Tumbleweed Valicert Validation Authority Security Target

Version 1.0

04/3/06

Prepared for:

Tumbleweed Communications

700 Saginaw Drive
Redwood City, CA 94063

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Valicert Validation Authority provided by Tumbleweed Communications. A Validation Authority provides a universal clearing house for establishing the validity of digital certificates.

The Security Target contains 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)

1.1 Security Target, TOE and CC Identification

ST Title – Tumbleweed Valicert Validation Authority Security Target

ST Version – Version 1.0

ST Date – 04/3/06

TOE Identification – Tumbleweed Valicert Validation Authority Version 4.8 Hot Fix 3 (build 388)

CC Identification – Common Criteria (CC) for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE conforms to the following CC specifications:

- Common Criteria (CC) for Information Technology (IT) Security Evaluation Part 2: Security functional requirements, Version 2.2, Revision 256, January 2004.
    - Part 2 extended
- Common Criteria (CC) for Information Technology Security Evaluation Part 2: Security assurance requirements, Version 2.2, Revision 256, January 2004.
    - Part 3 conformant
    - Evaluation Assurance Level 3 (EAL 3)
    - Certificate Issuing and Management Components (CIMC) Security Level 1 Protection Profile (PP), Version 1.0, October 31, 2001

1.3 Conventions

The following conventions have been applied in this document:

- 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.
    - 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.1a and FDP_ACC.1b 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**]).
    - 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.

2. TOE Description

The TOE is Tumbleweed Valicert Validation Authority, Version 4.8 Hot Fix 3. A Validation Authority (VA) provides a universal clearing house for establishing the validity of a digital certificate. The VA represents a centralized store of aggregated Certification Authority (CA) published Certificate Revocation Lists (CRLs). It is possible for a VA to aggregate CRLs from one or more different CAs. This store of certificate status data is continuously available and accessible to PKI enabled applications via several standard real-time protocols. These protocols allow Public Key Infrastructure (PKI) applications to obtain the status of a specific certificate rather than the raw cumulative CRL periodically published by the CA. Thus the introduction of a VA addresses the scalability and access issues associated with client certificate validation in PKI, as well as the audit.

The Validation Authority offers the following capabilities:

- Supports software and Public Key Certificate Standard (PKCS) #11 and Cryptographic Application Programming Interface (CAPI) token-based hardware signing and encryption.
- Allows digital signing of Online Certificate Status Protocol (OCSP) requests so that only authorized clients' queries are processed.
- Enables requests, responses, and administration to be carried out over an Secure Sockets Layer (SSL) session.
- Allows use of different private keys for signing responses, SSL, audit logs, forwarding requests and VA-to-VA mirroring.
- Provides audit trails and non-repudiation through digitally signed and tamper proof Extensible Markup Language (XML) logs.

2.1 TOE Architecture

The Validation Authority can be run in a server or desktop configuration. In the *server configuration*, there are three main components of the VA:

1. Tumbleweed Validation Authority – Validates revocation status of digital certificates and communicates over an HTTPS interface.
2. Tumbleweed Publisher – Collects revocation data from a CA or a directory server supporting Lightweight Directory Access Protocol (LDAP), Secure LDAP (LDAPS), Hyper-text Transfer Protocol (HTTP), and Secure HTTP (HTTPS) and publishes it to a VA.
3. Tumbleweed Server Validator (SV) - The (SV provides certificate revocation status checking for web servers requiring SSL and client authentication. SV can be used to add revocation checking for certificates used to authenticate to web servers or web enabled applications. SV provides validation capability within Microsoft ISA, Apache server (including Oracle Application Server and RedHat StrongHold variants), America On-line (AOL)/Netscape or Sun Web Server environments, and is supported on both Windows and UNIX. SV integrates with the VA server for automatic configuration and provides robust fail-over support.

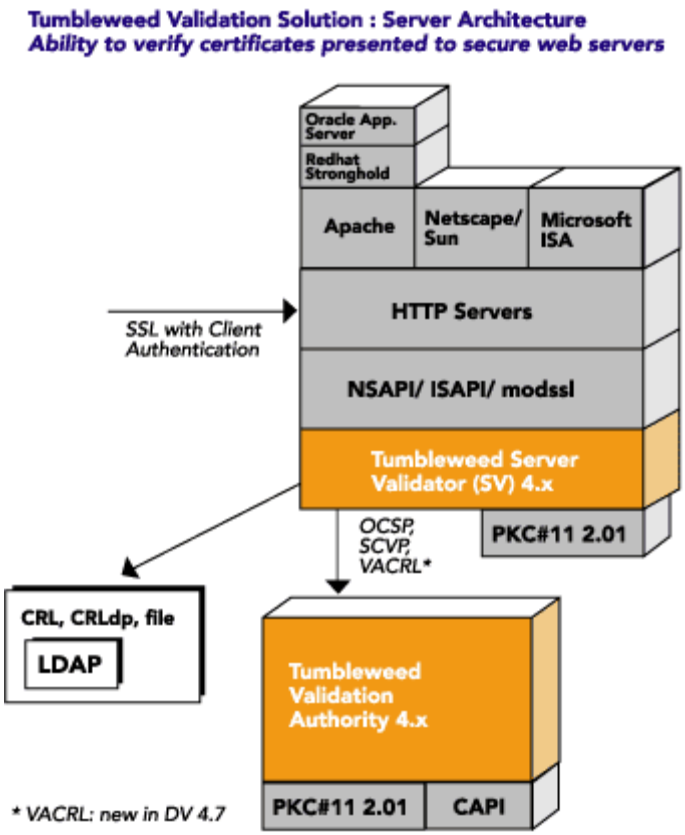


Figure 1 Server Validator Client Architecture - interaction with Validation Authority server for revocation information

The *desktop configuration* contains three components and Figure 2 shows the desktop components and their interfaces. :

1. VA Server: Robust, fourth generation server that provides online validation support using OCSP, Simple Certificate Validation Protocol (SCVP), CMP, and CSC standards. Integrates with major CA products and services including those from Baltimore Unicert, Entrust PKI, Microsoft CA, AOL/Netscape Certificate Management Server (CMS) and Sun

2. Tumbleweed Publisher: Obtains revocation data from a CA or a directory server supporting LDAP, LDAPS, HTTP, and HTTPS and publishes it to a Tumbleweed Valicert VA.

3. DV: A CAPI 2.0 compliant certificate revocation status checking provider for Windows 95/98/ME/XP/NT/2000/2003. DV provides revocation checking seamlessly for Microsoft applications (Internet Explorer (IE), Outlook, Outlook Express, Internet Information Services (IIS), Windows 2000 Domain Controllers and Windows 2000 server). DV provides certificate validation for secure e-mail, secure web access, VPN, and smart card login. DV can be deployed using Microsoft SMS for enterprise deployments. DV provides CA specific options that allows for flexible rules to be defined for certificate status checking. DV provides robust fail-over support from multiple sources of revocation information. DV supports Microsoft and Sun/AOL proxy servers and proxy synchronization with IE for custom proxy. DV supports automatic configuration with VA server.

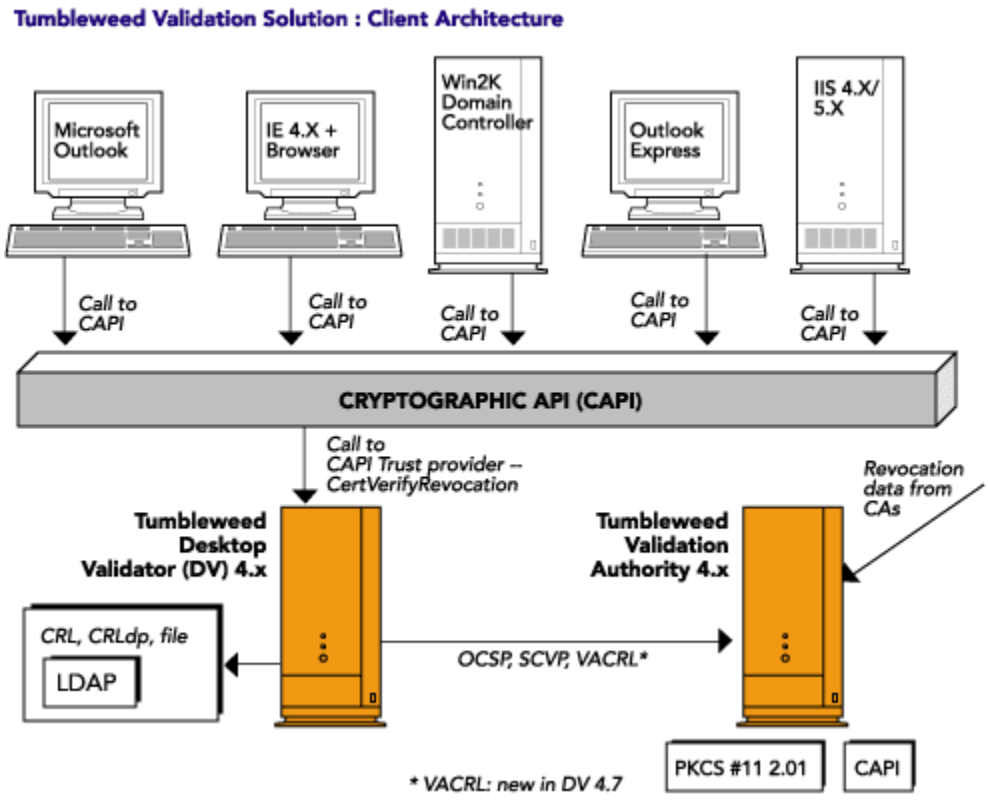


Figure 2 Desktop Validator Client Architecture – interaction with Validation Authority server for revocation information

Irrespective of which configuration is being used to plug revocation-checking into a client/server application, the TOE, as evaluated, consists of the following components:

- Tumbleweed Validation Authority 4.8
- Integrated Publisher

Note: The Publisher is also available as a stand-alone component that can be installed on a machine separate from the TOE.

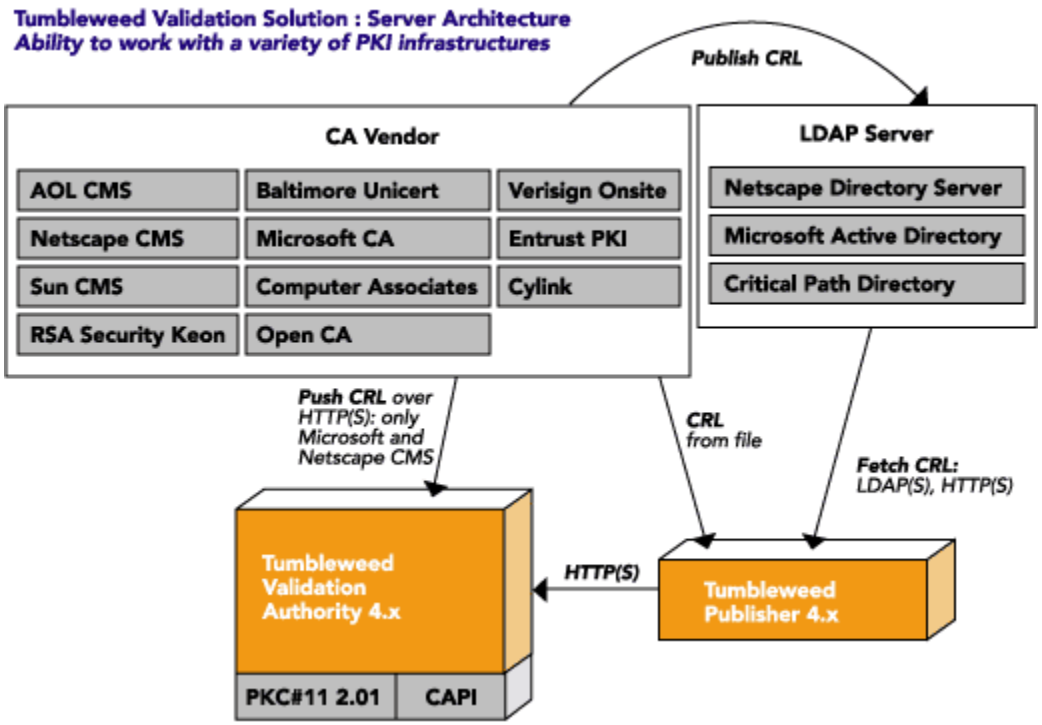
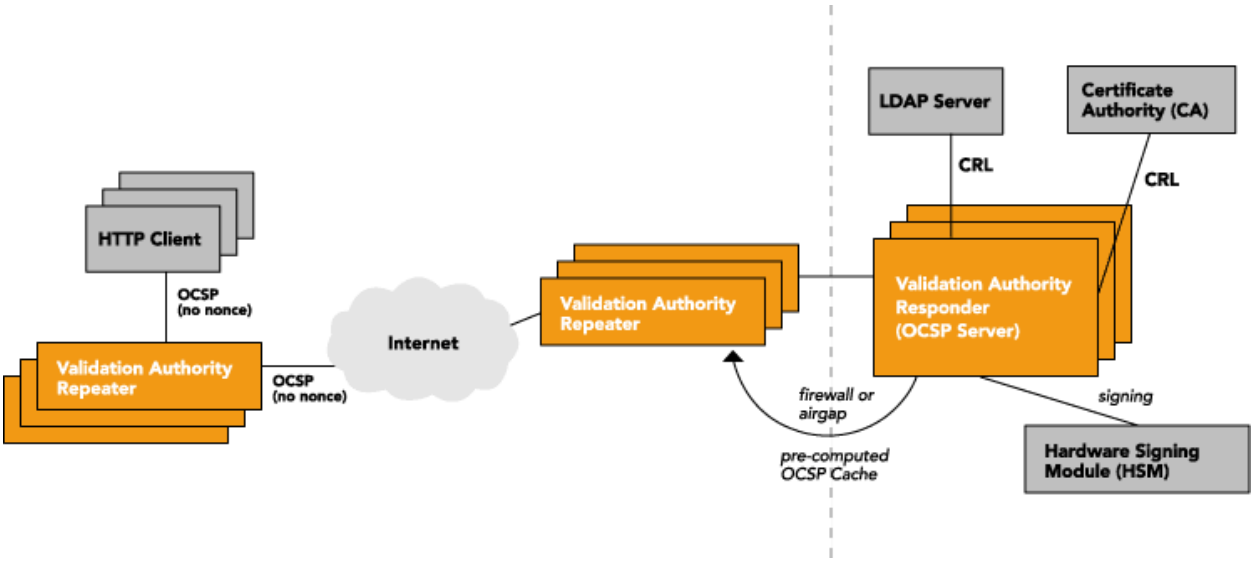


Figure 3 TOE architecture – traditional OCSP

The TOE can operate in both the **traditional** and **distributed** architectures. In the distributed OCSP architecture, the TOE is deployed in the following modes:

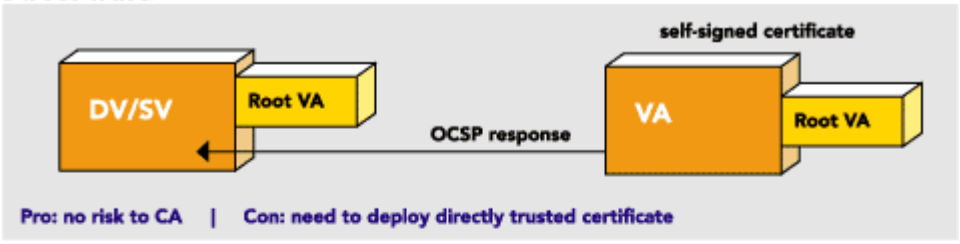
- Responder
- Repeater

In the evaluated configuration, the Responder uses software signing keys using its FIPS 140-1 approved software cryptographic module, while the Repeater is keyless. The Repeater's key management functionality is limited to SSL communications with the Responder and verification of signed revocation data mirroring messages.

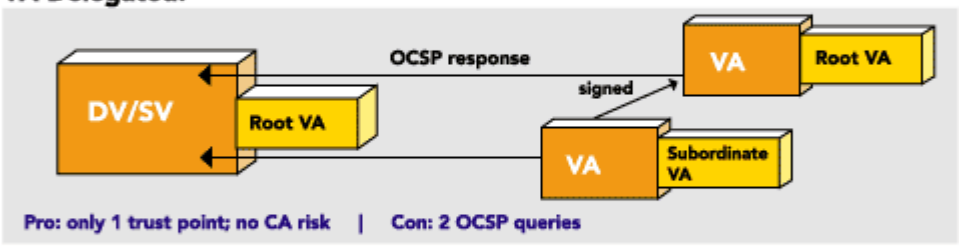


Certificate validation implies trust between the client and the VA. There are three models for this trust in the evaluated configuration:

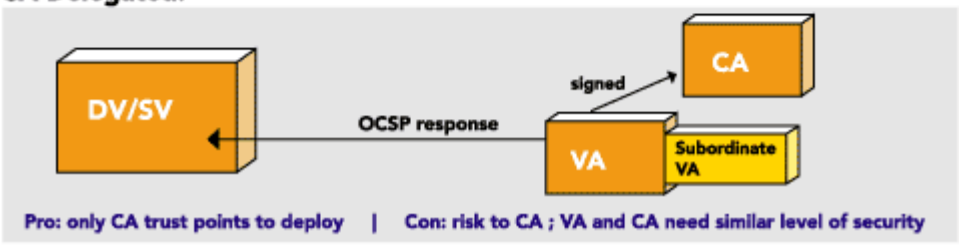
Direct Trust:



VA Delegated:



CA Delegated:



Direct Trust - Direct trust occurs when the client requesting validation has set up a direct trust relationship with the VA. Since the client directly trusts the VA certificate as a trusted authority, it can use the responder's self-signed certificate to verify the signature on revocation status responses (on behalf of any CA) from the authority. The advantage of this scheme is that it requires no trust chain to be established under a CA, thus reducing the risk/exposure to the CA for creating this chain. The disadvantage of this approach is that the directly trusted VA certificate needs to be distributed to the applications that will be making validation queries. When the VA certificate expires, or is compromised, the clients will need to be updated to trust a new directly trusted VA certificate.

VA delegated - VA delegated trust is a derivative of the direct trust model which enables a directly trusted VA to delegate its responsibilities to a "subordinate" VA further addressing scalability and operational domain issues that often come up in PKI. The directly trusted VA has a self-signed digital certificate referred to as a root VA certificate. The directly trusted VA uses this root certificate to issue a digital certificate to a subordinate VA, which in turn uses this digital certificate to sign client responses. In order for a client to trust the subordinate VA it must establish the certificate chain back to the directly trusted VA. The certificate depth is limited to one level, meaning the subordinate VA certificates can only be used to sign client responses, and cannot be used to issue other signing certificates. In this model, the subordinate VA certificates can be replaced without impacting the client configuration in any way. However, a compromise of the Root VA certificate will compromise the entire trust model, in which case, all clients will need to be updated to trust a new Root VA.

CA delegated - CA delegated trust occurs when a CA has explicitly given permission to a VA to respond to revocation requests on its behalf. This is similar to the VA Delegated trust model described above except that the certificate used by the VA to sign responses chains back to the issuing CA rather than to the directly trusted VA. In order to trust the VA, the client must still establish the certificate chain back to the CA, but in many cases this may not require any additional operations since the client already trusts the CA. This model relies on certain extensions to the digital certificates that all participants in the PKI must recognize. Additionally, since the CA and VA are under different administration boundaries in most operational environments, a CA is potentially opening itself up for

liability by delegating validation to a different entity. This model has some clear advantages: only CA trust points need to be distributed. The main disadvantage is that the CA must delegate a CA responsibility to a VA. If the VA is compromised, the CA is compromised, with respect to the integrity of the status information known about the CA. This is why for CA Delegated mode, the CA and VA servers need to have almost equivalent physical security requirements. However, in the event that a VA certificate needs to be re-keyed or updated, the clients do not need to be modified as the new VA credentials will also chain up to the same CA.

2.2 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 Figures 1 and 2, 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 single process. The runtime environment is provided by a trusted host operating system. The operating systems included in the evaluation are: Windows 2000, Windows Server 2003, Solaris 2.7, 2.8, 2.9 and 2.10, Red Hat Enterprise Linux versions 7, 8, and 9. An Apache server serves to offer a HTTPS-based interface to administrators, officers and auditors of the VA.

The TOE application supports LDAP interfaces, validation protocol, and also HTTP-based interfaces. The LDAP interfaces are used to connect to the LDAP Server used by Valicert VA exclusively as a data store, and also to connect to a Corporate LDAP server for publishing purposes, if configured. The validation protocol interfaces (OCSP, SCVP, and VACRL) are used to respond to client application requests for digital certificate status. The HTTPS-based interfaces allow users to connect to the VA to access its security functions and allow administrators to manage the VA.

2.3 Logical Boundaries

VA implements security functions that support Security Audit, Backup and Recovery, Access Control, Identification & Authentication, Remote Data Entry and Export, Key Management, and Profile Management.

Security Audit - VA provides the ability to audit security relevant events. Each audit records includes the responsible user, date, time, and other details. Valicert VA protects the audit trail and ensures that only authorized users can access the audit data.

Backup and Recovery - Valicert VA includes a backup and restore capability. In order to be able to recover from failures and other unanticipated undesired events, Valicert VA can back up the system. The backup can be used to restore the Valicert VA to an operational status at a previous point in time.

Access Control - Valicert VA provides the ability to limit access to the various services provided by the VA. These limitations are provided via a set of access control lists.

Identification and Authentication - Valicert VA requires that users be identified and authenticated before allowing them to perform any other functions.

Remote Data Entry and Export - Valicert VA uses SSL to protect remote data import and export functions.

Key Management - Valicert VA provides several key management functions. These functions include protecting secret and private keys.

Profile Management - Valicert VA provides management functions to manipulate several types of profiles including certificates, CRLs, and OCSP responses that are generated.

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 (SFRs) 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.

A.No Abusive Administrators, Operators, Officers and Auditors

Administrators, Operators, Officers and Auditors are trusted not to abuse their authority.

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

An Administrator, Operator, Officer or Auditor unintentionally commits errors that change the intended security policy of the system or application.

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 1 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.

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.

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 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.No Abusive Administrators, Operators, Officers and Auditors

Use trustworthy Administrators, Operators, Officers and Auditors.

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.Validation of security function

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

4.3 Security Objectives for both the TOE and the Environment

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

O.Configuration Management

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

O.Data import/export

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

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

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

O.Individual accountability and audit records

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

O.Integrity protection of user data and software

Provide appropriate integrity protection for user data and software.

O.Limitation of administrative access

Design administrative functions so that Administrators, 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.Security roles

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

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.

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_ATD.1 User attribute definition (iteration 1)
	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 (iteration 1)
	FMT_MSA.3 Static Attribute Initialization
	FMT_MTD.1 Management of TSF Data
	FMT_SMR.2 Restrictions on security roles (iteration 1)
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
	FPT_TST_CIMC.2 Software/Firmware Integrity Test
	FPT_TST_CIMC.3 Software/Firmware Load Test

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	
Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a role	
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) [***subject identity***]
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 unauthorized modifications to the audit records in the audit trail.

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 46-3 for DES and 3DES; FIPS 186-2 for RSA (PKCS#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 [**encryption, decryption, hashing**] in accordance with [**FIPS 46-3 for DES and 3DES; FIPS 186-2 for RSA (PKCS#1); FIPS 180-2 for SHA-1; and FIPS 198 for HMAC-SHA-1**].

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 file accesses**].

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

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

FDP_ACF.1.2 The IT environment shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: The capability to zeroize plaintext private and secret keys shall be restricted to Administrators, Auditors, and Officers~~, and Operators~~[2].

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)

[2] The CIMC PP includes Operator in the assignment but at SL1, the Operator role is not required

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_ATD.1 User attribute definition (iteration 1)

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 [**no actions**] on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1 Timing of Identification (iteration 1)

FIA_UID.1.1 The IT environment shall allow [**no actions**] 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) *(per International Interpretation #137)*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**user id.**]

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**The subject will be associated with the privileges associated to user id.**]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with subjects acting on the behalf of users: [**none**.]

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 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 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 (iteration 1)

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.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 (iteration 1)

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

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

FMT_SMR.2.3 The IT environment shall ensure that:
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.

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

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 load into 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.

5.2 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. .FIA_ATD.1 and FMT_SMR.2 are enforced by the TOE and the environment and have been placed on the TOE.

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
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_CIMC_BKP.1 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_ITT.1 Basic Internal Transfer Protection (iterations 3 and 4)
	FDP_UCT.1 Basic Data Exchange Confidentiality (iteration 2)
Identification and Authentication (FIA)	FIA_ATD.1 User Attribute Definition (iteration 2)
	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.2 Certificate Profile Management
	FMT_MOF_CIMC.4 Certificate Revocation List Profile Management
	FMT_MOF_CIMC.6 OCSP Profile Management
	FMT_MSA.1 Management of Security Attributes (iteration 2)
	FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection
	FMT_SMR.2 Restrictions on Security Roles (iteration 2)
Protection of the TSF (FPT)	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)

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	
Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a role	
		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	
Local Data Entry		All security-relevant data that is entered in the system	The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an “accept” button). This shall be included with the accepted data.
Remote Data Entry		All security-relevant messages that are received by the system	
Data Export and Output		All successful and unsuccessful requests for confidential and security-relevant information	
Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
Private Key Load		The loading of Component private keys	

Section/Function	Component	Event	Additional Details
Private Key Storage		All access to certificate subject private keys retained within the TOE for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
Secret Key Storage		The manual entry of secret keys used for authentication	
Private and Secret Key Export	FDP_ETC_CIMC.4 User private and secret key export	The export of private and secret keys (keys used for a single session or message are excluded)	
Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.).
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	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	All changes to the certificate revocation list profile	The changes made to the profile
Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP Profile Management	All changes to the OCSP profile	The changes made to the Profile

FAU_GEN.2 User Identity Association (iteration 2)

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

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 [**digital signature**] 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.

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, functions, and access to functions**].

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

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

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.

[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.

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 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.
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.
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.

Section/Function	Component	Event
		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_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_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, and the delta CRL standard**].

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_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 physically separated parts of the TOE.

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_ATD.1 User Attribute Definition (iteration 2)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: the set of roles that the user is authorized to assume, [**user id, authentication method, authentication data**].

FIA_UAU.1 Timing of Authentication (iteration 2)

FIA_UAU.1.1 The TSF shall allow [**Certificate Status Requests]** 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 Status Requests**] 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) *(per International Interpretation #3)*

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**user id, session id.**]

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**The subject will be associated with the session id and the privileges associated to the role assigned to the user id.**]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with subjects acting on the behalf of users: [**none**.]

5.2.6 Security Management (FMT)

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

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in **Table 8** to the authorized roles as specified in **Table 8**.

Table 8 Authorized Roles for Management of Security Functions Behavior

Section/Function	Component Function	Authorized Role
Security Audit		The capability to configure the audit parameters shall be restricted to Administrators.
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~~		~~Private key export shall be performed by the Administrator.~~
Certificate Status		Only Officers shall configure the automated

Section/Function	Component Function	Authorized Role
Change Approval		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.
Identification and Authentication	FIA_ATD.1 User attributes definition	The capability to change authentication mechanisms shall be restricted to Administrators
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to Administrators.
Certificate Revocation List Profile Management	FMT_MOF_CIMC.4 Certificate revocation list profile management; FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administrators.
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.
Account Administrator	FMT_SMR.2 Restriction on security roles	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_MOF_CIMC.2 Certificate Profile Management

FMT_MOF_CIMC.2.1 The TSF shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_CIMC.2.2 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;

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.4 Certificate Revocation List Profile Management

FMT_MOF_CIMC.4.1 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.4.2 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.)

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_MSA.1 Management of Security Attributes (iteration 2)

FMT_MSA.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in section **9.2** to restrict the ability to modify the security attributes [**user definitions and role assignments**] to Administrators.

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_SMR.2 Restrictions on Security Roles (iteration 2)

FMT_SMR.2.1 The TSF shall maintain the roles: Administrator, Auditor, and Officer.

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

FMT_SMR.2.3 The TSF 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:
2. *Administrator* – role authorized to install, configure, and maintain the CIMC; establish and maintain user accounts; configure profiles and audit parameters; and generate Component keys.
3. *Officer* – role authorized to request or approve certificates or certificate revocations.
4. *Auditor* – role authorized to view and maintain audit logs.

5.2.6 Protection of the TSF (FPT)

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.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 9 EAL 3 Assurance Components

Requirement Class	Requirement Component
ACM: Configuration Management	ACM_CAP.3: Authorization Controls
	ACM_SCP.1: TOE CM Coverage
ADO: Delivery and Operation	ADO_DEL.1: Delivery Procedures
	ADO_IGS.1: Installation, Generation, and Start-up Procedures
ADV: Development	ADV_FSP.1: Informal Functional Specification
	ADV_HLD.2: Security Enforcing High-level Design
	ADV_RCR.1: Informal Correspondence Demonstration
AGD: Guidance Documents	AGD_ADM.1: Administrator Guidance
	AGD_USR.1: User Guidance
ALC: Life Cycle Support	ALC_DVS.1: Identification of Security Measures
ATE: Tests	ATE_COV.2: Analysis of Coverage
	ATE_DPT.1: Testing: High-level Design
	ATE_FUN.1: Functional Testing
	ATE_IND.2: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_MSU.1: Examination of Guidance
	AVA_SOF.1: Strength of TOE Security Function Evaluation
	AVA_VLA.1: Developer Vulnerability Analysis

5.3.1 Configuration Management (ACM)

5.3.1.1 Authorisation Controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.6c The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7c The CM plan shall describe how the CM system is used.
ACM_CAP.3.8c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.9c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.10c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.11c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM Coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c 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.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, Generation, and Start-up Procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
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)

5.3.3.1 Informal Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security Enforcing High-level Design (ADV_HLD.2)

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.

5.3.3.3 Informal Correspondence Demonstration (ADV_RCR.1)

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.

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

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.

5.3.4.2 User Guidance (AGD_USR.1)

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)

5.3.5.1 Identification of Security Measures (ALC_DVS.1)

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.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of Coverage (ATE_COV.2)

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.

5.3.6.2 Testing: High-level Design (ATE_DPT.1)

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

5.3.6.3 Functional Testing (ATE_FUN.1)

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.

5.3.6.4 Independent Testing - Sample (ATE_IND.2)

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)

5.3.7.1 Examination of Guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.
AVA_MSU.1.1c 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.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE Security Function Evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer Vulnerability Analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

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

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

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 Personal Identification Number (PIN), false acceptance error rate of a biometric device, or some combination of authentication methods.)

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

5.4.2 Cryptographic Modules

FIPS 140-1 validated cryptographic modules 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.

5.4.2.2 Encryption Algorithms

The encryption specified for:

- FAU_STG.1 Protected Audit Trail Storage
- FDP_ACF_CIMC.2 User Private Key Confidentiality Protection
- FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection
- 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.

5.4.2.3 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
- FMT_MTD_CIMC.4 TSF Private Key Confidentiality Protection

shall be validated against FIPS 140-1.

5.4.2.4 Authentication Codes

The authentication code specified in:

- FAU_STG.1 Protected Audit Trail Storage
- 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.

5.4.2.5 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 1**
Certificate and Status Signing - single party signature - multiparty signature	 1 1
Integrity or Approval Authentication - single approval - dual approval	 1 1
General Authentication	1
Long Term Private Key Protection	1
Long Term Confidentiality	1
Short Term Private key Protection	1
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 1, with level Roles and Services.

5.4.2.6 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. 1.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

Valicert VA collects all security relevant audit records in an audit log. The audit logs are stored in a file in the environment. Access to the audit log files are protected by the file access controls of the environment. The audit log is maintained internally to Valicert VA. 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 Valicert VA TOE. In order to prevent undetected modification of audit records, Valicert VA can be configured to use the Rivest, Shamir and Adleman (RSA) algorithm to sign entries in the audit 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. Removal of an audit log must be done through the IT environment by a Valicert VA auditor.

Valicert VA collects the following audit events:

Event	Additional Details
Changes to the audit parameters	
Attempts to delete the audit log	
Startup and shutdown of the audit function	
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	
Successful and unsuccessful attempts to assume a role.	
An Administrator changes the type of authenticator, e.g., from password to certificate.	
Roles and users are added or deleted.	
The access control privileges of a user account or a role are modified.	
Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	
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	
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
Export of private and secret keys (keys used for a single session or message are excluded)	

Event	Additional Details
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

Each audit record contains the following information:

- Date,
- Time,
- Event type,
- Process ID,
- Responsible user or agent,
- Indication of success or failure, and
- Other relevant information depending on the event type:
    - Request identifier,
    - Authentication source,
    - Serial number,

Valicert VA ensures that each record includes a reliable time stamp by always obtaining the current time and date from its environment. Valicert VA provides a set of audit tools to select which events will be audited and to view the audit trail. If the audit trail becomes full, Valicert VA will shutdown until the Auditor makes space available for the audit trail.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1 (iteration 2) – Valicert VA 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) – Valicert VA records the responsible user in the contents of each audit record.
- FAU_SEL.1 (iteration 2) – Valicert VA provides the ability to determine which events will be audited based on the event type.
- FAU_STG.1 (iteration 2) – Valicert VA protects audit records by only allowing an Auditor to review or delete the audit log via the administrator console. Valicert VA also provides the ability to sign the audit trail so that detections to the audit trail can be identified.
- FAU_STG.4 (iteration 2) – When the audit log becomes full, Valicert VA will shutdown until the Auditor allocates additional space for the audit trail.

6.1.2 Backup and Recovery

Valicert VA includes a backup and restore utility. The utility is invoked from within the TOE. The utility can be used on demand and is capable of restoring a Valicert VA configuration using only the applicable backup files and applicable encryption keys.

The Backup and Recovery function is designed to satisfy the following security functional 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 the configuration.

6.1.3 Access Control

Valicert VA requires all users to authenticate before performing any restricted functions. After a user has successfully authenticated to Valicert VA, the user is presented with a list of functions that user can perform based upon the role associated with the user.

Users can access the TOE only after performing authentication. By enforcing an access control check on all functions based upon the user authentication, Valicert VA ensures that its access control mechanism cannot be bypassed

The Access Control security function satisfies the following security requirements:

- FDP_ACC.1 (iteration 2) – Users are defined internally in Valicert VA and once authenticated, their user identity and associated roles are used to make access decisions. Users are only presented functions associated with their roles.
- FDP_ACF.1 (iteration 2) – Valicert VA uses its access control mechanism to enforce user access and role restrictions defined in Table 7 Access Controls
- FPT_RVM.1 (iteration 2) – Valicert VA offers well-defined interfaces and ensures that users are authenticated and appropriate access control checks are made and enforced prior to allowing a service to be used

6.1.4 Identification and Authentication

There are three roles in Valicert VA. Those roles are: Administrator, Auditor, and Operator. Each role has a specific set of actions it is permitted to per form. The set of actions each role is permitted to perform is defined in Table 8 Authorized Roles for Management of Security Functions Behavior.

Valicert VA supports two types of identification and authentication. For Auditor and Operator, Valicert VA identifies users using certificates. Valicert VA validates the certificate against its internal certificate database when the user first attempts to access the TOE. If the certificate matches an entry, a user session is created for the user. All subsequent user sessions are created with the entry of the userID as long as the certificate is valid. All subsequent requests from that user contain the user session identifier. For Administrators, Valicert VA uses basic (username/password) authentication into the administrative console, and uses the user session identifier as before. The TOE enforces a minimum password structure. The passwords are required to have a minimum of 8 characters, with at least 1 alpha character and 1 numeric character.

Note: The TOE identifies the Officer role as the Operator.

The Identification and authentication security function satisfies the following security requirements:

- FIA_ATD.1 (iteration 2) – Valicert VA defines and maintains the user information that includes user id, authentication method (password-based or certificate-based authentication), authentication data (password or certificate), and the role.
- FIA_UAU.1 (iteration 2) – Valicert VA requires users to authenticate with a valid certificate before performing any actions except requesting the status of a certificate. Administrators must login with a username and password before performing any administrative functions.
- FIA_UID.1 (iteration 2) – Valicert VA requires users to identify themselves with a valid certificate before performing any actions except requesting the status of a certificate. Administrators must identify themselves with a username and password before performing any administrative functions.
- FIA_USB.1 (iteration 2) – Valicert VA ensures that users are associated with their actions by creating a authentication key ID when a user is identified and authenticated, and then associating that authentication key with every request made in the context of the corresponding SSL. For administrative users, the user ID is associated with administrator actions.

- FMT_MOF.1 (iteration 2) – Valicert VA uses the access control mechanism to ensure that the various security roles can only perform appropriate functions as indicated in SFR.
- FMT_MSA.1 (iteration 2) – Valicert VA uses the access control mechanisms to ensure that the Administrator is able to modify the security attributes of the user accounts.
- FMT_SMR.2 (iteration 2)– Valicert VA defines the security roles, provides the ability to associate users to the roles and ensures that a user is able to assume only one role.

6.1.5 Remote Data Entry and Export

Valicert VA is responsible for importing and exporting certificates, keys, key components, certificate status, and other data. Valicert VA protects these data transfers from unauthorized disclosure and modification using SSL sessions. In addition, the TOE provides certificate status information by following means: OCSP responses and CRLs.

The Valicert VA only issues certificates and CRLs in the VA delegated trust model. The directly trusted VA has a self-issued digital certificate that it uses to issue a digital certificate to a subordinate VA. The subordinate VA uses the certificate to sign client OCSP responses only. The directly trusted VA issues Base64encoded X509 certificates.

The directly delegated VA issues standard X509 CRLs to the subordinate VAs. In the VA-delegated model, TOE issues two types of CRLs, full and delta CRLs. The full CRLs are a mirror of the CRLs received from the CAs or a delta CRL that include the serial numbers of the revoked and invalid certificates issued by the directly trusted VA.

The Remote Data Entry and Export function is designed to satisfy the following security functional requirements:

- FCO_NRO_CIMC.3 – Valicert VA generates digital signatures for certificates, CRLs, and OCSPs.
- FDP_UCT.1 (iteration 2), FDP_ITC.1 (iteration 2) – With the exception of the repeaters, communications external to the TOE and internal on remote components are performed over a SSL session. The SSL session protects the data transmitted from unauthorized modification or disclosure. Internal communications between repeaters and responders and external for remote administration are performed over a SSL session. External communications dealing with signed OCSP and CRLs responses are over port 80.
- FDP_CIMC_CSE.1 - The TOE provides certificate status information by OCSP messages (RFC 2560 compliant) and CRLs (X.509 (RFC 3280) 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 protects 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 protects the data transmitted from unauthorized modification or disclosure.

6.1.6 Key Management

Valicert VA supports key management functions. Valicert VA generates and store keys using a FIPS 140-1 validated software module.

The Key Management function is designed to satisfy the following security functional requirements:

- FDP_ACF_CIMC.2 – Certificate private keys are encrypted using a software cryptographic module, and are not stored within the TOE. The private keys are encrypted with 3DES using a symmetric key of 168 bits.
- FMT_MTD.CIMC.4 –All Valicert VA private keys are stored in a software cryptographic module
- FCS_CKM_CIMC.5 – Valicert VA invokes the software cryptographic module to perform all zeroization functions.

6.1.7 Profile Management

Valicert VA offers many options in the area of profile management. All certificate and certificate status requests are generated meeting published standards. In addition to generating standard certificate and status messages, Valicert VA provides profile management so the administrator can set appropriate values for certificate and OCSP profiles.

The Profile Management function is designed to satisfy the following security functional requirements:

The Certificate Management security function satisfies the following security requirements:

- FDP_CIMC_CER.1 – In the VA-delegated model, Valicert VA only generates X.509 v3 certificates that contains the following information:
  - The **version** field contains the integer **2**.
  - The unique sequential **serialNumber** used to identify each certificate issued by the directly trusted VA.
  - The **validity** field specifies a validity period from the current date time to a period in the future. The validity period is configurable by the Administrator.
  - The **issuerUniqueID** field contains the authority key ID of the issuer certificate.
  - The **issuer** field contains the subject DN of the issuing OCSP responder certificate.
  - The **subjectUniqueID** field contains the DHA1 public key hash of the issuing certificate.
  - The **signature** field and the **algorithm** in the **subjectPublicKeyInfo** field are set to SHA-1 with RSA encryption, which is a FIPS-validated algorithm.
- FDP_CIMC_CRL.1 – Valicert VA ensures that issued CRLs contain appropriate values. The following items are checked for validity:
  - The **version** field contains an integer **2,** because of the presence of the X509 v3 Authority Key Identifier.
  - The **issuer** field contains subject DN of the issuing OCSP responder certificate.
  - The **signature** field and the **signatureAlgorithm** in the **subjectPublicKeyInfo** field are set to SHA-1 with RSA encryption, which is a FIPS-validated algorithm.
  - The **thisUpdate** field contains the issue date and time of the CRL.
  - The **nextUpdate** field specified the date and time of the next CRL update.
  - The X509 v3 Authority Key ID.
- FDP_CIMC_OCSP.1 – Valicert VA ensures that issued OCSPs contain appropriate values. The following items are checked for validity:
  - The **version** field contains a **0** by default.
  - The **signatureAlgorithm** field is set to SHA-1 with RSA encryption, which is a FIPS-validated algorithm.
  - The **thisUpdate** field contains the issue date and time of the CRL from which the response is issued.
  - The **producedAt** field shall indicate the time at which the OCSP responder signed the response.
  - The **nextUpdate** field can be set to null, to match the nextUpdate of the CRL from which the response is issued, or can be configured to a specific time by the Administrator. .
- FMT_MOF_CIMC.2 – Valicert VA requires the administrator to specify the set of acceptable values for certificates issued in the VA-delegated trusted model:
  - 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.4 –Valicert VA does not allow the administrator the ability to specify the issuer field of the CRLs issued in the VA-delegated model. The **issuer** contains the distinguished name of the directly trusted VA which is set by default.

- FMT_MOF_CIMC.6 – Valicert VA provides basic OCSP responses. The administrator must specify the set of acceptable values for the following:
  - The **responseType** is by default set to Basic. This is not configurable by the Administrator.
  - The **ResponderID** field by default is set to match signing certificate distinguished or the Administrator can configure the response ID to match the key identifier.

6.2 TOE Security Assurance Measures

6.2.1 Configuration Management

The configuration management measures applied by Tumbleweed ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Tumbleweed ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. Tumbleweed performs configuration management on the TOE, design, tests, user and administrator guidance, life cycle, vulnerability, and the CM documentation.

These activities are documented in:

- Configuration Management Plan for Tumbleweed Validation Authority.

The Configuration management assurance measure satisfies the following EAL 3 assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Delivery and Operation

Tumblweed provides delivery documentation that explains how the TOE is delivered and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Tumblweed's delivery procedures describe the steps to be used for the secure installation, generation, and start-up of the TOE

These activities are documented in:

- Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed Validation Authority™ Version 4.8, Release Date: version 1.6, October 31, 2005.

The Delivery and operation assurance measure satisfies the following EAL 3 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

The Design Documentation provided for the TOE is provided in following documents:

- High-Level Design and Functional Specifications for Tumbleweed Validation Authority,
- CRL Mirroring Design VA 4.5 Release, Tumbleweed,
- Tumbleweed Valicert Validation Authority Operator's Guide Release 4.8, AG-EVA-480-Rev02,
- Identrus Transaction Coordinator CSC Protocol Definition—Version 2.0b,
- JITC OCSP certification, May 11, 2005 (JITC_OCSP_TMWD_VLCT-4.8.pdf),
- FIPS 140-1 certification, 06/10/2004(140crt288.pdf),
- Simple Certificate Validation Protocol (SCVP) Internet-Draft, draft-ietf-pkix-scvp-04.txt.

These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

The Development assurance measure satisfies the following EAL 3 assurance requirements:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Guidance Documents

Tumbleweed provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Tumbleweed Valicert Validation Authority Operator's Guide Release 4.8, AG-EVA-480-Rev02
- Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed Validation Authority Version 4.8, version 1.6, October 31, 2005

The Guidance documents assurance measure satisfies the following EAL 3 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life Cycle Support

The Life Cycle Support documentation describes how 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 it development environment.

These activities are documented in:

- Life-Cycle Support for Tumbleweed Validation Authority version 4.8.

The Life cycle support assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_DVS.1

6.2.6 Tests

The Test Documentation is found in the following documents:

- Testing Documentation for Tumbleweed Validation Authority Version 4.8.

These documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification and high-level design have been appropriately tested.

The Tests assurance measure satisfies the following EAL 3 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability Assessment

Tumbleweed performs vulnerability analyses of the TOE to identify weaknesses that can be exploited in the TOE. A Strength of function rationale will also be provided in the vulnerability analysis.

These activities are documented in:

- Vulnerability Analysis Documentation for Tumbleweed Validation Authority Version 4.8.

The Vulnerability assessment assurance measure satisfies the following EAL 3 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

This section provides the PP conformance claims.

7.1 PP Identification

The TOE conforms to the Certificate Issuing and Management Components (CIMC) Security Level 1 (SL1) Protection Profile (PP), Version 1.0, October 31, 2001.

7.2 PP Tailoring

The Security Environment, Objectives, and Requirements in this ST have been reproduced[4] from the CIMC SL1 PP, as indicated below:

- The Assumptions, Threats, and Policies have been reordered to group the Security Level 1 specific environment statements with the statements that apply to all Security Levels. All of the CIMC SL1 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 1 specific security objectives with the objectives that apply to all Security Levels. All of the CIMC SL1 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 SL1 PP Requirements for the IT environment have been included with the exception of the removes noted below 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 SL1 PP TOE Security Functional Requirements have been included with the exceptions noted below and 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 augmented to be EAL3. The CIMC SL1 PP claims EAL1 augmented. EAL3 is a superset of the CIMC SL1 PP claims.
- The Strength of Function Requirements have been entirely copied from the CIMC SL1 PP. These requirements are presented in Section 5.4.
- The statement of Security Functional and Assurance Requirements has been updated to match the statements given in CC v2.2.

Note that all of the corresponding rationale elements in the CIMC PP have been referenced in Section 8 of the ST.

Security Objective:

Section 4 has been modified to move the following security objective:

- O.Security roles – This objective is moved from the Section 4.3 (IT security objectives for the environment) to Section 4.3 (Security Objectives for both the TOE and the Environment). The objective is associated to the FMT_SMR.2 requirement which is also added to the statement of the requirements for the TOE. The threats and organizational security policy associated with the objective are still applicable, and consistent.

Requirements:

[4] 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.

Section 5.2 has been modified to only include the requirements that are applicable to the TOE. The following requirements are not applicable to the TOE:

- FDP_ACF_CIMC.3 – The TOE does not store the user secret keys. All keys are stored encrypted in the IT environment. The keys are encrypted by the TOE using a FIPS-validated software module.
- FDP_ETC_CIMC.4 – The TOE does not export private and secret keys.
- FMT_MTD_CIMC.5 – The TOE does not store the user secret keys. All keys are stored encrypted in the IT environment. The keys are encrypted by the TOE using a FIPS-validated software module.
- FMT_MTD_CIMC.6 – The TOE does not export private and secret keys.
- FPT_STM.1 – The TOE depends upon the IT environment to provide reliable timestamp for the TOE's use.

The following requirements or elements of a requirement were added to the TOE. The TOE does not rely upon the environment to provide the identified requirements:

- FIA_ATD.1 – The TSF defines and maintains the user security attributes. This requirement has been added to the TOE.
- FMT_MSA.1 – The TSF provides the functions to manage the user security attributes. This requirement had been added to the TOE.
- FMT_SMR.2 – The TSF defines the roles and enforces the role separation. This requirement has been added to the TOE.
- FAU_GEN.1 – The audit events for Identification and Authentication and Account Management are added to the TOE. The TOE provides the functions, monitors, and generates the audit records for the events.
- FMT_MOF.1 – The TSF provides the functions applicable to Account Administration and Identification and Authentication.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

The CIMC PP provides rationale for the security objectives demonstrating that security objectives are suitable to cover the intended environment. The rationale in the CIMC is valid for this ST since no changes have been made to the environment statements.

8.2 Security Requirements Rationale

The CIMC PP provides rationale for the security functional requirements demonstrating that security functional requirements are suitable to address the security objectives. The rationale in the CIMC is valid for this ST. There is one additional security functional requirement in this ST. The following paragraph provides the rationale for the change.

The O.Certificates objective addresses this added requirement because it ensures the OCSP response is valid. The additional requirement is acceptable since the CIMC PP assumed the TOE dealt only with a server and in the case of the Valicert VA, the client is included in the TOE.

Additionally the requirement FMT_SMR.2 has been expanded to include the Auditor role from SL3. This expansion is consistent with the objectives rationale in the CIMC PP and the TOE SFRs include the Auditor role for consistency and completeness.

The Data import/export objective is adequately satisfied with FPT_ITC.1 (iteration 1 and 2) and FDP_UCT.1 (iterations 1 and 2). The two requirements ensure that data other than private and security keys are protected when they are transmitted to and from the CIMC. The TOE does not import or export private and secret keys outside the TOE boundaries.

The modification made to the TOE statement of requirements does not affect the mapping of the security objectives given in the PP with the exception of O.Security Roles. Other affected security objectives are for the TOE and the Environment. Therefore the rationale given in the PP is applicable.

8.3 Security Assurance Requirements Rationale

The assurance requirements for CIMCs at Security Level 1 are the requirements for EAL 1 with the addition of ATE_FUN.1 Functional Testing and AVA_SOF.1 Strength of TOE Security Function Evaluation. These requirements are designed to provide evidence that the CIMC functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.. This ST has increased the assurance level to EAL3. While the EAL chosen is not the same as is specified in the CIMC PP, this ST remains CIMC PP

conformant because the EAL chosen in this ST (EAL3) is hierarchical to the EAL specified in the CIMC PP. EAL 3 was chosen instead of EAL 1 augmented because it is the highest level of commercial assurance without significant product or development changes.

8.4 Strength of Functions Rationale

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 FIPS 140-1 Level for Validated Cryptographic Module.

The TOE provides an authentication mechanism (password) that meets the strength of the function level defined in Section 5.4.1 Authentication Mechanisms.

8.5 Requirement Dependency Rationale

The CIMC provides rationale for the completeness of security functional requirements. The rationale in the CIMC is valid for this ST.

FMT_SMF.1 requirement is not included in the ST because the requirement only explicitly states what is implied with the inclusion of the FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1. The management requirements identify all the functions that the TOE provides. Any functions not provides by the TOE are clearly identified in Section 6 TOE Summary Specification.

8.6 Explicitly Stated Requirements Rationale

The CIMC provides rationale for the explicitly stated security functional requirements. The rationale in the CIMC is valid for this ST.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6 TOE Summary Specification describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6 TOE Summary Specification provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 11 Security Functions vs. Requirements demonstrates the relationship between security requirements and security functions.

Table 11 Security Functions vs. Requirements

	Security Audit	Backup and Recovery	Access Control	Identification and Authentication	Remote Data Entry and Export	Key Management	Profile Management
FAU_GEN.1 (iteration 2)	X						
FAU_GEN.2 (iteration 2)	X						
FAU_SEL.1 (iteration 2)	X						
FAU_STG.1 (iteration 2)	X						
FAU_STG.4 (iteration 2)	X						
FCO_NRO_CIMC.3					X		
FCS_CKM_CIMC.5						X	
FDP_ACC.1 (iteration 2)			X				
FDP_ACF.1 (iteration 2)			X				
FDP_ACF_CIMC.2						X	
FDP_CIMC_BKP.1		X					
FDP_CIMC_CER.1							X
FDP_CIMC_CRL.1							X
FDP_CIMC_CSE.1					X		
FDP_CIMC_OCSP.1							X
FDP_ITT.1 (iteration 3 & 4)					X		
FDP_UCT.1 (iteration 2)					X		
FIA_ATD.1 (iteration 2)				X			
FIA_UAU.1 (iteration 2)				X			
FIA_UID.1 (iteration 2)				X			
FIA_USB.1 (iteration 2)				X			
FMT_MOF.1 (iteration 2)				X			
FMT_MOF_CIMC.2							X
FMT_MOF_CIMC.4							X
FMT_MOF_CIMC.6							X
FMT_MSA.1 (iteration 2)				X			
FMT_MTD_CIMC.4						X	
FMT_SMR.2 (iteration 2)				X			
FPT_ITC.1 (iteration 2)					X		
FPT_ITT.1 (iteration 3 & 4)					X		
FPT_RVM. (iteration 2)			X				

8.8 PP Claims Rationale

All environment statements, security objectives, and security functional requirements were copied directly from the CIMC PP. This requirement is addressed by the objectives in the CIMC PP as described in the Security Requirements rationale. For additional information see Section 7, Protection Profile Claims.

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.