of the certificates. Additionally, CMS6.1 enforces proof of possession to ensure that certificates are issued securely. CMS6.1 offers Administrators the ability to configure filters that are applied to certificates, CRLs, and OCSP. These filters either remove disallowed content or add mandatory content as certificate, CRL and OCSP requests are processed. The security requirement mapping below describes minimum capabilities provided by CMS6.1.

The Certificate Management security function satisfies the following security requirements:

FMT_MOF_CIMC.3 – CMS6.1 requires the Administrator to specify the set of acceptable values for:

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

FMT_MOF_CIMC.5 – CMS6.1 allows the Administrator to define a CRL profile that constrains CRLs. The Administrator must specify the set of acceptable values for the following:

- **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); and
- the set of acceptable CRL and CRL entry extensions.

FMT_MOF_CIMC.6 – CMS6.1 provides basic OCSP responses. The Administrator must specify the set of acceptable values for the following:

- **ResponderID**
- **responseType**

FDP_CIMC_CER.1 – CMS6.1 only generates X.509 certificates that meet the following guidelines:

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

Furthermore, CMS6.1 performs a POP check before issuing a certificate to ensure that the recipient has the corresponding private key.

FDP_CIMC_CRL.1 – CMS6.1 ensures that issued CRLs contain appropriate values. The following items are checked for validity:

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

FDP_CIMC_OCSP.1 – CMS6.1 ensures that issued OCSPs contain appropriate values. The following items are checked for validity:

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

6.2 TOE Security Assurance Measures

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

- CMS Configuration Management Plan

6.2.1.2 Life cycle support

Netscape 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. Netscape 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 the secure operation of the TOE. Netscape 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. Netscape has procedures for accepting and addressing identified flaws, including tracking, describing, correcting, and taking other remedial actions such as producing guidance related to such flaws. These procedures are documented in:

- CMS Life-Cycle Plan

The Process Assurance measures satisfy the following assurance requirements:

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

6.2.2 Delivery and Guidance

Netscape 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. Netscape's delivery procedures describe the electronic and non-electronic procedures to be used to detect modification to the TOE. These procedures are documented in:

- CMS Delivery and Installation Guide

Netscape provides administrator and user guidance on how to utilize the TOE security functions 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 CMS6.1 in accordance with the evaluated configuration. Administrator and user guidance is documented in:

- CMS Administration Guide
- CMS User Guide

The Delivery and Guidance assurance measure satisfies the following assurance requirements:

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

6.2.3 Development

The Design Documentation security assurance measure satisfies the following security assurance requirement:

- ADV_FSP.2: The CMS Functional Specification fully describes all interfaces to the TSF.

- ADV_HLD.2: The CMS High-level Design satisfies the requirement for decomposing the TOE into subsystems and fully describes each subsystem, including inter-subsytem interfaces.
- ADV_LLD.1: The CMS Low-level Design satisfies the requirement to decompose each subsystem into modules and fully describes each module.
- 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 CMS Functional Specification describes how the interfaces correspond with the security functions in the ST.
    - FSP to HLD: The CMS High-level Design describes how the various security behavior in the CMS Functional Specification are further refined.
    - HLD to LLD: The CMS Low-level Design describes how the various security behavior in the CMS High-level Design are further refined.
    - LLD to IMP: The CMS Low-level Design also serves to correspond modules with their specific implementations.
- ADV_SPM.1: The CMS Security Model models the entities and rules related to the policies for identification and authentication, audit, and all of the information flow policies. Additionally, correspondence with the CMS Functional Specification is described.

6.2.4 Tests

The Tests assurance measure satisfies the following assurance requirements:

- ATE_COV.2: The test case descriptions (in the CMS 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 CMS High-level Design) include more detailed test case descriptions that demonstrate that all of the corresponding interfaces are appropriately exercised.
- ATE_FUN.1: The CMS 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 CMS Administration Guide and CMS User Guide describe the operation of CMS6.1 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:

- CMS Administration Guide
- CMS User Guide

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

- CMS Misuse Analysis

6.2.5.2 Strength of TOE Security Functions

All of the Strength of Function claims related to CMS6.1 are based on cryptographic features. An analysis of these features in relation to the SOF requirements is documented in:

- CMS Strength of Function Analysis

6.2.5.3 Vulnerability Analysis

Netscape performs vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. The vulnerability analysis is documented in:

- CMS Vulnerability Analysis

The Vulnerability Assessment assurance measure satisfies the following assurance requirements:

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

7. Protection Profile Claims

As documented in this Security Target (ST), Netscape Certificate Management System 6.1 Service Pack 1 (CMS6.1) complies with Certificate Issuing and Management Components (CIMC) Security Level 3 (SL3) Protection Profile (PP), Version 1.0, October 31, 2001.

The Security Environment, Objectives, and Requirements in this ST have been reproduced[6] from the CIMC SL3 PP, as indicated below:

- The Assumptions, Threats, and Policies have been reordered to group the Security Level 3 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 Security Level 3 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 have been reordered to be presented alphabetically. All of the CIMC SL3 PP Requirements for the IT environment have been included and no new Requirements for the IT environment have been introduced. Operations have been completed on the Requirements for the IT environment as indicated using bold and bold-italic text in Section 5.1.
- The TOE Security Functional Requirements have been reordered to be presented alphabetically. All of the CIMC SL3 PP TOE Security Functional Requirements have been included and no new Security Functional Requirements have been introduced. Operations have been completed on the TOE Security Functional Requirements as indicated using bold and bold-italic text in Section 5.2.
- The TOE Security Assurance Requirements 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 TOE Security Assurance Requirements 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. 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 Strength of Function Requirements have been entirely copied from the CIMC SL3 PP. These requirements are presented in Section 5.4.

Note that all of the corresponding rationale elements in the CIMC PP have also been reproduced in this ST in Section 8. The rationale elements have been modified in this ST only as necessary to support the introduction of the three security assurance requirements, identified above, to bring the overall assurance level to EAL 4 augmented with ALC_FLR.2.

[6] 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.

8. Rationale

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

8.1 Security Objectives Rationale

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

The following tables provide a mapping of security objectives to the environment defined by the threats, policies, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy or assumption is covered by at least one security objective. Table 13 maps security objectives for the TOE to threats, Table 14 maps security objectives for the environment to threats, and Table 15 maps security objectives for both the TOE and the environment to threats. Table 16 maps the organizational security policies to security objectives. Table 17 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 13 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 14 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, 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,

Non-IT Security Objective	Threat
	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

Table 15 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
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.Respond to possible loss of stored audit records	T.Administrators, Operators, Officers and Auditors
commit errors or hostile actions	
O.Restrict actions before authentication	T.Hacker gains access, T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Security-relevant configuration management	T.Administrative errors of omission
O.Time stamps	T.Critical system component fails, T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

Table 16 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

Security Policy	Objective
	O.Security roles O.User authorization management
P.Cryptography	O.Cryptographic functions

Table 17 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 can not 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 faildue 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 TSFdiscovered attacks is implemented in an effort to identify attacks and to create an attack deterrent. This objective is relevant if actions that the organization deems essential also pose a potential attack that could be exploited.

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

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

It is countered by:

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

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

It is countered by:

O.Administrators, 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 18, addresses the mapping of security functional requirements to security objectives. The second table, Table 19, addresses the mapping of security assurance requirements to security objectives.

Table 18 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 (iterations 1 and 2)	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss (iterations 1 and 2)	O.Respond to possible loss of stored audit records
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	O.Non-repudiation, O.Control unknown source communication traffic
FCO_NRO_CIMC.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM.1 Cryptographic key generation	O.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_COP.1 Cryptographic operation	O.Cryptographic functions
FDP_ACC.1 Subset access control (iterations 1 and 2)	O.Limitation of administrative access
FDP_ACF.1 Security attribute based access control (iterations 1 and 2)	O.Limitation of administrative access
FDP_ACF_CIMC.2 User private key confidentiality protection	O.Certificates, O.Procedures for preventing malicious code
FDP_ACF_CIMC.3 User secret key confidentiality protection	O.Certificates, O.Procedures for preventing malicious code
FDP_CIMC_BKP.1 CIMC backup and recovery	O.Object and data recovery free from malicious code, O.Preservation/trusted recovery of secure state, O.Sufficient backup storage and effective restoration
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	O.Detect modifications of firmware, software, and backup data, O.Object and data recovery free from malicious code
FDP_CIMC_CER.1 Certificate Generation	O.Certificates
FDP_CIMC_CRL.1 Certificate revocation list validation	O.Certificates
FDP_CIMC_CSE.1 Certificate status export	O.Certificates
FDP_CIMC_OCSP.1 OCSP basic response validation	O.Certificates
FDP_ETC_CIMC.5 Extended user private and secret key export	O.Data import/export

Functional Requirement	Objective
FDP_ITT.1 Basic internal transfer protection (iterations 1 and 3)	O.Integrity protection of user data and software, O.Protect user and TSF data during internal transfer
FDP_ITT.1 Basic internal transfer protection (iterations 2 and 4)	O.Protect user and TSF data during internal transfer
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	O.Integrity protection of user data and software
FDP_UCT.1 Basic data exchange confidentiality (iterations 1 and 2)	O.Data import/export
FIA_AFL.1 Authentication failure handling	O.React to detected attacks
FIA_ATD.1 User attribute definition	O.Maintain user attributes
FIA_UAU.1 Timing of authentication (iterations 1 and 2)	O.Limitation of administrative access, O.Restrict actions before authentication
FIA_UID.1 Timing of identification (iterations 1 and 2)	O.Individual accountability and audit records, O.Limitation of administrative access
FIA_USB.1 User-subject binding (iterations 1 and 2)	O.Maintain user attributes
FMT_MOF.1 Management of security functions behavior (iterations 1 and 2)	O.Configuration management, O.Manage behavior of security functions, O.Security-relevant configuration management
FMT_MOF_CIMC.3 Extended certificate profile management	O.Configuration management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	O.Configuration management
FMT_MOF_CIMC.6 OCSP Profile Management	O.Configuration management
FMT_MSA.1 Management of security attributes	O.Maintain user attributes, O.User authorization management
FMT_MSA.2 Secure security attributes	O.Security-relevant configuration management
FMT_MSA.3 Static attribute initialization	O.Security-relevant configuration management
FMT_MTD.1 Management of TSF data	O.Individual accountability and audit records, O.Protect stored audit records
FMT_MTD_CIMC.4 TSF private key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.7 Extended TSF private and secret key export	O.Data import/export
FMT_SMR.2 Restrictions on security roles	O.Security roles
FPT_AMT.1 Abstract machine testing	O.Periodically check integrity, O.Validation of security function
FPT_CIMC_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_ITC.1 Inter-TSF confidentiality during transmission (iterations 1 and 2)	O.Data import/export
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 1-4)	O.Protect user and TSF data during internal transfer
FPT_RVM.1 Non-bypassability of the TSP (iteration 1)	O.Operating System
FPT_RVM.1 Non-bypassability of the TSP (iteration 2)	O.Limitation of administrative access
FPT_SEP.1 TSF domain separation	O.Operating System
FPT_STM.1 Reliable time stamps (iterations 1 and 2)	O.Individual accountability and audit records, O.Time stamps
FPT_TST_CIMC.2 Software/firmware integrity test	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software, O.Object and data recovery free from

Functional Requirement	Objective
	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 19 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 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.2 Flaw reporting procedures	O.Lifecycle security, O.Repair identified security flaws, selection of EAL-CSPP
ALC_LCD.1 Developer defined life-cycle model	selection of EAL 4
ALC_TAT.1 Well-defined development tools	selection of EAL 4
ATE_COV.2 Analysis of coverage	selection of EAL-CSPP, EAL 3, EAL 4
ATE_DPT.1 Testing - High-Level Design	selection of EAL-CSPP, EAL 3
ATE_FUN.1 Functional testing	selection of EAL-CSPP, EAL 3, EAL 4
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	selection of EAL-CSPP, EAL 3, EAL 4

Assurance Requirement	Objective
Evaluation	
AVA_VLA.2 Independent vulnerability analysis	selection of 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, and **FDP_CIMC_CRL.1 (Certificate revocation list validation)**, **FDP_CIMC_CSE.1 (Certificate status export)**, and **FDP_CIMC_OCSP.1 (OCSP basic response validation)** which ensure that certificate revocation lists and certificate status information are valid. In the case that the TOE maintains a copy of the certificate subject's private key**, FDP_ACF_CIMC.2 (User private key confidentiality protection)** ensures that the certificate is not invalidated by the disclosure of the private key by the TOE. In the case that a secret key is used by the certificate subject as an authenticator in requesting a certificate, **FDP_ACF_CIMC.3 (User secret key confidentiality protection)** ensures that an attacker can not obtain a bad certificate by obtaining a user's authenticator from the TOE and then using that authenticator to obtain a bad certificate.

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.

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. **FMT_MOF_CIMC.6 (OCSP Profile Management)** covers the requirement that Administrators be able to control to the types of information that are included in generated OCSP responses. **O.Configuration Management** is supported by **AGD_ADM.1 (Administrator Guidance)** which covers the requirement that Administrators be provided with documentation describing the configuration management features of the TOE and by **A.Competent Administrators, Operators, Officers and Auditors** and **A.CPS** which ensure that Administrators are competent and are familiar with the CPS under which the TOE is to be operated. **O.Configuration Management** is also supported by **ACM_AUT.1 (Partial CM automation), ACM_CAP.4 (Generation support and acceptance procedures), and ACM_SCP.2 (Problem tracking CM coverage)** which ensure that a configuration management system is implemented and used.

O.Data import/export is provided by **FDP_UCT.1 (Basic data exchange confidentiality) (iterations 1 and 2)** and **FPT_ITC.1 (Inter-TSF confidentiality during transmission) (iterations 1 and 2)** which cover the requirement that data other than private and secret keys be protected when they are transmitted and from the CIMC. **FDP_ETC_CIMC.5 (Extended user private and secret key export)** and **FMT_MTD_CIMC.7 (Extended TSF private and secret key export)** cover the requirement that private and secret keys be protected when they are transmitted to and from the TOE.

O.Detect modifications of firmware, software, and backup data is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** which covers the requirement that modifications to software or firmware be detected and **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery)** which covers the requirement that modifications to backup data be detected. Since **FPT_TST_CIMC.2** and **FDP_CIMC_BKP.2** make use of digital signatures, keyed hashes, or authentication codes to detect modifications, **FMT_MTD_CIMC.4 (TSF private key confidentiality protection)** and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are necessary to ensure that an attacker who has modified firmware, software, or backup data can not prevent detection of the modification by computing a new digital signature, keyed hash, or authentication code.

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

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

O.Integrity protection of user data and software is provided by **FDP_ITT.1 (Basic internal transfer protection) (iterations 1 and 3)** and **FDP_SDI_CIMC.3 (Stored public key integrity monitoring and action)** which cover the requirement that user data be protected and **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** which cover the requirement that software and firmware be protected. Since data and software are protected using cryptography, **FMT_MTD_CIMC.4 (TSF private key confidentiality protection)** and **FMT_MTD_CIMC.5 (TSF secret key confidentiality protection)** are required to protect the confidentiality of the private and secret keys used to protect the data and software.

O.Limitation of administrative access is provided by **FDP_ACC.1 (Subset access control) (iterations 1 and 2)**, **FDP_ACF.1 (Security attribute based access control) (iterations 1 and 2)**, **FIA_UAU.1 (Timing of authentication) (iterations 1 and 2)**, and **FIA_UID.1 (Timing of identification) (iterations 1 and 2)**. **FIA_UAU.1 (Timing of authentication) (iterations 1 and 2)** and **FIA_UID.1 (Timing of identification) (iterations 1 and 2)** ensure that Administrators, Operators, Officers, and Auditors can not perform any security-relevant operations until they have been identified and authenticated and **FDP_ACC.1 (Subset access control) (iterations 1 and 2)** and **FDP_ACF.1 (Security attribute based access control) (iterations 1 and 2)** ensure that Administrators, Operators, Officers, and Auditors can only perform those operations necessary to perform their jobs. **FPT_RVM.1 Non-bypassability of the TSP (iteration 2)** ensure that Administrators, Operators, Officers, and Auditors can not perform operations that they are not authorized to perform by bypassing the TSP enforcement functions.

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

O.Manage behavior of security functions is provided by **FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2)** which covers the requirement that authorized users be able to configure, operate, and maintain the security mechanisms.

O.Object and data recovery free from malicious code is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** and **FPT_TST_CIMC.3 (Software/firmware load test)** which cover the requirement that the recovered state is free from malicious code. **FDP_CIMC_BKP.1 (CIMC backup and recovery)**, **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery)** covers the requirement to be able to recover to a viable state.

O.Procedures for preventing malicious code is provided by **FPT_TST_CIMC.2 (Software/firmware integrity test)** which ensures that only signed code can be executed and **AGD_ADM.1 (Administrator Guidance), AGD_USR.1 (User Guidance)** and **A.Malicious Code Not Signed** which ensure that those who are capable of signing code do not to sign malicious code. It is also supported by **FDP_ACF_CIMC.2 (User private key confidentiality protection), FDP_ACF_CIMC.3 (User secret key confidentiality protection), FCS_CKM.4 (Cryptographic key destruction) and FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** which ensure that an untrusted entity can not use a trusted entity's key to sign malicious code.

O.Protect stored audit records is provided by **FAU_STG.1 (Protected audit trail storage) (iterations 1 and 2)** which covers the requirement that audit records be protected against modification or unauthorized deletion and **FMT_MTD.1 (Management of TSF data)** which covers the requirement that audit records be protected from unauthorized access. At Security Level 3, where the threat of malicious activity is greater, **FPT_CIMC_TSP.1 (Audit log signing event)** is required so that modifications to the audit logs can be detected.

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

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

O.Respond to possible loss of stored audit records is provided by **FAU_STG.4 (Prevention of audit data loss) (iterations 1 and 2)** which covers the requirement that no auditable events, except those taken by the Auditor, can be performed when audit trail storage is full.

O.Restrict actions before authentication is provided by **FIA_UAU.1 (Timing of authentication) (iterations 1 and 2)** which covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.

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

O.Time stamps is provided by **FPT_STM.1 (Reliable time stamps) (iterations 1 and 2)** which covers the requirement that the time stamps be reliable.

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

O.React to detected attacks is provided by **FCS_CKM.4 (Cryptographic key destruction)** and **FCS_CKM_CIMC.5 (CIMC private and secret key zeroization)** which cover the requirement that the user who detected the attack be able to destroy any plaintext keys within the TOE in order to prevent the attacker from obtaining copies of these keys. **FIA_AFL.1 (Authentication failure handling)** covers the requirement that the TSF respond to detected attacks (in the form of repeated authentication attempts) by taking actions to prevent the attacker from successfully authenticating him/herself. In the case that an attack is detected by an Administrator, Auditor, Officer, or Operator.

8.3 Assurance Requirements Rationale

CIMCs designed to meet Security Level 3 (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 Security Level 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 Security Level 3. As a result, it is important that some penetration analysis and testing be performed.

8.3.1 Rationale for EAL 4

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

It is important that changes to the TOE be appropriately controlled. This requirement helps to ensure that the development and maintained are appropriately controlled.

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 Security Functional Requirements Dependencies

The following table provides a summary of the security functional requirements dependency analysis.

Table 20 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
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit	FAU_STG.1 Protected audit trail	Included

Component	Dependencies	Which is:
data loss	storage	
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3	Included
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included
	FCS_CKM.4 Cryptographic key destruction	Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ACF.1 Security attribute based access control	Included
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Included
	FMT_MSA.2 Secure security attributes	Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	FMT_MOF.1 Management of security functions behavior	Included
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	
FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	None	

Component	Dependencies	Which is:
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	NOT Included
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MOF_CIMC.6 OCSP profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.2 Secure security attributes	ADV_SPM.1 Informal TOE security policy model	Included
	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security Roles	Included (hierarchical to FMT_SMR.2)
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included (hierarchical to FMT_SMR.2)
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	

Component	Dependencies	Which is:
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FMT_MTD_CIMC.6	Included
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_AMT.1 Abstract machine testing	None	
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1 Audit data generation	Included
	FMT_MOF.1 Management of security functions behavior	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	
FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_AMT.1 Abstract machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_AMT.1 Abstract Machine Testing	Included
FTP_TRP.1 Trusted path	None	

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

Component FDP_UCT.1 Basic data exchange confidentiality has a direct dependency on FTP_ITC.1 Inter- TSF trusted channel or FTP_TRP.1 Trusted path that is unmet. This product uses basic encryption to ensure basic data exchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path at Security Level 3.

8.4.1.2 Security Assurance Requirements Dependencies

The following table provides a summary of the security assurance requirements dependency analysis.

Table 21 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
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

Component	Depends On:	Which is:
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) 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.2	no dependencies	not applicable
ALC_LCD.1	no dependencies	not applicable
ALC_TAT.1	ADV_IMP.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_HLD.2	included
	(indirect) ADV_LLD.1	included
	(indirect) ADV_RCR.1	included
ATE_COV.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ATE_FUN.1	included
	(indirect) ADV_RCR.1	included
ATE_DPT.1	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	ATE_FUN.1	included
	(indirect) ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	(indirect) ADV_RCR.1	included
ATE_FUN.1	no dependencies	not applicable
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

Component	Depends On:	Which is:
AVA_MSU.2	ADO_IGS.1	included
	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	AGD_ADM.1	included
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
AVA_SOF.1	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.1	included (hierarchical to ADV_HLD.2)
	(indirect) ADV_RCR.1	included
AVA_VLA.2	ADV_FSP.1	included (hierarchical to ADV_FSP.2)
	ADV_HLD.2	included
	ADV_IMP.1	included
	ADV_LLD.1	included
	AGD_ADM.1	included
	AGD_USR.1	included
	(indirect) ADV_RCR.1	included
	(indirect) ALC_TAT.1	included

8.4.2 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.1 and FIA_UAU.1 support other functions' allowing user access to data by limiting the actions the user can take prior to identification and authentication.

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

FPT_TST_CIMC.2 provides for integrity testing to ensure that selected security functions are operational, thus checking for 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.1 and FIA_UAU.1 support other functions allowing user access to data by limiting the actions the user can take prior to identification and authentication.

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

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

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

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 Security Target includes three security assurance requirements 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), and require a life-cycle model and with provisions for controlling the development and maintenance of the TOE (ALC_LCD.1). 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 TOE Security Functions and the TOE Security Functional Requirements. This table in conjunction with rationale provided in Section 6.1 demonstrates that the TOE Security Functional Requirements are satisfied.

Table 22 Security Function to TOE SFR Mapping

Security Function	Security Functional Components
Identification and authentication	FIA_UAU.1 Timing of authentication (iteration 2)
	FIA_UID.1 Timing of identification (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)
Security Management	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)
	FAU_STG.1 Protected audit trail storage (iteration 2)
	FAU_STG.4 Prevention of audit data loss (iteration 2)
	FPT_STM.1 Reliable time stamps (iteration 2)
	FPT_CIMC_TSP.1 Audit log signing event
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
	FDP_UCT.1 Basic data exchange confidentiality (iteration 2)
	FDP_ITT.1 Basic internal transfer protection (iterations 3 and 4)
	FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 2)
	FPT_ITT.1 Basic internal TSF data transfer protection (iterations 3 and 4)

Security Function	Security Functional Components
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
	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
	FDP_CIMC_OCSP.1 Basic Response Validation
	FMT_MOF_CIMC.3 Extended certificate profile management
	FMT_MOF_CIMC.5 Extended certificate revocation list profile management
	FMT_MOF_CIMC.6 OCSP Profile Management

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 PP is intended to operate in a range of environments, from benign to hostile. Also, the users may be hostile. Therefore, the TOE requires cryptographic functions to provide for integrity, confidentiality, nondisclosure, and authentication. The 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, Netscape Certificate Management System 6.1 Service Pack 1 (CMS6.1) complies with Certificate Issuing and Management Components (CIMC) Security Level 3 (SL3) Protection Profile (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 Security Target (ST) with the exception of ACM_CAP.3 which is replaced with ACM_CAP.4. 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 three exceptions: ACM_AUT.1, ACM_CAP.4, and ALC_LCD.1. These three security assurance requirements have been introduced 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 PP.

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

ANSI	American National Standards Institute
CA	Certification Authority
CC	Evaluation Criteria for Information Technology Security (Common Criteria)
CIMC	Certificate Issuing and Management Component
CIMS	Certificate Issuing and Management System
CMS	Certificate Management System
CMS6.1	Netscape Certificate Management System 6.1 Service Pack 1
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
I&A	identification and authentication
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JSS	Netscape Java Security Services
KRA	Key Archival and Retrieval Authority
NSS	Netscape Network Security Services
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
POP	Proof of Possession
PP	Protection Profile
RA	Registration Authority
SFP	Security Function Policy
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy