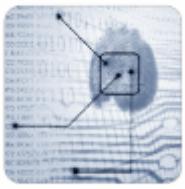
OPENTRUST™

OpenTrust PKI v4

Security Target



OpenTrust SA
15-17, avenue de Ségur
F-75007 Paris
France

Document Information

Purpose	OpenTrust PKI v4 Security Target
Applicable to	OpenTrust PKI version 4.3.4
Reference	pki-cc-st
Version	2.2
Revision	r96095
Last modified	Wed, 03 Jun 2009
Status	VALIDATED

Table of Contents

1. Security Target Introduction

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

1.1. Identification

ST Title	OpenTrust PKI v4 Security Target
ST Reference	pki-cc-st v2.2 r96095
TOE Identification	OpenTrust PKI v4.3.4
CC Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1
PP Conformance	Certificate Issuing and Management Components (CIMC) Security Level 2 Protection Profile, Version 1.0, October 31, 2001
Assurance Level	Evaluation Assurance Level 3 augmented with ALC_CMS.4 and ALC_FLR.2

1.2. TOE overview

1.2.1. Usage and major security features of a TOE

1.2.1.1. TOE Usage

Below are some of the key usage of the OPENTRUST-PKI product:

- Policy-based generating and distributing Public Key (including X.509) Certificates
- Secure management of multiple profiles (certificate, authority, security)
- Certificate enrolment or request based on
- Generation of key pairs in centralized mode (for encryption), decentralized mode (for authentication and signature) or mixed mode (for mixed populations)
- Certificate renewal/revocation/retrieval
- Key backup and recovery (simple or partitioned, online or offline)
- Multiple Certification and Registration Authorities
- Certification and CRL (Certificate Revocation Lis) Management
- OCSP (Online Certificate Status Protocol) Responder
- Certificate database backup and restore

1.2.1.2. TOE Security Services

This section lists and describes, at a high level, the security functions that are provided by the TOE:

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

  Each of these functions is further defined and mapped to requirements in Section 7.

Security Audit

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

Roles

The TOE implements the required roles specified in the PP at the security level 2: Administrator and Officer. The 2 other definitions, Operator and Auditor are agregated to the Administrator role in this target.

Access Control

The TOE enforces user roles and access control whenever users access TOE-provided functions. The TOE maintains a secure database of authorized operators, including all identities and permissions.

Access Control is defined by a list of rules composed of Resource, Principal, Right and Privilege.

Backup and Recovery

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

Identification and Authentication

The TOE requires identification and authentication before performing any security-relevant functions. The TOE maintains a secure database of authorized

operators, including all certificate information and roles that can be assumed. Users of the TOE are authenticated during the establishment of the mutually authenticated TLS connection.

Remote Data Entry and Export

The TOE provides mecanisms to secure remote data entry and export over an untrusted exchange environment or network.

Key Management

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

Certificate Management

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

The TOE processes certificate requests formatted according to the following standards: PKCS#7, PKCS#10. The TOE generates certificates and CRLs according to the following standard: RFC 3280 Internet X.509 PKI Certificate and CRL Profile.

1.2.2. TOE type

OPENTRUST PKI is a software suite for implementing a Public Key Infrastructure (PKI). It can be used to implement a wide variety of infrastructures from the most basic to the most structurally complex and provides a certificate management solution for:

- Encryption - Server authentication (Web, VPN, application servers etc.)
- Client Authentication
- Digital Signatures

1.2.3. Required non-TOE hardware/software/firmware

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

1.2.3.1. Hardware and operating system platform (Abstract Machine)

The TOE abstract machine consists of the SUSE Linux Enterprise Server (SLES) v10 operating system and any hardware for which the operating system and TOE configurations are valid. The justification for excluding the abstract machine from the TOE boundary is based on the following factors, described below.

Operating system: The TSP is enforced by the TOE, and the SFRs are completely satisfied by TOE functions (aside from those with environmental dependencies). The operating system with which the TOE interfaces is assumed to be trusted, meaning that it can be relied upon to correctly execute the TOE functions. As well, Linux SLES 10 operating system has been certified Common Criteria EAL4+.

Hardware independence: The OpenTrust PKI software is optimized to execute any x86 (i.e., Intel or equivalent processor)-based machines, regardless of the hardware vendor. That is, any hardware platform that meets the following minimum system requirements: Intel 32bits architecture, 1 Go Ram, HD Storage 36 Go (Raid 5 recommended), Pentium 4 or better.

No interaction with hardware platform: The OpenTrust PKI software does not interact with the hardware platform directly. That is, the software interacts with the operating system, which is assumed to be trusted. The operating system, in turn, interacts with the hardware platform (e.g., via the computer's BIOS and/or various device drivers).

1.2.3.2. OpenTrust PKI Database

The justification for excluding the database from the OpenTrust PKI TOE boundary is based on the following factors, described below.

Database security provided by OpenTrust PKI: This Security Target makes no claims about inherent database security. All database security (i.e., confidentiality and integrity) is provided by OpenTrust PKI, not the database. As such, all sensitive data items stored in the OpenTrust PKI database are encrypted.

Database functionality not mapped to SFRs: This Security Target makes no claims about database functionality (aside from the inherent, fundamental, and basic function of data storage). The OpenTrust PKI database operates only as a data warehouse for user and system data. Database functionality is not mapped to any of the SFRs in this Security Target.

1.2.3.3. Hardware Security Module

A hardware security module, HSM, is part of the TOE IT Environment. The TOE relies on FIPS validated (nCipher nShield or NetHSM, Utimaco CryptoServer) or Common Criteria EAL4+ certified (Bull Trustway) cryptographic security modules to provide all FIPS 140-1 for FIPS 140-2 approved cryptography and key management.

1.3. TOE description

The OPENTRUST-PKI software suite comprises numerous modules and entities that ensure both basic and advanced PKI features and functions.

1.3.1. Operational structure

The following diagram shows an example of OPENTRUST-PKI operational structure.

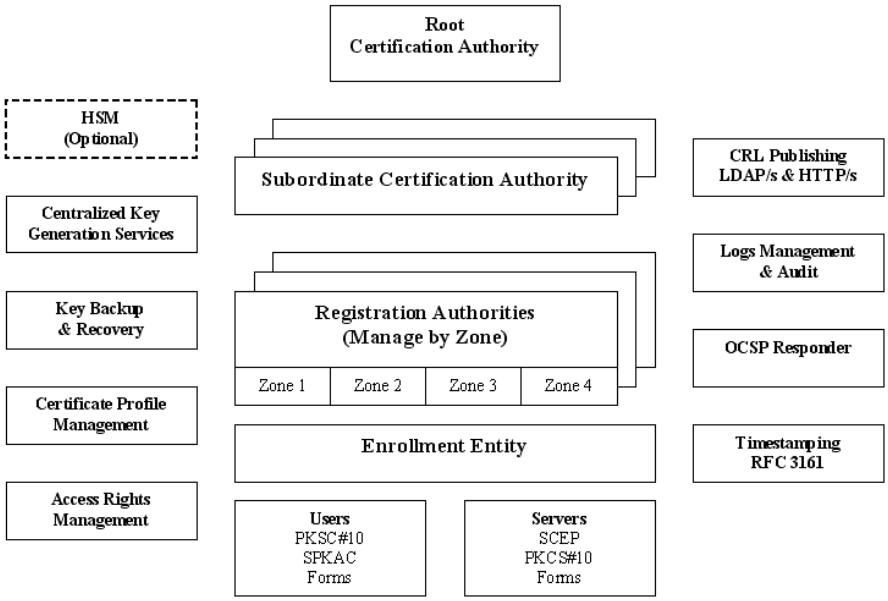


Figure 1. PKI Operational Structure Sample

All modules shown in the above diagram are available as part of the OPENTRUST-PKI solution.

The Root Certification Authority

The Root Certification Authority assures the following functions:

- Hardware or software root key generation
- The signature of Subordinate Certification Authority certificates from an external PKCS#10 request or a request originating from private key generation on the Root CA or a HSM.
- The revocation of Subordinate Certification Authorities
- The issuing of Certificate Revocation List (CRL)

Subordinate Certification Authorities

OPENTRUST-PKI enables implementation of an unlimited number of Subordinate Certification Authorities able to issue different types of certificates.

A Subordinate Certification Authority ensures the following functions:

- Generation of user or server keys, via a software or hardware key generation center. This is "centralized" key generation mode (used primarily for encryption keys that must be backed up)
- Signature of Certificate Requests (PKCS#10) generated by third-party applications (applications of users or servers making the request)
- Backup of encryption key pairs on the backup and recovery module (for centralized mode only)
- Revocation of certificates and immediate issuing/ publication of a CRL using the publication module
- Automatic and scheduled publication of the CRL
- Management of Certificate Renewal (email reminders, renewal assistance, automatic renewal of certain certificates etc.)

Registration Authority

The OPENTRUST-PKI Registration Authority validates the different requests associated with the life-cycle of the certificates (initial request, validation, renewal, recovery, revocation). It also enables management of centralized requests (i.e. performed by an authorized agent - PKI officer - for a third party) and the customization of centrally initialized user tokens (retrieval of a PKCS#12 to be placed on a smart card or USB dongle).

A Registration Authority ensures the following functions:

- Validation/modification/refusal of certificate requests (with possibility of managing certificate extensions)
- Validation/ refusal of key recovery requests
- Validation/refusal of revocation requests
- Validation/refusal of renewal requests
- Search/retrieval of issued certificates
- Creation/validation of certificate, revocation or recovery request

1.3.2. Technical Architecture

Modules can be deployed on just one machine or several machines according to the client deployment architecture.

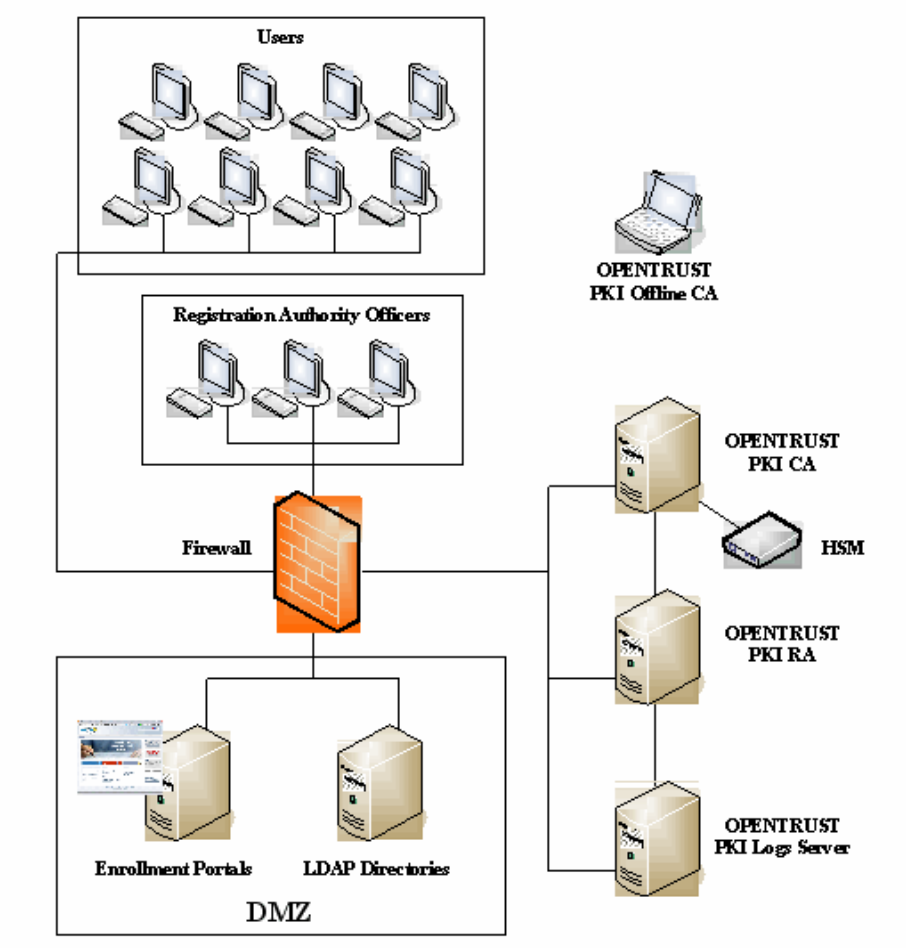


Figure 2. Multi machines deployement architecture sample

1.3.3. TOE Boundary

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

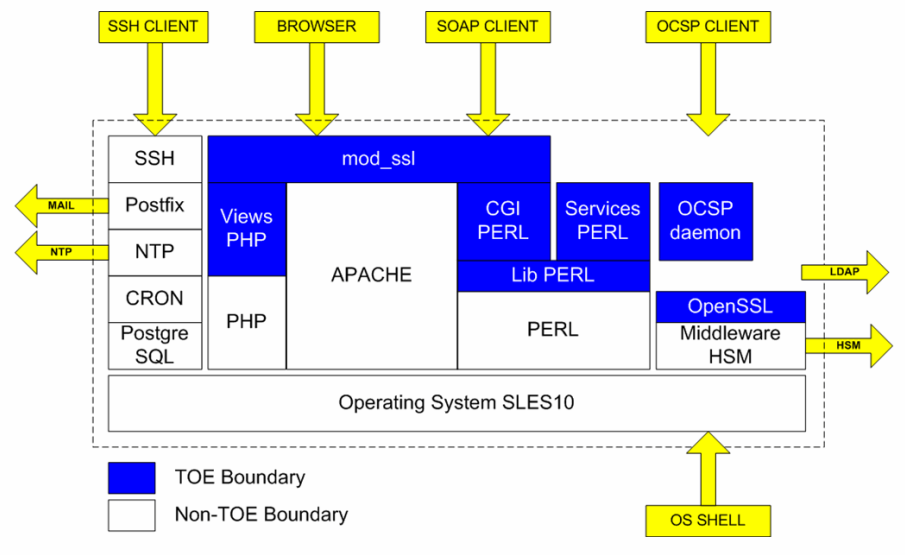


Figure 3. OpenTrust PKI Technical Components

For this evaluation, the logical scope of the TOE is illustrated in the following figure.

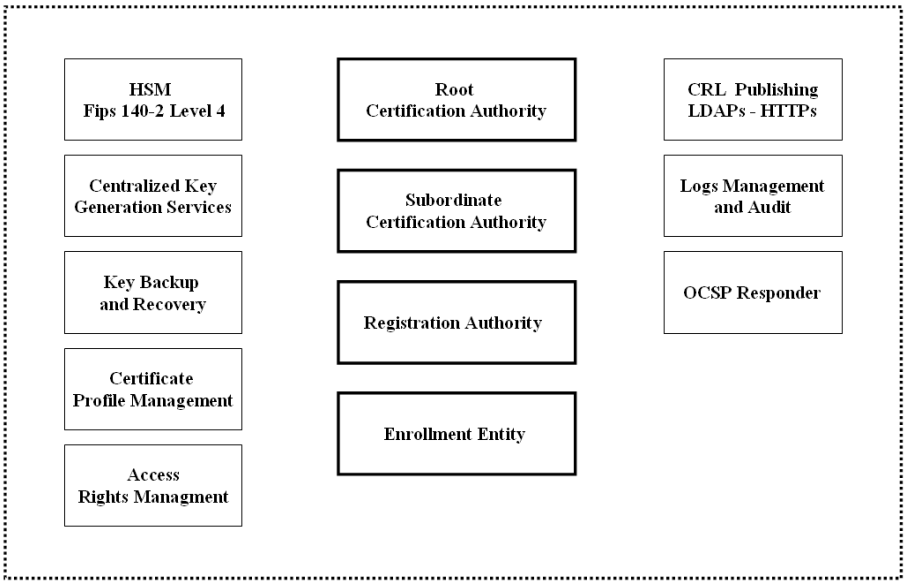


Figure 4. Evaluated logical scope of the TOE

For this evaluation, the target deployment is the one-machine architecture model based on the following configuration:

- Machine Model: HP ProLiant DL360 G3
- Operating System: SUSE Linux Enterprise Server 10 SP1
- HSM: nCipher nShield PCI

2. Conformance Claims

2.1. CC conformance claim

The TOE conforms to:

- Common Criteria for Information Technology Security Evaluation, Version 3.1, part 2 extended.
- Common Criteria for Information Technology Security Evaluation, Version 3.1, part 3 conformant.
  - Evaluation Assurance Level 3 augmented with ALC_CMS.4, and ALC_FLR.2.

2.2. PP conformance claim

As previously mentioned in this ST, OpenTrust PKI is strictly conformed to the following Protection Profile (PP): Certificate Issuing and Management Components (CIMC) Security Level 2 PP, version 1.0, October 31, 2001.

2.3. Conformance rationale

All of the assumptions, threats, policies, objectives and security requirements defined for CIMC PP Security Level 2 (which includes also the ones defines for all levels) have been reproduced in this ST and adapted for CC v3.1. No additional assumption, threat, policy, objective or security requirement has been used.

All operations performed on the IT security requirements are within the bounds set by the CIMC PP for Security Level 2. Assignment and selection operations on security requirements are indicated in Section 5.

3. Security problem definition

This section includes the following:

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

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

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 securityissues 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. Connectivity

A.Operating System	The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the appropriate Security Level identified in this family of PPs.

3.1.3. Physical

A.Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected fromun authorized physical modification.

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	A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.
T.Flawed code	A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

3.2.3. Cryptography

T.Disclosure of private and secret keys	A private or secret key is improperly disclosed.
T.Modification of private/ secret keys	A secret/private key is modified.

3.2.4. External Attacks

T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.
T.Hacker physical access	A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

3.3. Organizational Security Policies

P.Authorized use of information	Information shall be used only for its authorized purpose(s).
P.Cryptography	FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

4. Security Objectives

4.1. Security Objectives for the TOE

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 both the TOE and the Environment

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

O.Configuration Management	Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.
O.Data import/export	Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
O.Detect modifications of firmware, software, and backup data	Provide integrity protection to detect modifications to firmware, software, and backup data.
O.Individual accountability and audit records	Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.
O.Integrity protection of user data and software	Provide appropriate integrity protection for user data and software.
O.Limitation of administrative access	Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.
O.Maintain user attributes	Maintain a set of security attributes (which may include role membership. access privileges, etc.) associated with individual users. This is in addition to user identity.
O.Manage behavior of security functions	Provide management functions to configure, operate, and maintain the security mechanisms.
O.Object and data recovery free from malicious code	Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.
O.Procedures for preventing malicious code	Incorporate malicious code prevention procedures and mechanisms.
O.Protect stored audit records	Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

O.Protect user and TSF data during internal transfer	Ensure the integrity of user and TSF data transferred internally within the system.
O.Require inspection for downloads	Require inspection of downloads/transfers.
O.Respond to possible loss of stored audit records	Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.
O.Restrict actions before authentication	Restrict the actions a user may perform before the TOE authenticates the identity of the user.
O.Security-relevant configuration management	Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
O.Time stamps	Provide time stamps to ensure that the sequencing of events can be verified.
O.User authorization management	Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.
O.React to detected attacks	Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.

Common Criteria version 3.1 require the strict separation between security objectives for the TOE and security objectives for the operational environment. This section is directly extracted from the CIMC protection profile and is however considered as acceptable because:

a. separation between security requirements for the TOE and security requirements for the environment is clearly defined in the rationale for objectives coverage (section 6.3)

b. security requirements statement is the basis for CC 3.1 evaluation tasks (e.g. for ADV class evaluation workunits).

4.3. Security Objectives for the Environment

4.3.1. Non-IT security objectives for the environment

O.Administrators, Operators, Officers and Auditors guidance documentation	Deter Administrator, Operator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.
O.Auditors Review Audit Logs	Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.
O.Authentication Data Management	Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)
O.Communications Protection	Protect the system against a physical attack on the communications capability by providing adequate physical security.
O.Competent Administrators, Operators, Officers and Auditors	Provide capable management of the TOE by assigning competent Administrators, Operators, Officers and Auditors to manage the TOE and the security of the information it contains.
O.CPS	All Administrators, Operators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.
O.Disposal of Authentication Data	Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).
O.Installation	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

O.Malicious Code Not Signed	Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.
O.Notify Authorities of Security Issues	Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
O.Physical Protection	Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.
O.Social Engineering Training	Provide training for general users, Administrators, Operators, Officers and Auditors in techniques to thwart social engineering attacks.
O.Cooperative Users	Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE.
O.Lifecycle security	Provide tools and techniques used during the development phase to ensure security is designed into the CIMC. Detect and resolve flaws during the operational phase.
O.No Abusive Administrators, Operators, Officers and Auditors	Use trustworthy Administrators, Operators, Officers and Auditors.
O.Repair identified security flaws	The vendor repairs security flaws that have been identified by a user.

4.3.2. IT security objectives for the environment

O.Cryptographic functions	The TOE must implement approved cryptographic algorithms for encryption/ decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. (Validated is defined as FIPS 140-1 validated.)
O.Operating System	The operating system used is validated to provide adequate security, including domain separation and non- bypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology.
O.Periodically check integrity	Provide periodic integrity checks on both system and software.
O.Security roles	Maintain security-relevant roles and the association of users with those roles.
O.Validation of security function	Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

4.4. Security objectives rationale

Because the security problem definition and the security objectives are directly extracted from the CIMC protection profile, the rationale from the PP is directly applicable.

5. Extended components definition

Extended components have been defined in the CIMC Protection Profile.

Extended security requirements are explicitly identified and listed in Table 1.

6. Security Requirements

6.1. TOE Security Requirements

Table 1 lists all the functional security requirements for the TOE.

Security Functional Requirement	Security Function	CC Part2 extended
FAU_GEN.1 Audit data generation	Security Audit	
FAU_GEN.2 User identity association	Security Audit	
FAU_SEL.1 Selective audit	Security Audit	
FAU_STG.1 Protected audit trail storage	Security Audit	
FAU_STG.4 Prevention of audit data loss	Security Audit	
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	Remote Data Entry and Export	yes
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	Key Management	yes
FDP_ACC.1 Subset access control	Access Control	
FDP_ACF.1 Security attribute based access control	Access Control	
FDP_ACF_CIMC.2 User private key confidentiality protection	Key Management	yes
FDP_ACF_CIMC.3 User secret key confidentiality protection	Key Management	yes
FDP_CIMC_BKP.1 CIMC backup and recovery	Backup and Recovery	yes
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	Backup and Recovery	yes
FDP_CIMC_CER.1 Certificate Generation	Certificate Management	yes
FDP_CIMC_CRL.1 Certificate Revocation	Certificate Management	yes
FDP_CIMC_CSE.1 Certificate status export	Certificate Management	yes
FDP_CIMC_OCSP.1 Basic Response Validation	Certificate Management	yes
FDP_ETC_CIMC.4 User private and secret key export	Key Management	yes
FDP_ITT.1 Basic internal transfer protection (iterations 1 and 2)	Remote Data Entry and Export	
FDP_UCT.1 Basic data exchange confidentiality	Remote Data Entry and Export	
FIA_UAU.1 Timing of authentication	Identification and Authentication	
FIA_UID.1 Timing of identification	Identification and Authentication	
FIA_USB.1 User-subject binding	Identification and Authentication	
FMT_MOF.1 Management of security function behavior	Roles	
FMT_MOF_CIMC.3 Extended certificate profile management	Certificate Management	yes
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	Certificate Management	yes
FMT_MOF_CIMC.6 OCSP Profile Management	Certificate Management	yes
FMT_MTD_CIMC.4 TSF private key confidentiality protection	Key Management	yes
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	Key Management	yes
FMT_MTD_CIMC.6 TSF private and secret key export	Key Management	yes

Security Functional Requirement	Security Function	CC Part2 extended
FPT_CIMC_TSP.1 Audit log signing event	Security Audit	yes
FPT_ITC.1 Inter-TSF confidentiality during transmission	Remote Data Entry and Export	
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 1 and 2)	Remote Data Entry and Export	
FPT_STM.1 Reliable time stamps	Security Audit	

Table 1. CIMC TOE Functional Security Requirements

6.1.1. Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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

a. Start-up and shutdown of the audit functions;

b. All auditable events for the minimum level of audit; and

c. The events listed in Table 2 below.

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*additional audit relevant information*].

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

Dependencies:

- FPT_STM.1 Reliable time stamps

Security Function	Component	Event
Security Audit	FAU_GEN.1	Any changes to the audit parameters
Security Audit	FAU_GEN.1	Any attempt to delete the audit log
Security Audit	FPT_CIMC_TSP.1	Audit log signing event
Remote Data Entry and Export		All security-relevant data that is entered in the system (local data entry)

Security Function	Component	Event
Remote Data Entry and Export		All security-relevant messages that are received by the system (remote data entry)
Remote Data Entry and Export		All successful and unsuccessful requests for confidential and security-relevant information
Key Management		Whenever the TSF requests generation of a cryptographic key
Key Management		The loading of Component private keys
Key Management		All access to certificate subject private keys retained within the TOE for key recovery purposes
Key Management		All changes to the trusted public keys, including additions and deletions
Key Management	FDP_ETC_CIMC.4, FMT_MTD_CIMC.6	The export of private and secret keys
Certificate Management	FDP_CIMC_CER.1	All certificate requests
Certificate Management		All requests to change the status of a certificate
Certificate Management		Any security-relevant changes to the configuration of the TSF
Certificate Management	FMT_MOF_CIMC.3	All changes to the certificate Profile
Certificate Management	FMT_MOF_CIMC.5	All changes to the certificate revocation list Properties

[1]The TOE allows only one CRL profile which is hard coded. Therefore no change can be made on CRL profile properties.
[2]The TOE allows only one OCSP profile which is hard coded. Therefore no change can be made on OCSP profile properties.

Table 2. Auditable Events and Audit Data [1] [2]

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies:

- FAU_GEN.1 Audit data generation
- FIA_UID.1 Timing of identification

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes:

a. [*object identity, event type*]

b. [*date*].

Dependencies:

- FAU_GEN.1 Audit data generation
- FMT_MTD.1 Management of TSF data

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to detect unauthorised modifications to the stored audit records in the audit trail.

Dependencies:

- FAU_GEN.1 Audit data generation

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall [*prevent audited events, except those taken by the authorised user with special rights*] and [no other actions in case of audit storage failure] if the audit trail is full.

Dependencies:

- FAU_STG.1 Protected audit trail storage

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Dependencies:

- No dependencies.

FPT_CIMC_TSP.1 Audit log signing event

Hierarchical to: No other components.

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

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

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

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

Dependencies:

- FAU_GEN.1 Audit data generation
- FMT_MOF.1 Management of security functions behavior

6.1.2. Roles

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in Table 3 to the authorised roles as specified in Table 3.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

Security Function	Component	Function/Authorised Role
Security Audit		The capability to configure the audit parameters shall be restricted to Administrators.
Security Audit		The capability to change the frequency of the audit log signing event shall be restricted to Administrators.
Backup and Recovery		The capability to configure the backup parameters shall be restricted to Administrators.
Backup and Recovery		The capability to initiate the backup or recovery function shall be restricted to Administrators.
Key Management		Private Key export shall be performed by the Administrators.
Certificate Management		The capability to approve fields or extensions to be included in a certificate shall be restricted to Officers.
Certificate Management		If an automated process is used to approve fields or extensions to be included in a certificate, the

Security Function	Component	Function/Authorised Role
		capability to configure that process shall be restricted to Officers.
Certificate Management		Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate.
Certificate Management	FMT_MOF_CIMC.3	The capability to modify the certificate profile shall be restricted to Administrators.
Certificate Management	FMT_MOF_CIMC.5	The capability to modify the certificate revocation list properties shall be restricted to Administrators.
CIMC Configuration		The capability to configure any TSF functionality shall be restricted to Administrators.

[1]The TOE allows only one CRL profile which is hard coded. Therefore no operation can be made on CRL profile.
[2]The TOE allows only one OCSP profile which is hard coded. Therefore no operation can be made on OCSP profile.

Table 3. Authorised Roles for Management of Security Functions Behavior [1] [2]

6.1.3. Backup and recovery

FDP_CIMC_BKP.1 CIMC backup and recovery

Hierarchical to: No other components.

FDP_CIMC_BKP.1.1 The TSF shall include a backup function.

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

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

a. a copy of the same version of the CIMC as was used to create the backup data;

b. a stored copy of the backup data;

c. the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and

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

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

Dependencies:

- FMT_MOF.1 Management of security functions behavior

FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Hierarchical to: No other components.

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

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

Dependencies:

- FDP_CIMC_BKP.1 CIMC backup and recovery

6.1.4. Access Control

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 8.2 on [*resource, principal, right, privilege*].

Dependencies:

- FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 8.2 to objects based on the following: the identity of the subject and the set of roles that the subject is authorised to assume.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules specified in Table 4.

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

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

Dependencies:

- FDP_ACC.1 Subset access control

- FMT_MSA.3 Static attribute initialization

Security Function	Component	Event
Remote Data Entry and Export		The entry and export of confidential and security-relevant data shall only be at the request of authorised users.
Key Management		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.
Key Management		The capability to request the loading of Component private keys into cryptographic modules shall be restricted to Administrators.
Key Management		The capability to decrypt certificate subject private keys within a CIMC shall be restricted to Officers.
Key Management		The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators.
Key Management		The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators and Officers.
Key Management		The capability to export a component private key shall be restricted to Administrators.
Key Management		The capability to export certificate subject private keys shall be restricted to Officers.
Certificate Management		The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate.
Certificate Management		The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked.
Certificate Management		Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate.
Certificate Management		Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

Table 4. Access Controls

6.1.5. Identification and Authentication

Identification and authentication includes recognizing an entity (e.g., user, device, or system) and verifying the identity of that entity.

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [*few EE (enrolment entity) requests and public information retrieval 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.

Dependencies:

- FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [*few EE (enrolment entity) requests and public information retrieval 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.

Dependencies:

- No dependencies.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

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

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: [*no rules for the initial association of attributes*].

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

Dependencies:

- FIA_ATD.1 User attribute definition

6.1.6. Remote Data Entry and Export

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

Hierarchical to: FCO_NRO.2

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

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

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

Dependencies:

- FIA_UID.1 Timing of identification

FDP_ITT.1 Basic internal transfer protection (iteration 1)

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 8.2 to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the TOE.

Dependencies:

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

FDP_ITT.1 Basic internal transfer protection (iteration 2)

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 8.2 to prevent the disclosure of confidential user data when it is transmitted between physically-separated parts of the TOE.

Dependencies:

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

FDP_UCT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 8.2 to be able to transmit user data in a manner protected from unauthorised disclosure.

Dependencies:

- [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
- [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FPT_ITC.1 Inter-TSF confidentiality during transmission

Hierarchical to: No other components.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Dependencies:

- No dependencies

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

Hierarchical to: No other components.

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

Dependencies:

- No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection (iteration 2)

Hierarchical to: No other components.

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

Dependencies:

- No dependencies

FDP_CIMC_CSE.1 Certificate status export

Hierarchical to: No other components.

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

Dependencies:

- No dependencies

6.1.7. Key Management

FDP_ACF_CIMC.2 User private key confidentiality protection

Hierarchical to: No other components.

FDP_ACF_CIMC.2.1 CIMS personnel private keys shall be stored in a FIPS 140-1 validated cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-1 validated cryptographic module.

FDP_ACF_CIMC.2.2 If certificate subject private keys are stored in the TOE, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the FIPS 140-1 validated cryptographic module.

Dependencies:

- No dependencies

FMT_MTD_CIMC.4 TSF private key confidentiality protection

Hierarchical to: No other components.

FMT_MTD_CIMC.4.1 CIMC private keys shall be stored in a FIPS 140-1 validated cryptographic module or stored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-1 validated cryptographic module.

Dependencies:

- No dependencies

FDP_ACF_CIMC.3 User secret key confidentiality protection

Hierarchical to: No other components.

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

Dependencies:

- No dependencies

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

Hierarchical to: No other components.

FMT_MTD_CIMC.5.1 TSF secret keys stored within the TOE, but not within a FIPS 140-1 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-1 validated cryptographic module.

Dependencies:

- No dependencies

FCS_CKM_CIMC.5 CIMC private and secret key zeroization

Hierarchical to: No other components.

FCS_CKM_CIMC.5.1 The TSF shall provide the capability to zeroize plaintext secret and private keys within the FIPS 140-1 validated cryptographic module.

Dependencies:

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

FDP_ETC_CIMC.4 User private and secret key export

Hierarchical to: No other components.

FDP_ETC_CIMC.4.1 Electronically distributed private and secret keys shall only be exported from the TOE in encrypted form.

FDP_ETC_CIMC.4.2 Certificate subject private keys that are used to generate digital signatures shall not be exported from the TOE in plaintext form.

Dependencies:

- No dependencies

FMT_MTD_CIMC.6 TSF private and secret key export

Hierarchical to: No other components.

FMT_MTD_CIMC.6.1 Electronically distributed private and secret keys shall only be exported from the TOE in encrypted form.

Dependencies:

- No dependencies

6.1.8. Certificate Management

FMT_MOF_CIMC.3 Extended certificate profile management

Hierarchical to: FMT_MOF_CIMC.2

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

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

- the key owner's identifier;

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

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

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

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

Dependencies:

- FMT_MOF.1 Management of security functions behavior
- FMT_SMR.1 Security roles

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: FMT_MOF_CIMC.4

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

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

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

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

Dependencies:

- FMT_MOF.1 Management of security functions behavior
- FMT_SMR.1 Security roles

FMT_MOF_CIMC.6 OCSP profile management

Hierarchical to: No other components.

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

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

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

Dependencies:

- FMT_MOF.1 Management of security functions behavior
- FMT_SMR.1 Security roles

FDP_CIMC_CER.1 Certificate Generation

Hierarchical to: No other components.

FDP_CIMC_CER.1.1 The TSF shall only generate certificates whose format complies with [*the X.509 standard for public key certificates*].

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

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

FDP_CIMC_CER.1.4 If the TSF generates X.509 public key certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that:

a. The **version** field shall contain the integer **0**, **1**, or **2**.

b. If the certificate contains an **issuerUniqueID** or **subjectUniqueID** then the version field shall contain the integer **1** or **2**.

c. If the certificate contains **extensions** then the **version** field shall contain the integer **2**.

d. The **serialNumber** shall be unique with respect to the issuing Certification Authority.

e. The **validity** field shall specify a **notBefore** value that does not precede the current time and a **notAfter** value that does not precede the value specified in **notBefore**.

f. If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **issuerAltName** extension.

g. If the **subject** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical **subjectAltName** extension.

h. The **signature** field and the **algorithm** in the **subjectPublicKeyInfo** field shall contain the OID for a FIPS-approved or recommended algorithm.

Dependencies:

- No dependencies.

FDP_CIMC_CRL.1 Certificate revocation list validation

Hierarchical to: No other components.

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

1. If the **version** field is present, then it shall contain a **1**.

2. If the CRL contains any critical extensions, then the **version** field shall be present and contain the integer 1.

3. If the **issuer** field contains a null **Name** (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical **issuerAltName** extension.

4. The **signature** and **signatureAlgorithm** fields shall contain the OID for a FIPS-approved digital signature algorithm.

5. The **thisUpdate** field shall indicate the issue date of the CRL.

6. The time specified in the **nextUpdate** field (if populated) shall not precede the time specified in the **thisUpdate** field.

Dependencies:

- No dependencies

FDP_CIMC_OCSP.1 OCSP basic response validation

Hierarchical to: No other components.

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

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

Dependencies:

- No dependencies

6.2. TOE Security Assurance Requirements

the EAL 2 augmentations in the CIMC SL2 PP bring the assurance level nearly to EAL 3. As a result, **EAL3 augmented with ALC_CMS.4 and ALC_FLR.2** components has been selected as the overall assurance level for the TOE.

Assurance Class	Component	Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.3	Authorisation controls
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
Security target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction

Assurance Class	Component	Title
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 5. Assurance Requirements

6.3. Security requirements rationale

The security requirements rationale is directly extracted from the PP except for the items described below.

Because the protection profile is compliant with the CC version 2.1 and that the TOE claims a conformity with CC version 3.1, the security requirements rationale is adapted as follow :

- FPT_RVM.1 does not exist anymore in CC 3.1: functional requirements are replaced by assurance requirements from ADV_ARC.1 component.
- dependency between the component FMT_MOF.1 and the component FMT_SMF.1 did not exist in CC 2.1 : the dependency is not satisfied in this security target because management functions are already required by explicit components FMT_MOF_CIMC.3, FMT_MOF_CIMC.5 and FMT_MOF_CIMC.6.

6.3.1. SFR Dependencies

Table 6 lists all the security requirements dependencies for Security Level 2.

Component	Dependencies	Which is:
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1	Included
	FIA_UID.1	Included
FAU_SEL.1	FAU_GEN.1	Included
	FMT_MTD.1	Not included but covered by FMT_MTD_CIMC.4, FMT_MTD_CIMC.5 and FMT_MTD_CIMC.6
FAU_STG.1	FAU_GEN.1	Included
FAU_STG.4	FAU_STG.1	Included
FCO_NRO_CIMC.3	FIA_UID.1	Included
FCS_CKM_CIMC.5	FCS_CKM.4	Not included because secret keys are stored within the HSM and the operation of erasing is done internally by the HSM

Component	Dependencies	Which is:
	FDP_ACF.1	Included
FDP_ACC.1	FDP_ACF.1	Included
FDP_ACF.1	FDP_ACC.1	Included
	FMT_MSA.3	Not included because none default profile is present in the TOE
FDP_ACF_CIMC.2	None	
FDP_ACF_CIMC.3	None	
FDP_CIMC_BKP.1	FMT_MOF.1	Included
FDP_CIMC_BKP.2	FDP_CIMC_BKP.1	Included
FDP_CIMC_CER.1	None	
FDP_CIMC_CRL.1	None	
FDP_CIMC_CSE.1	None	
FDP_CIMC_OCSP.1	None	
FDP_ETC_CIMC.4	None	
FDP_ITT.1	FDP_ACC.1, orFDP_IFC.1	FDP_ACC.1 Included
FDP_UCT.1	FDP_ACC.1, or FDP_IFC.1	FDP_ACC.1 Included
	FTP_ITC.1, or FTP_TRP.1	Not Included because this product uses basic encryption to ensure basic data exchange confidentiality. It is unnecessary for this product to require Inter-TSF trusted channel or trusted path at this Security Level.
FIA_UAU.1	FIA_UID.1	Included
FIA_UID.1	None	
FIA_USB.1	FIA_ATD.1	Not included because the list of attributes is not configurable
FMT_MOF.1	FMT_SMR.1	Not included because the list of supported roles is not restricted by the TOE
	FMT_SMF.1	Not included but covered by FMT_MOF_CIMC.3, FMT_MOF_CIMC.5 and FMT_MOF_CIMC.6
FMT_MOF_CIMC.3	FMT_MOF.1	Included
	FMT_SMR.1	Not included because the list of supported roles is not restricted by the TOE
FMT_MOF_CIMC.5	FMT_MOF.1	Included
	FMT_SMR.1	Not included because the list of supported roles is not restricted by the TOE
FMT_MOF_CIMC.6	FMT_MOF.1	Included
	FMT_SMR.1	Not included because the list of supported roles is not restricted by the TOE
FMT_MTD_CIMC.4	None	
FMT_MTD_CIMC.5	None	
FMT_MTD_CIMC.6	None	
FPT_CIMC_TSP.1	FAU_GEN.1	Included
	FMT_MOF.1	Included
FPT_ITC.1	None	
FPT_ITT.1	None	
FPT_STM.1	None	

Table 6. Summary of SFR Dependencies for Security Level 2

7. TOE Summary Specifications

7.1. TOE Security Functions

This section describes the security functions provided by the TOE to meet the security functional requirements previously specified.

7.1.1. Security Audit

The OpenTrust PKI manages 2 types of log: system logs and application logs. The system logs are generated by differents system services (os, apache, postgresql, postfix, etc.). Applications logs are generated by the TOE.

The TOE collects audit data for internal actions and user actions and works in conjunction with the IT Environment (via the PostGreSQL Database) to securely record and store this information. When a TOE related security relevant event occurs, the TOE generates the corresponding audit log event in XML fragments. These fragments are stored in the OpenTrust PKI Database.

Logs can be consulted as an expanded display or a compact display via a Web Interface. Several search functionalities are available.

Logs integrity is assured by a digital signature mechanism.

Disk occupation is monitored by the TOE. When the critical threshold is reached, the TOE stops itself to prevent any data loss (in particular, audit data loss)

Time Stamps of audit logs reliability is guaranted by the synchronisation of the TOE with an NTP source.

7.1.2. Roles

The roles definitions are listed below:

- Administrator: role authorized to install, configure, and maintain the CIMC; establish and maintain user accounts; configure profiles and audit parameters; and generate Component keys.
- Operator: role authorized to perform system backup and recovery.
- Officer: role authorized to request and approve certificates or certificate revocations.
- Auditor: role authorized to view and maintain audit logs.

The TOE implements the required roles specified in the PP at the security level 2: Administrator and Officer. The 2 other definitions, Operator and Auditor are agregated to the Administrator role in this target.

7.1.3. Backup and Recovery

The TOE provides command line applications to backup and to restore the following data:

- TOE database content
- logs archives
- configuration files
- pending request data
- confidential data (e.g. private keys for services)

Backup data integrity is assured by a digital signature mechanism.

7.1.4. Access Control

The TOE enforces user roles and access control whenever users access TOE-provided functions. The TOE maintains a secure database of authorized operators, including all identities and permissions.

Access Control is defined by a list of rules composed of the following objects:

- Resource: an element on which an action is performed. This can be a OpenTrust PKI module, a zone/profile association, an OpenTrust PKI certificate, a group, etc.
- Principal: an user or a group to whom rights can be granted on resources.
- Right: a right is used to authorize a principal to perform one or several actions. The right can be limited to a group of resources or type of resources.
- Privilege: a privilege describes the way in which a granted right can be used by an actor. There are 3 types of privileges:
  - the privilege to perform the action(s) associated with right
  - the privilege to grant the right to other actors
  - the privilege to grant other actors the right to grant the right

Access Control Lists allow to restrict the ability to modify the behavior of the security functions to the authorized roles.

7.1.5. Identification and Authentication

Users must be identified and authenticated before to perform any operations except few EE (Enrolment Entity) request and public information retrieval requests (e.g. CRL, CA certificates, OCSP requests). Non authenticated EE requests need to be approved later by an authenticated officer before to be processed by the TOE.

All security-relevant interfaces are made through a mutually authenticated TLS connections. User are required to authenticate themselves with certificates. Operator certificates should be stored in a FIPS140-2 compliant token.

7.1.6. Remote Data Entry and Export

Internal communication between TOE modules are secured by https protocol with mutual authentication.

The TOE relies on HSM mechanisms to protect data exchange between itself and the HSM.

The TOE is responsible for importing and exporting certificates, public keys, certificate status, and other data. The TOE processes certificate requests formatted according to the following standards: PKCS#7, PKCS#10. The TOE generates certificates and CRLs according to the following standard: RFC 3280 Internet X.509 PKI Certificate and CRL Profile. The TOE also complies with the RFC 2560 for OCSP protocol.

The above standards include digital signature mechanism for proof of origin and verification of origin.

7.1.7. Key Management

The TOE uses software and hardware cryptographic service modules for a number of key management functions. In particular, security critical keys (CA private keys, ciphering user private keys) are protected by either encrypting it or storing it within a hardware cryptographic service module. The TOE also relies on the FIPS 140-1 validated cryptographic module mechanisms for the export of the CA private keys.

Digital signatures are used when appropriate to ensure the integrity of key management related information.

User secrets (PIN code, PKCS#12 passphrases, etc.) are either specified by the users or generated by the TOE key management modules. In anycase, the TOE doesn't store those secrets.

A formal key recovery process assures confidentialy of exported user private and secret key. The user private key is exported in a PKCS#12 format and encrypted by a passphrase. This PKCS#12 file is sent to the user. The associated passphrase is sent encrypted to the Officer who has validated the key recovery request. The officer decrypts the passphrase with his private key and communicates it to the user.

7.1.8. Certificate Management

The TOE generates certificates and CRLs according to the following standard: RFC 3280 Internet X.509 PKI Certificate and CRL Profile.

The TOE manages and securely stores all certificates that have been signed using the private key of any of the internal CAs. The TOE provides functionality to issue, suspend, reinstate, reissue, renew, revoke and delete certificates, report status of certificates, and generate CRLs. All these certificate services are provided in a secure manner, protecting the integrity of the certificate administrative

data. Additionally, the TOE enforces proof of origin and verification of origin of certificate status information at all times.

The TOE provides Certificate status by CRL publication and OCSP service. The OCSP responder module complies with the RFC 2560 standard. CRL profile properties are defined within the CA parameters. For the current target version, only one OCSP profile is supported.

The TOE permits Certificate Profile Management. Only Administrators can access to the Certificate Profile Management modules.

7.2. TOE summary specifications rationale

Security Functional Requirements	Security Functions	Rationale
FAU_GEN.1 Audit data generation	Security audit	The OpenTrust PKI manages 2 types of log: system logs and application logs. The system logs are generated by differents system services (os, apache, postgresql, postfix, etc.). Applications logs are generated by the TOE.
FAU_GEN.2 User identity association	Security audit	Each log entry contains user identity information
FAU_SEL.1 Selective audit	Security audit	The TOE provides a Log consultation Web interface
FAU_STG.1 Protected audit trail storage	Security audit	Log entries are signed.
FAU_STG.4 Prevention of audit data loss	Security audit	Disk occupation is monitored by the TOE. When the critical threshold is reached, the TOE stops itself to prevent any data loss (in particular, audit data loss).
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	Remote Data Entry and Export	The TOE complies with the RFC 3280 (for X.509 PKI Certificate and CRL Profile management) and the RFC 2560 (for OCSP protocol).The above standards include digital signature mechanism for proof of origin and verification of origin.
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	Key Management	The TOE relies on software and hardware (FIPS 140-1 Level 3 validated) cryptographic security modules for key destruction zeroization
FDP_ACC.1 Subset access control	Acces Control	Acces Control are managed by Access Control List.
FDP_ACF.1 Security attribute based access control	Acces Control	Acces Control are managed by Access Control List.
FDP_ACF_CIMC.2 User private key confidentiality protection	Key Management	User private key are stored in FIPS 140-1 validated cryptographic module or in encrypted form within the OS File system.
FDP_ACF_CIMC.3 User secret key confidentiality protection	Key Management	The TOE doesn't store any user secrets (PIN code, PKCS#12 passphrases).

Security Functional Requirements	Security Functions	Rationale
FDP_CIMC_BKP.1 CIMC backup and recovery	Backup and Recovery	Command line applications are available
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	Backup and Recovery	Backup data are digitally signed
FDP_CIMC_CER.1 Certificate Generation	Certificate Management	The TOE generates certificates according to the RFC 3280 Internet X.509 standard.
FDP_CIMC_CRL.1 Certificate Revocation	Certificate Management	The TOE generates CRLs according to the RFC 3280 Internet X.509 standard.
FDP_CIMC_CSE.1 Certificate status export	Certificate Management	The TOE provides Certificate status by CRL publication and OCSP service.
FDP_CIMC_OCSP.1 Basic Response Validation	Certificate Management	The TOE OCSP responder module complies with the RFC 2560 standard
FDP_ETC_CIMC.4 User private and secret key export	Key Management	Confidentialy of exported user private and secret key is assured by a formal key recovery process.
FDP_ITT.1 Basic internal transfer protection (iterations 1 and 2)	Remote Data Entry and Export	Internal communication between TOE modules are secured by https protocol with mutual authentication.
FDP_UCT.1 Basic data exchange confidentiality	Remote Data Entry and Export	The TOE relies on HSM mechanisms to protect data exchange between itself and the HSM.
FIA_UAU.1 Timing of authentication	Identification and Authentication	The only functions that do not require identification nor authentication are: • EE requests that need a later approval by an authenticated officer. • public information retrieval such as CRL or OCSP request.
FIA_UID.1 Timing of identification	Identification and Authentication	The only functions that do not require identification nor authentication are: • EE requests that need a later approval by an authenticated officer. • public information retrieval such as CRL or OCSP request.
FIA_USB.1 User-subject binding	Identification and Authentication	User is identified by the DN field of his certificate.
FMT_MOF.1 Management of security function behavior	Roles	Access Control Lists define user or group that can manage security function behavior.
FMT_MOF_CIMC.3 Extended certificate profile management	Certificate Management	The TOE permits Certificate Profile Management.
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	Certificate Management	CRL profile properties are defined within the CA parameters.

Security Functional Requirements	Security Functions	Rationale
FMT_MOF_CIMC.6 OCSP Profile Management	Certificate Management	For the current target version, only one OCSP profile is supported
FMT_MTD_CIMC.4 TSF private key confidentiality protection	Key Management	TSF private key are stored in FIPS 140-1 validated cryptographic module.
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	Key Management	The TOE doesn't use any TSF secret key.
FMT_MTD_CIMC.6 TSF private and secret key export	Key Management	The TOE relies on the key export mechanisms provided by the FIPS 140-1 validated cryptographic module
FPT_CIMC_TSP.1 Audit log signing event	Security audit	Log entries are signed.
FPT_ITC.1 Inter-TSF confidentiality during transmission	Remote Data Entry and Export	The TOE relies on HSM mechanisms to protect data exchange between itself and the HSM.
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 1 and 2)	Remote Data Entry and Export	Internal communication between TOE modules are secured by https protocol with mutual authentication.
FPT_STM.1 Reliable time stamps	Security audit	The TOE requires a NTP synchronization.

Table 7. Security Functions Rationale

8. Access Control Policies

8.1. 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:

a. Identity of the subject requesting access,

b. Role (or roles) the subject is authorized to assume,

c. Type of access requested,

d. Content of the access request, and,

e. 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.

8.2. 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:

a. Identity of the subject requesting access,

b. Role (or roles) the subject is authorized to assume,

c. Type of access requested,

d. Content of the access request, and,

e. 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

9. Glossary of terms

The following definitions are used throughout this document:

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

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

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

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

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

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

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

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

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

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

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

Enrollment (Certificate):
Digital Certificates are normally allocated by a trusted body known as a CA (Certification Authority). When a party or entity is allocated a certificate it is described as certificate enrolment. This process involves the party requesting a certificate providing the CA with a copy of its public key and additional identity information. Once validated by an EE (Enrollment Entity), this information in turn is signed by the CA. This involves the CA encrypting this information with its private key. The certificate is returned to the requesting party, which has now been enrolled.

Enrollment Entity (EE):
An Enrollment Entity (EE) is a trusted entity in charge of validating certificate enrollment request, in particular the provided identity information.

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

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

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

Firmware:
the programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution.

Hardware:
the physical equipment used to process programs and data in a CIMC.

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

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

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

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

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

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

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

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

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

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

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

Secret key:
a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public.

The use of the term "secret" in this context does not imply a classification level rather the term implies the need to protect the key from disclosure or substitution.

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

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

SLES (SUSE Linux Enterprise Server):
a server-oriented Linux distribution supplied by Novell, Inc. and targeted at the business market.

Software:
the programs and associated data that can be dynamically written and modified. Split knowledge: a condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

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

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

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

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

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

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

