Date: March, 28th 2011

Issued by: DES/SEC/Trusty

File: *TRUSTYKEY V6*

Title: # SECURITY TARGET TRUSTYKEY 6

Reference: CSSI/HLS/TRUSTY/ENG/08/0128 rev 7.1

Status: ***APPROVED***

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

TABLE OF CONTENTS

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

References

[CC]	Common Criteria for Information Technology Security Evaluation, version 3.1 revision 2 - Part 1: Introduction and general model, ref. CCMB-2006-09-001 - Part 2: Security functional requirements, ref. CCMB-2007-09-002 - Part 3: Security assurance requirements, ref. CCMB-2007-09-003
[PP CIMC]	Certificate Issuing and Management Components, Family of Protection profiles, version 1.0

Terms and acronyms

CC	Common Criteria [CC]
OSP	Organizational Security Policy
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functions

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

1. INTRODUCTION

1.1. ST IDENTIFICATION

Title	Security Target TrustyKey 6: CSSI/HLS/TRUSTY/ENG/08/0128
Version	7.1
Author(s)	VERGNES Stephane
Date	March 28st 2011

1.2. TOE IDENTIFICATION

Developer	CS Communication & Systèmes
Product name	TrustyKey
Version	6.0.14

1.3. TOE OVERVIEW

1.3.1. TOE type

TrustyKey V6 is a software program that forms part of a Public Key Infrastructure (PKI).

1.3.2. TOE usage and major security features

A PKI is a set of hardware devices, software programs, procedures and persons that manage the life cycle of digital certificates. The certificate owners use them to ensure security functions such as authentication, integrity, non-repudiation and confidentiality.

TrustyKey V6 is a flexible PKI product that provides the operational and administration services to manage the certificates of any organisation type.

TrustyKey V6 is composed of a main and mandatory TrustyKey CA component that manages the certification authorities, collects and processes the certification issuance and revocation requests, and publishes the certificate status.

Optional components can be deployed to provides additional services:

- A registration authority (RA) application to be used by enrollment operators
- A pre-initialization center (PIC) that is able to generate user encryption keys on user tokens.
- A recovery center (RC) that ensures secure storage and recovery of user private encryption keys.

CS proposes these applications as TrustyKey V6 additional components. As standard interfaces are used between all these components (CMP, PKCS formats), an organization can choose to deploy TrustyKey V6 with its own additional products, such as a Card Management System (CMS) as registration authority.

The TOE of this Security Target is TrustyKey, restricted to the main CA component.

1.3.2.1. Services offered by the TOE

Certificate issuance: a registration authority submits certificate requests to TrustyKey CA. TrustyKey CA subsequently allows such certificates to be renewed.

Certificate revocation: If a secret key is compromised or user status changes, a registration authority can send a certificate revocation request to TrustyKey CA. TrustyKey CA generates certificate revocation lists at regular intervals or immediately after a revocation operation is performed.

Certificate and Revocation List publication: TrustyKey CA publishes revocation lists and some of the certificates in one or more repositories that can be accessed by users. These repositories may be directories or file systems.

Certificate status export: TrustyKey CA exports the certificate status through a dedicated OCSP interface.

1.3.2.2. Services required for correct operation of the TOE

Certificate generation: TrustyKey CA generates and signs certificates.

Certificate Revocation List generation: TrustyKey CA generates and signs certificate revocation lists (CRL and ARL).

Administration:

- Authority management: TrustyKey CA allows the Certification Authorities to be declared and their certificates managed (generated, renewed, revoked).
- operator management: TrustyKey CA allows operators and the associated profiles to be managed (created, edited, deleted).
- Profile management: TrustyKey CA generate the certificates according to certificate generation profile managed by operators, and CRL according to revocation list generation profiles.
- Function configuration: TrustyKey CA can be adapted to meet the needs of many different types of organizations. To allow this, operators can configure environment settings and security functions (especially publication functions).

Supervision: TrustyKey CA records all security sensitive actions and provides a supervision interface to consult recorded audit.

1.3.3. Roles

This security target uses security functional requirement from the CIMC Protection profile; these requirements make reference to a set of roles described in §1.3.3.1.

These roles are implemented in TrustyKey with its own nameset, described in §1.3.3.2.

The correspondence between the two sets can be found in §1.3.3.3.

1.3.3.1. CIMC roles

- **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 or approve certificates or certificate revocations.
- **Auditor** – role authorized to view and maintain audit logs.

Notes :

- The term “user” is used for any individual interacting with the TOE;
- An “authorized user” is a user interacting with the TOE in conformance with its role;
- the role “Operator” will be described, in this document, as operator[CIMC] to avoid confusion with the notion of TrustyKey operators (see section below).

1.3.3.2. TrustyKey roles

The TOE provides a certification service for users that may be persons or IT systems. All users possess a certificate issued by the TOE.

operators are the personnel who use the services provided by the TOE. They are the only people who interact directly with the TOE, within the limit of the rights assigned to them. They perform administration and supervision tasks.

The **system engineer** is responsible for start-up, configuration and technical maintenance of the platform on which the TOE is installed.

The **Registration Authority** is the application (IT system) that request certificate issuance and revocation.

The **final users** are end-entity users that request certificate status.

1.3.3.3. Correspondence between roles

The TrustyKey roles cover the CIMC roles as follows:

- CIMC Administrator tasks are performed either by:
  - A system engineer for the operations related to environment and installation
  - A TrustyKey operator for other tasks. Such an operator is granted all TrustyKey rights except the audit consultation right.
- CIMC Operator[CIMC] tasks are performed either by a system engineer
- CIMC Officer tasks are performed by the Registration Authority (request and revoke final user certificates)
- CIMC Auditor tasks are performed by a TrustyKey operator who is only granted the right to consult the audit logs in TrustyKey

The correspondence is summarized in the following table:

Required CIMC role	Function	Required TrustyKey role	Required TrustyKey additional rights
Administrator	install the CIMC configure the CIMC (system configuration) maintain the CIMC	System engineer	-
Administrator	configure the CIMC (Functional configuration) maintain user accounts configure profiles configure audit parameters (not applicable as audit is not configurable generate Component keys	Operator	Declare a root authority Declare a child authority Configure an authority Request an authority certificate Import an authority certificate Generate an authority certificate Revoke sub-authority certificates Revoke certificates signed by an authority Manage publication repositories Declare revocation of an authority certificate Manage operators Manage operator profiles Manage CGPs and RGPs Request a server certificate Import a server certificate Manage RA, PIC and RC certificates Generate a technical certificate Revoke a technical certificate Publish certificates Publish revocation lists
operator[CIMC]	perform system	System engineer	-

	backup and recovery		
Officer	request user certificates or user certificate revocations	Registration authority	-
Auditor	view and maintain audit logs	operator	View audit log
-	Request certificates status	Final users	-

1.3.4. Required non-TOE hardware/software/firmware

For the evaluation, the TOE is installed on the following platform:

- operator station:
  - OS: Windows XP SP3 (32 bits)
  - Java: Java JRE 1.5.0.19
  - Browser: Internet Explorer 8
  - Smartcard Reader: Omnikey Cardman 3821
  - Smartcard Reader driver: Omnikey 1.1.2.4
  - Smartcard Middleware: AuthentIC Web Pack 4.4
- Root CA server:
  - OS: Windows Server 2003
  - Java: Java JRE 1.5.0.19
  - Database: Oracle 10g
  - HSM: Safenet Luna CA4
  - Browser: Internet Explorer 8
  - Smartcard Reader: Omnikey Cardman 3821
  - Smartcard Reader driver: Omnikey 1.1.2.4
  - Smartcard Middleware: AuthentIC Web Pack 4.4
- CA server:
  - OS: Windows Server 2003
  - Java: Java JRE 1.5.0.19
  - Database: Oracle 10g
  - HSM: Safenet Luna SA
  - Browser: Internet Explorer 8
  - Smartcard Reader: Omnikey Cardman 3821
  - Smartcard Reader driver: Omnikey 1.1.2.4
  - Smartcard Middleware: AuthentIC Web Pack 4.4
- LDAP directory
  - OS: Fedora Core 9
  - OpenLDAP 2.4
- Smartcard
  - AuthentIC ID-One Cosmo v5.4

The TOE also requires an XML file editing application to edit the XML files required for operation of the TOE (CGP: Certificate Generation Profile, RGP: Revocation (list) Generation Profile).

1.4. TOE DESCRIPTION

The TOE is composed of software programs allowing the services described above to be provided.

- TrustyKey CA server applications
  - TrustyKey CA CMP services application
  - TrustyKey CA OCSP responder application
  - TrustyKey CA Administration application
- TrustyKey CA applet executed on TrustyKey CA operator station

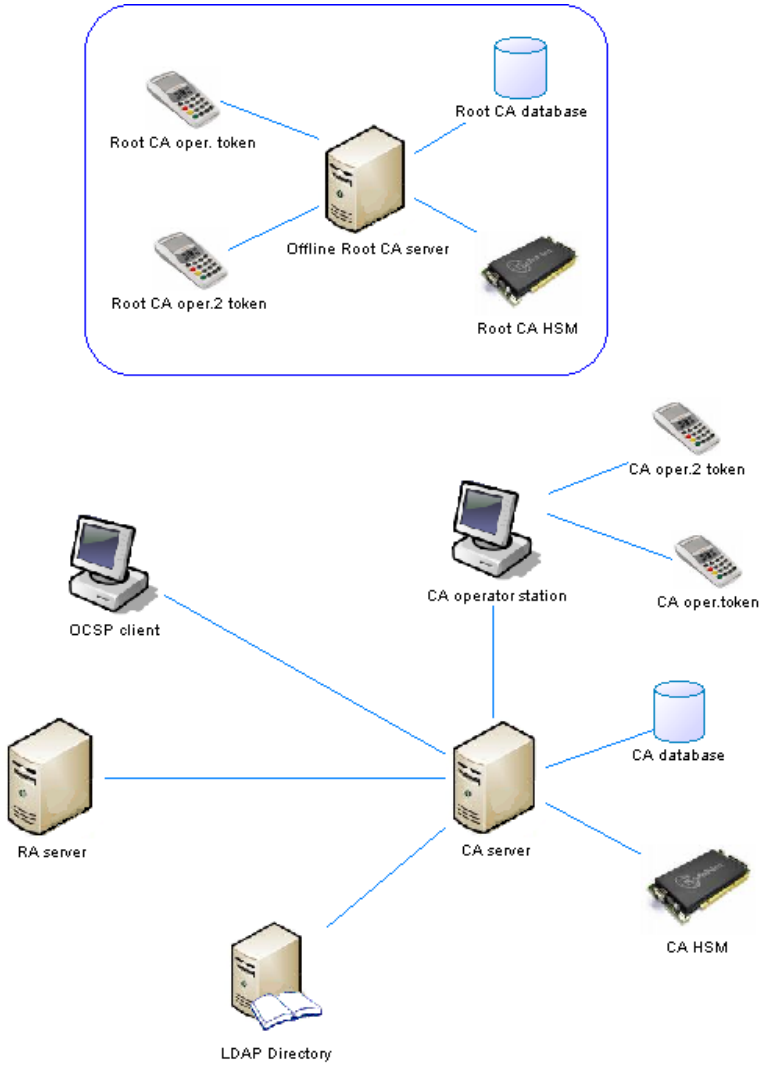

Figure 1 Evaluated architecture

The operating systems, databases and directories used by the TOE are not included in the scope of evaluation.

The hardware components required for operation of the TOE (HSM, tokens, token readers,) are not included in the scope of evaluation.

The XML policy file editing application is not included in the scope of evaluation.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

2. CONFORMANCE CLAIMS

2.1. CC CONFORMANCE

This security target is compliant with the Common Criteria version 3.1 revision 2 [CC].

The security functional requirements are compliant with the extended CC Part 2.

The security assurance requirements are strictly compliant with the CC Part 3.

2.2. PROTECTION PROFILES CONFORMANCE

This security target does not claim any compliance with any protection profile but the majority of requirements are extracted from the CIMC protection profile Level 2 [PP-CIMC].

2.3. PACKAGE CONFORMANCE

The evaluation level claimed in this security target is the package EAL3 augmented with ALC_FLR.3.

2.4. CONFORMANCE RATIONALE

This security target does not claim any compliance with any protection profile.

3. SECURITY PROBLEM DEFINITION

This section identifies the security aspects of the environment in which the TOE is operated.

3.1. ASSUMPTIONS

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, operator[CIMC]s, Officers and Auditors

Competent Administrators, operator[CIMC]s, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

A.CPS

All Administrators, operator[CIMC]s, 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, operator[CIMC]s, 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, operator[CIMC]s, 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, operator[CIMC]s, Officers and Auditors

Administrators, Operators, [CIMC]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 identified in this security target.

3.1.3. Physical

A.Communications Protection

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

A.Physical Protection

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

3.2. THREATS

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

3.2.1. Authorized Users

T.Administrative errors of omission

Administrators, operator[CIMC]s, 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, operator[CIMC]s, Officers and Auditors commit errors

An Administrator, operator[CIMC], 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.

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

OT.Certificates

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

OT.Restrict actions before authentication

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

OT.Limitation of administrative access

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

OT.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.

4.1.2. System

OT.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.

OT.Sufficient backup storage and effective restoration

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

OT.Integrity protection of user data

Provide appropriate integrity protection for user data.

OT.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.

OT.Manage behavior of security functions

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

OT.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.

OT.Protect stored audit records

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

OT.Protect user and TSF data during internal transfer

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

OT.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.

OT.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.

4.1.3. External Attacks

OT.Control unknown source communication traffic

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

OT.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.

4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

4.2.1. Non-IT security objectives for the environment

OE.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.

OE.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.)

OE.Communications Protection

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

OE.Competent Administrators, operator[CIMC]s, Officers and Auditors

Provide capable management of the TOE by assigning competent Administrators, operator[CIMC]s, Officers and Auditors to manage the TOE and the security of the information it contains.

OE.CPS

All Administrators, operator[CIMC]s, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.

OE.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).

OE.Installation

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

OE.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.

OE.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.

OE.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.

OE.Social Engineering Training

Provide training for general users, Administrators, operator[CIMC]s, Officers and Auditors in techniques to thwart social engineering attacks.

OE.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.

OE.No Abusive Administrators, operator[CIMC]s, Officers and Auditors

Use trustworthy Administrators, operator[CIMC]s, Officers and Auditors.

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

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

OE.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.

OE.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.

OE.Require inspection for downloads

Require inspection of downloads/transfers.

OE.Prevent malicious code

Incorporate malicious code prevention mechanisms.

OE.Procedures for preventing malicious code

Incorporate malicious code prevention procedures.

OE.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.

OE.User authorization management

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

4.2.2. IT security objectives for the environment

OE.Cryptographic functions

Cryptographic algorithms used for encryption/decryption, authentication, signature generation/verification and key generation techniques must be approved and used cryptographic modules must be validated. (Validated is defined as FIPS 140-1 validated.)

OE.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.

OE.Periodically check integrity

Provide periodic integrity checks on both system and software.

OE.Security roles

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

OE.Validation of security function

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

OE.Time stamps

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

4.3. SECURITY OBJECTIVES RATIONALE

Threats coverage

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

OE.CPS provides Administrators, operator[CIMC]s, Officers, and Auditors with information regarding the policies and practices used by the system. Providing this information ensures that these authorized users of the system are aware of their responsibilities, thus reducing the likelihood that they will fail to perform a security-critical operation.

OT.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. These audit records will expose administrators that fail to perform security-critical operations so they can be held accountable.

OT.Security-relevant configuration management ensures that system security policy data and enforcement functions, and other security-relevant configuration data are managed and updated.

This ensures that they are consistent with organizational security policies and that all changes are properly tracked and implemented.

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

It is countered by:

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

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

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

- User misunderstands a system command and issues a command that unintentionally deletes user data.

It is countered by:

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

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

T.Critical system component fails addresses the failure of one or more system components that results in the loss of system-critical functionality. This threat is relevant when there are components that may fail due to hardware and/or software imperfections and the availability of system functionality is important.

It is countered by:

OE.Configuration management assures that a configuration management program is implemented. The configuration management program includes configuration identification and change control. This ensures that critical system components do not fail as a result of improper configuration.

OE.Installation ensures that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security. This ensures that critical system components do not fail as a result of improper installation.

OT.Manage behavior of security functions provides management controls/functions for security mechanisms. This ensures that critical system components do not fail as a result of improper configuration of security mechanisms.

OT.Preservation/trusted recovery of secure state ensures that the system remains in a secure state throughout operation in the presence of failures and subsequent system recovery. This objective is relevant when system failures could result in insecure states that, when the system returns to operational mode (or continues to operate), could lead to security compromises.

OT.Sufficient backup storage and effective restoration ensures that there is sufficient backup storage and effective restoration to recreate the system, when required. This ensures that data is available from backup, even if the current copy is lost through failure of a system component (e.g., a disk drive).

OE.Time stamps provides time stamps to ensure that the sequencing of events can be verified. If the system must be reconstructed, it may be necessary to establish the order in which transactions were performed to return the system to a state consistent with the state when a critical component failed.

T.Malicious code exploitation addresses the threat where an authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. The execution of malicious code is done through a triggering event.

It is countered by:

OE.Configuration management assures that a configuration management program is implemented. The configuration management program includes configuration identification and change control. This ensures that malicious code is not introduced during the configuration process.

OT.Integrity protection of user data ensures that appropriate integrity protection is provided for user data. This prevents malicious code from attaching itself to user data.

OT.Object and data recovery free from malicious code ensures that the system recovers to a viable state after malicious code has been introduced and damage has occurred. The malicious code, e.g., virus or worm, is removed as part of the process.

OE.Periodically check integrity ensures that periodic integrity checks are performed on both system and software. If these checks fail, malicious code may have been introduced into the system.

OE.Prevent malicious code provides a set of mechanisms that work to prevent incorporation of malicious code into the system.

OE.Procedures for preventing malicious code provides a set of procedures that work to prevent incorporation of malicious code into the system.

OE.Require inspection for downloads ensures that software that is downloaded/transferred is inspected prior to being made operational.

OE.Validation of security function. Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures such as underlying machine testing and integrity checks.

T.Message content modification addresses the situation where a hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient. Several kinds of modification are possible: modification of a single message, deletion or reordering of selected messages, insertion of bogus messages, replay of previous messages, and modification of accompanying message security attributes.

It is countered by:

OT.Data Import/Export protects data when being transmitted to or from the TOE. Protection of data in transit permits the TOE or the external user to detect modified messages, message replay, or fraudulent messages.

OT.Protect user and TSF data during internal transfer protects data being transmitted between separated parts of the TOE. Protection of data in transit permits the TOE to detect modified messages, message replay, or fraudulent messages.

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

It is countered by:

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

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

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

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

It is countered by:

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

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

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

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

T.Hacker gains access addresses:

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

It is countered by:

OT.Restrict actions before authentication ensures that only a limited set of actions may be performed before a user is authenticated. This prevents a hacker who is unable to circumvent the access control mechanisms from performing security-relevant operations.

OT.Control unknown source communication traffic ensures that communication traffic from an unknown source is controlled (e.g., rerouted or discarded) to prevent potential damage. Various kinds of hacker attacks can be detected or prevented by rerouting or discarding suspected hacker traffic.

OT.Individual accountability and audit records provides individual accountability for audited events. Each user is uniquely identified so that auditable actions can be traced to a user. Audit records provide information about past user behavior to an authorized individual through system mechanisms. This allows for the detection of unauthorized activity. Once detected, the damage resulting from such activity can be eliminated or mitigated.

OE.Notify Authorities of Security Issues ensures that proper authorities are notified regarding any security issues that impact their systems. This minimizes the potential for the loss or compromise of data.

OE.React to detected attacks ensures that automated notification or other reactions to the TSF discovered attacks is implemented in an effort to identify attacks and to create an attack deterrent.

This objective is relevant if actions that the organization deems essential also pose a potential attack that could be exploited.

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

It is countered by:

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

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

It is countered by:

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

OE.Social Engineering Training which ensures that general users, Administrators, operator[CIMC]s, Officers, and Auditors are trained in techniques to thwart social engineering attacks.

T.Administrators, operator[CIMC]s, Officers and Auditors commit errors addresses errors committed by administrative personnel that directly compromise organizational security objectives, change the technical security policy enforced by the system or application.

It is countered by:

OE.Competent Administrators, operator[CIMC]s, Officers and Auditors ensures that users are capable of maintaining effective security practices. This reduces the likelihood that they will commit errors.

OT.Certificates ensures that certificates, certificate revocation lists, and certificate status information are valid. The validation of information provided by Officers that is to be included in certificates helps to prevent improperly entered information from appearing in certificates.

OT.Maintain user attributes. Maintains a set of security attributes (which may include group membership, access rights, etc.) associated with individual users in addition to user identity. This prevents users from accidentally performing operations that they are not authorized to perform.

OT.Respond to possible loss of stored audit records ensures that only auditable events executed by the Auditor shall be audited if the audit trail is full. This ensures that operations that are performed in error by users other than the Auditor are audited and so can be detected.

OE.Respond to possible loss of stored audit records ensures that only auditable events executed by the Auditor shall be audited if the audit trail is full. This ensures that operations that are performed in error by users other than the Auditor are audited and so can be detected.

OE.Security roles ensures that security-relevant roles are specified and that users are assigned to one (or more) of the defined roles. This prevents users from accidentally performing operations that they are not authorized to perform.

OSP coverage

P.Authorized use of information establishes that information is used only for its authorized purpose(s).

This is addressed by the following objectives: **OT.Maintain user attributes**, **OT.Restrict actions before authentication**, **OE.Security roles**, and **OE.User authorization management**. **OT.Restrict actions before authentication** ensures that the capability to perform security-relevant operations is limited to those who have been authorized to perform those operations. **OT.Maintain user attributes**, **OE.Security roles**, and **OE.User authorization management** ensure that users are only authorized to perform those operations that are necessary to perform their jobs. Finally, **OE.Auditors review audit logs** deters users from misusing the authorizations they have been provided.

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

Assumption coverage

A.Auditors Review Audit Logs establishes that audit logs are necessary for security-relevant events and that they must be reviewed by auditors. This is addressed by **OE.Auditors Review Audit Logs**, which ensures that security-relevant events recorded in audit logs are reviewed by auditors.

A.Authentication Data Management establishes that management of user authentication data is external to the TOE. This is addressed by **OE.Authentication Data Management**, which ensures that users modify their authentication data in accordance with appropriate security policy.

A.Competent Administrators, operator[CIMC]s, Officers and Auditors establishes that security of the TOE is dependent upon those that manage it. This is addressed by **OE.Competent Administrators, operator[CIMC]s, Officers and Auditors**, which ensures that the system managers will be competent in its administration.

A.CPS establishes that Administrators, operator[CIMC]s, Officers, and Auditors are familiar with the CP and CPS under which the TOE is operated. This is addressed by **OE.CPS,** which ensures that Administrators, operator[CIMC]s, Officers, and Auditors are familiar with the CP and CPS under which the TOE is operated.

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

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

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

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

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

A.Communications Protection establishes that the communications infrastructure is outside the TOE.

This is addressed by **OE.Communications Protection**, which ensures that adequate physical protections are afforded the necessary communications infrastructure.

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

A.Cooperative Users establishes that a secure IT environment is required to securely operate the TOE, and that users must work within the constraints of that environment. This is addressed by **OE.Cooperative Users**, which ensures that users will cooperate with the constraints established.

A.No Abusive Administrators, operator[CIMC]s, Officers and Auditors establishes that administrators, operator[CIMC]s, officers, and auditors have a great deal of authority. This is addressed by **OE.No Abusive Administrators, operator[CIMC]s, Officers and Auditors**, which ensures that individuals hired to be administrators, operator[CIMC]s, officers, and auditors are deemed to be trustworthy.

5. SECURITY REQUIREMENTS

5.1. EXTENDED COMPONENTS DEFINITION

Extended components are defined in section 7.3 of the document.

5.2. SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

The list of subject/operation/object required by the CC v3.1 is the list of roles and function as defined in §1.3.3.3.

Table 1 List of SFRs

Requirements		Titles	CC Part 2 extended
Audit			
	FAU_GEN.1	Audit data generation	
	FAU_GEN.2	User identity association	
	FAU_SEL.1	Selective audit	
	FAU_STG.1	Protected audit trail storage	
	FAU_STG.4	Prevention of audit data loss	
	FPT_CIMC_TSP.1	Audit log signing event	Yes
Roles			
	FMT_SMR.1	Security roles	
	FMT_MOF.1	Management of security functions behavior	
Access Control			
	FDP_ACC.1	Subset access control	
	FDP_ACF.1	Security attribute based access control	
Identification and authentication			
	FIA_UAU.1	Timing of authentication	
	FIA_UID.1	Timing of identification	
	FIA_USB.1	User-subject binding	
Remote Data Entry and Export			
	FCO_NRO_CIMC.3	Enforced proof of origin and verification of origin	Yes
	FDT_ITT.1 (user data integrity)	Basic internal transfer protection	
	FDT_ITT.1 (user data confidentiality)	Basic internal transfer protection	
	FPT_ITT.1 (internal data integrity)	Basic internal TSF data transfer protection	
	FPT_ITT.1 (internal data confidentiality)	Basic internal TSF data transfer protection	

	FPT_ITC.1	Inter-TSF confidentiality during transmission	
Certificate Status Export			
	FDP_CIMC_CSE.1	Certificate status export	Yes
Key Management (Private Key Storage)			
	FMT_MTD_CIMC.4	TSF private key confidentiality protection	Yes
Key Management (Public Key Storage)			
	FDP_SDI_CIMC.3	Stored public key integrity monitoring and action	Yes
Key Management (Secret Key Storage)			
	FMT_MTD_CIMC.5	TSF secret key confidentiality protection	Yes
Certificate Profile Management			
	FMT_MOF_CIMC.3	Extended certificate profile management	Yes
Certificate Revocation List Management			
	FMT_MOF_CIMC.5	Extended certificate revocation list profile management	Yes
Online Certificate Status Protocol (OCSP) Management			
	FMT_MOF_CIMC.6	OCSP profile management	Yes
Certificate Generation			
	FDP_CIMC_CER.1	Certificate Generation	Yes
Certificate Revocation			
	FDP_CIMC_CRL.1	Certificate revocation list validation	Yes
	FDP_CIMC_OCSP.1	OCSP basic response validation	Yes
Backup and Recovery			
	FDP_CIMC_BKP.1	CIMC backup and recovery	Yes
	FDP_CIMC_BKP.2	Extended CIMC backup and recovery	Yes

Conventions:

- SFR description extracted from CIMC profile is written with standard characters: requirement
- Assignments and selections are surrounded with brackets: [assignment] and [selection]
- Iterations on a requirement are specified using parenthesis: SFR (iteration description)
- Refinements are written with italic characters: *refinement*
- Notes are highlighted as follows: NOTE: additional details

5.2.1. 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: TrustyKey CA events 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, [the information specified in the Additional Details column in Table 2: TrustyKey CA events below.]

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

Dependencies: FPT_STM.1 Reliable time stamps

Events audited by TrustyKey CA

Authority Administration		
Event	**Main details data**	**Other details data**
Root authority declaration	Authority name	Authority DN, Authority Type, Co-signer
Sub-authority declaration	Authority name	Parent authority name, Authority DN, Authority type, Co-signer
Configure the remote authority	Authority name	List of operators, Co-signer
Configure the local authority	Authority name	CRL profile, ARL profile, CRL generation delay after revocation, Certificate publication periodicity,CRL publication periodicity, CRL validity duration, operators list, Co-signer
Authority certificate request	Authority name	Certificate usage, Key pair algorithm and parameters, Co-signer
Authority certificate generation	Authority name	Sub authority DN, Certificate Serial Number, CGP Profile, Co-signer
Authority certificate import	Authority name	Certificate Serial number, Certificate usage
Sub-authority certificate revocation	Authority name	Revoked authority name, Revoked authority DN, Revoked certificate serial number, Revocation reason, Co-signer
Revocation of certificates signed by an authority	Authority name	Revocation reason, Serial number, Co-signer
Declaration of authority certificate revocation	Authority name	Certificate Serial number, Revocation reason
Certificate publication	Authority name	Publication types, Include of sub-authorities flag,

		Republication flag
Revocation lists publication	Authority name	Publication type, Include sub-authorities flag, CRL generation flag
PKI server certificate importation	Authority name	Server type, Serial number, Issuer DN, Subject DN
PKI server certificate removal	Authority name	Server type, Serial number, Issuer DN, Subject DN
Technical certificate generation	Authority name	Subject DN, Serial number, CGP Profile
Technical certificate revocation	Authority name	Subject DN, Serial number, Revocation reason, Type of token

operator Profile Administration		
Event	**Main details data**	**Other details data**
operator profile creation	Profile name	Rigths
operator profile modification	Profile name	Rigths
operator profile removal	Profile name	

operator Administration		
Event	**Main details data**	**Other details data**
Authenticate	operator name	operator DN, Cert Serial number, Cert Issuer DN
Logout	operator name	operator DN
operator creation	operator name	operator DN, operator profile name
operator token creation	operator name	Type of token, Serial Number, Expiration date
operator modification	operator name	operator DN, operator Profile name
operator removal	operator name	operator DN, operator Profile name
operator token revocation	operator name	Token serial number, Revocation reason

Server Administration		
Event	**Main details data**	**Other details data**
Repository creation (File system)	Repository name	Publication path
Repository creation (LDAP)	Repository name	LDAP directory URL
Repository modification	Repository name	New Publication path, New LDAP directory URL
Repository removal	Repository name	
Server certificate request	Server Certificate usage	Subject DN, Key pair algorithm and parameters
Server certificate importation	Server Certificate usage	Issuer DN, Serial number, Subject DN
CGP creation	CGP Profile name	
RGP creation	RGP Profile name	
CGP modification	CGP Profile name	Profile version

RGP modification	RGP Profile name	Profile version
CGP removal	CGP Profile name	Profile version
RGP removal	RGP Profile name	Profile version

Certificate Services		
Event	**Main details data**	**Other details data**
Certificate generation	Authority name	Subject DN, Serial Number, CGP Profile name, CGP Profile version
Certificate confirmation	Authority name	Subject DN, Serial Number, acceptance
Certificate revocation	Authority name	Subject DN, Serial Number, Revocation reason
Certificate publication	Authority name	Publication types
CRL generation and publication	Authority name	CRL type, CRL number, number of certificates
Revocation of unconfirmed certificates	Authority name	Holder DN, Serial number Revocation reason

Launcher functions		
Event	**Main details data**	**Other details data**
Start application	Application name	Application version
Stop application	Application name	Application version

Table 2: TrustyKey CA events

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 [3.1rev2 : The TSF shall be able to select the set of audited events from the set of all auditable events based on the following attributes] [3.1 rev3 : The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:] attributes:

a) [event type]

b) [event date, user identity].

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 action], if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

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 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

5.2.2. Roles

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [defined in §1.3.3].

FMT_SMR.1.2 The TSF shall be able to associate users with 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 authorized roles as specified in table Table 3].

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of management functions

function	behaviour configuration	authorized to	With additional right
Audit	None		
Roles	None		
Backup and Recovery	None		
Access Control	Capability to create operators and modify operator rights	Operator	Manage operators Manage operator profiles
Identification and authentication	None		
Remote Data Entry and Export	Capability to add or remove authorized Registration Authorities	Operator	Manage RA, PIC and RC certificates
Certificate Status Export	Capability to configure the revocation list generation policy	Operator	Configure authority
Key Management (Private Key Storage)	None		
Key Management (Public Key Storage)	None		
Key Management (Secret Key Storage)	None		
Key Management (Private and Secret Key Destruction)	None		
Certificate Profile Management	None		
Certificate Revocation List Management	None		
Online Certificate Status Protocol (OCSP) Management	None		

function	behaviour configuration	authorized to	With additional right
Certificate Generation	Capability to create and modify CGPs	Operator	Manage CGPs and RGPs
Certificate Revocation	Capability to create and modify RGPs	Operator	Manage CGPs and RGPs

Table 3: Security function configuration management roles

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

5.2.3. 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 §7.1] on [operations, profiles and certification authorities data].

Dependencies: FDP_ACF.1 Security attribute based access control

Refinement: the resources controlled are:

- *Access to TrustyKey CA functions.*
- *The certification authorities that can be administered by an operator on TrustyKey CA.*

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [Access Control Policy specified in §7.1] to objects based on the following: [identity of the subject and the set of roles that the subject is authorized to assume].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules specified in§7.1.1.3, §7.1.2, §7.1.3]

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 following additional rules : [no additional rules].

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

5.2.4. Identification and Authentication

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [access to public information (CRLs, OCSP)] 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 [access to public information (CRLs, OCSP)] 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 the behalf of that user: [user roles].

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: [see §1.3.3.3 for the specification of roles].

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: [roles are not manageable].

Dependencies: FIA_ATD.1 User attribute definition

5.2.5. Remote data entry and export

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

Hierarchical to: FCO_NRO.2

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

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity and [the certificate] 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

Refinement: the following are concerned:

- *operator request signature.*
- *CA/RA online exchanges.*

FDP_ITT.1 (user data integrity) Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the [CIMC TOE Access Control Policy specified in section 7.2.1] to prevent the [modification] of 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]

Refinement: this concerns integrity protection of user data exchanges between the CA server and CA applet.

FDP_ITT.1 (user data confidentiality) Basic internal transfer protection

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the [CIMC TOE Access Control Policy specified in section 7.2.1] to prevent the [disclosure] of 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]

Refinement: this concerns the confidentiality protection of user data exchanges between the CA server and CA applet.

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

Hierarchical to: No other components.

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

Dependencies: No dependencies

Refinement: this concerns integrity protection of internal data exchanged between the CA server and CA applet.

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

Hierarchical to: No other components.

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

Dependencies: No dependencies

Refinement: this concerns confidentiality protection of internal data exchanged between the CA server and CA applet.

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

Refinement: this concerns confidentiality protection of internal data exchanged between CA server and operator stations.

5.2.6. Certificate status export

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 and the OCSP standard as defined by RFC 2560].

Dependencies: No dependencies

5.2.7. Key Management (Private Key Storage)

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

Refinement: this concerns the confidentiality protection of CA private keys.

5.2.8. Key Management (Public Key Storage)

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

Hierarchical to: No other components

FDP_SDI_CIMC.3.1 Public keys stored within the CIMC, but not within a FIPS 140-1 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_CIMC.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall [prevent use of that public key and generate an auditable event].

Dependencies: No dependencies

Refinement: this concerns the integrity protection of the public keys stored by the CA.

5.2.9. Key Management (Secret Key Storage)

NOTE: the term secret key is used to mean user secret data (token secret code).

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

5.2.10. Certificate Profile Management

FMT_MOF_CIMC.3 Extended certificate profile management

Hierarchical to: FMT_MOF_CIMC.2

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

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

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

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

- keyUsage;
- basicConstraints;
- certificatePolicies

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

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

Refinement: For this requirement, the CIMC Administrator role is performed by a TrustyKey operator as defined in §1.3.3.

5.2.11. Certificate Revocation List Management

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: FMT_MOF_CIMC.4

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

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

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

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

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

Refinement: For this requirement, the CIMC Administrator role is performed by a TrustyKey operator as defined in §1.3.3.

5.2.12. Online Certificate Status Protocol (OCSP) Management

FMT_MOF_CIMC.6 OCSP profile management

Hierarchical to: No other components.

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

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

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

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

Refinement: For this requirement, the CIMC Administrator role is performed by a TrustyKey operator as defined in §1.3.3.

5.2.13. Certificate Generation

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.

5.2.14. Certificate Revocation

FDP_CIMC_CRL.1 Certificate revocation list validation

Hierarchical to: No other components.

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

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

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:

- The version field shall contain a 0.
- If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical issuerAltName extension.
- The signatureAlgorithm field shall contain the OID for a FIPS-approved digital signature algorithm.
- The thisUpdate field shall indicate the time at which the status being indicated is known to be correct.
- The producedAt field shall indicate the time at which the OCSP responder signed the response.

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

Dependencies: No dependencies

5.2.15. 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

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 OT.Object and data recovery free from malicious code and OT.Preservation/trusted recovery of secure state.

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

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 OT.Object and data recovery free from malicious code and OT.Preservation/trusted recovery of secure state.

5.3. SECURITY ASSURANCE REQUIREMENTS (SARS)

The target level is **EAL3 augmented with the ALC_FLR.3** components.

Table 4 Summary of Security Assurance Requirements

Requirements		Title
ADV : Development		
	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD : Guidance documents		
	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC : Life-cycle support		
	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.3	Systematic flaw remediation
ASE : Security Target evaluation		
	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE : Tests		
	ATE_FUN.1	Functional testing
	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_IND.2	Independent testing - sample
AVA : Vulnerability assessment		
	AVA_VAN.2	Vulnerability analysis

5.3.1. Dependencies

Component:	Required Dependencies	Effective Dependencies
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	ADV_FSP.3 ADV_TDS.2
ADV_FSP.3	ADV_TDS.1	ADV_TDS.2
ADV_TDS.2	ADV_FSP.3	ADV_FSP.3

AGD_OPE.1	ADV_FSP.1	ADV_FSP.3
AGD_PRE.1	None	
ALC_CMC.3	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1	ALC_CMS.3 ALC_DVS.1 ALC_LCD.1
ALC_CMS.3	None	
ALC_DEL.1	None	
ALC_DVS.1	None	
ALC_FLR.3	None	
ALC_LCD.1	None	
ASE_CCL.1	ASE_ECD.1 ASE_INT.1 ASE_REQ.1	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
ASE_ECD.1	None	
ASE_INT.1	None	
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1 ASE_OBJ.2	ASE_ECD.1 ASE_OBJ.2
ASE_SPD.1	None	
ASE_TSS.1	ADV_FSP.1 ASE_INT.1 ASE_REQ.1	ADV_FSP.3 ASE_INT.1 ASE_REQ.2
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	ADV_FSP.3 ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	ADV_FSP.3 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
ATE_DPT.1	ADV_ARC.1 ADV_TDS.2 ATE_FUN.1	ADV_ARC.1 ADV_TDS.2 ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 ADV_FSP.1 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1	ADV_ARC.1 ADV_FSP.3 ADV_TDS.2 AGD_OPE.1 AGD_PRE.1

5.4. SECURITY REQUIREMENTS RATIONALE

Dependencies

Table 5 SFR dependencies

Component:	Dependencies	Which is
FAU_GEN.1	FPT_STM.1	Not included because provided by the operating system
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, and FMT_MTD_CIMC.5
FAU_STG.1	FAU_GEN.1	Included
FAU_STG.4	FAU_STG.1	Included
FCO_NRO_CIMC.3	FIA_UID.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_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	
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	
FPT_CIMC_TSP.1	FAU_GEN.1	Included

	FMT_MOF.1	Included
FPT_ITC.1	None	
FDP_SDI_CIMC.3	None	
FDP_ITT.1	FDP_ACC.1 (or FDP_IFC.1)	FDP_ACC.1 included
FPT_ITT.1	None	

Security objective coverage

OT.Certificates is provided by **FDP_CIMC_CER.1 (Certificate Generation)** which ensures that certificates are valid, and **FDP_CIMC_CRL.1 (Certificate revocation list validation)**, **FDP_CIMC_CSE.1 (Certificate status export)**, and **FDP_CIMC_OCSP.1 (OCSP basic response validation)** which ensure that certificate revocation lists and certificate status information are valid.

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

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

OT.Control unknown source communication traffic is provided by **FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin)** which covers the requirement that the TOE discard messages from an unknown source that contain security-relevant information

OT.Data import/export is provided by **FPT_ITC.1 (Inter-TSF confidentiality during transmission)** which cover the requirement that data other than private and secret keys be protected when they are transmitted to and from the CIMC.

OT.Individual accountability and audit records is provided by a combination of requirements

FIA_UID.1 (Timing of identification) covers the requirement that users be identified before performing any security-relevant operations. **FAU_GEN.1 (Audit data generation)** and **FAU_SEL.1 (Selective audit)** cover the requirement that security-relevant events be audited while **FAU_GEN.2 (User identity association)** covers the requirement that the date and time of audited events are recorded in the audit records along with the identities of the entities responsible for the actions

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

OT.Limitation of administrative access is provided by **FDP_ACC.1 (Subset access control)**, **FDP_ACF.1 (Security attribute based access control)**, **FIA_UAU.1 (Timing of authentication)**, and **FIA_UID.1 (Timing of identification)**. **FIA_UAU.1 (Timing of authentication)** and **FIA_UID.1 (Timing of identification)** ensure that Administrators, operator[CIMC]s, Officers, and Auditors can not perform any security-relevant operations until they have been identified and authenticated and **FDP_ACC.1 (Subset access control)** and **FDP_ACF.1 (Security attribute based access control)** ensure that Administrators, operator[CIMC]s, Officers, and Auditors can only perform those operations necessary to perform their jobs.

OT.Maintain user attributes is provided by **FIA_USB.1 (User-subject binding)** which cover the requirement to maintain a set of security attributes associated with individual users and/or subjects acting on users' behalves.

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

OT.Object and data recovery free from malicious code is provided by **FDP_CIMC_BKP.1 (CIMC backup and recovery)**, **FDP_CIMC_BKP.2 (Extended CIMC backup and recovery)** cover the requirement to be able to recover to a viable state

OT.Protect stored audit records is provided by **FAU_STG.1 (Protected audit trail storage)** which covers the requirement that audit records be protected against modification or unauthorized deletion. **FPT_CIMC_TSP.1 (Audit log signing event)** is required so that modifications to the audit logs can be detected

OT.Protect user and TSF data during internal transfer is provided by **FDP_ITT.1 (Basic internal transfer protection) (user data integrity and user data confidentiality)** which covers the requirement that user data be protected during internal transfer and **FPT_ITT.1 (Basic internal TSF data transfer protection) (internal data integrity and internal data confidentiality)** which covers the requirement that TSF data be protected during internal transfer

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

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

OT.Security-relevant configuration management is provided by **FMT_MOF.1 (Management of security functions behavior)** which covers the requirement that only authorized users can change the configuration of the system. **FMT_MOF_CIMC.3 (Extended certificate profile management)** cover the requirement that Administrators be able to control the types of information that are included in generated certificates. **FMT_MOF_CIMC.5 (Extended certificate revocation list profile management)** covers the requirement that Administrators be able to control to the types of information that are included in generated certificate revocation lists. **FMT_MOF_CIMC.6 (OCSP Profile Management)** covers the requirement that Administrators be able to control to the types of information that are included in generated OCSP responses..

6. TOE SUMMARY SPECIFICATION

The objective for the TOE summary specification is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs.

6.1. SECURITY FUNCTIONS

6.1.1. Certificate generation

The TOE provides a certificate generation service.

The certificate requests originate from:

- A Registration Authority
- A Certification Authority operator.

The certificates generated are conformant with Certificate Generation Profiles (CGPs) configured on the CA that generates them.

Table 6: Coverage of certificate generation related SFRs

Requirements	Titles	Rationales
FCO_NRO_CIMC.3	Enforced proof of origin and verification of origin	All certificate requests must be signed in order to be processed. The signature is either that of a Registration Authority, or that of a Certification Authority operator. Signature validity is verified by the TOE.
FDP_CIMC_CER.1	Certificate generation	The TOE generates certificates conformant with defined certificate profiles.
FMT_MOF_CIMC.3	Extended certificate profile management	The TOE provides a certificate profile management interface.

6.1.2. Certificate revocation

The TOE provides a certificate revocation service.

The certificate revocation requests originate from:

- A Registration Authority
- A Certification Authority administration operator.

The TOE revokes the certificate once the request has been verified. It generates Certificate Revocation Lists (CRLs) for each certification authority.

Revocation list generation is initiated:

- Periodically (the interval can be configured by a CA operator).
- Manually by a CA operator.
- Within a configurable set time limit after revocation of a certificate.

A revocation list (CRL) is generated according to a Revocation list Generation Profile (RGP) configured on the CA, then published by the TOE.

Table 7: Coverage of certificate revocation related SFRs

Requirements	Titles	Rationales
FCO_NRO_CIMC.3	Enforced proof of origin and verification of origin	All requests must be signed in order to be processed. The signature is either that of a Registration Authority, or that of a Certification Authority operator. Signature validity is verified by the TOE.
FDP_CIMC_CRL.1	Certificate revocation list validation	The TOE generates a revocation list.
FMT_MOF_CIMC.5	Extended certificate revocation list profile management	The TOE provides a CRL profile management interface.

6.1.3. Certificate status publication

The TOE publishes the CRLs it generates in publication repositories that can be configured by a CA operator.

These repositories are LDAP directories or file systems. File systems may be replicated in order to be made available on a Web server.

The TOE provides an OCSP service for certificate status verification.

The TOE accepts OCSP requests conformant with the IETF RFC 2560 standard on http. The request must concern a certificate issued by a CA of the server receiving the OCSP request. Certificate status is directly read in the database and thus contains the most recent information. The responses are in the "basic response" format of the IETF RFC 2560 standard and are signed with a specific key pair of the OCSP responder.

Table 8: Coverage of certificate status publication related SFRs

Requirements	Titles	Rationales
FDP_CIMC_CSE.1	Certificate status export	The TOE provides an OCSP service.
FDP_CIMC_OCSP.1	OCSP basic response validation	OCSP responses conform to the IETF RFC 2560 standard
FMT_MOF_CIMC.6	OCSP profile management	The OCSP responses are in "basic response" format.

6.1.4. Identification and authentication

- TrustyKey identifies and then authenticates users who connect to the CA programs (see 7.1.2).

However, identification or authentication is not required to view public information (certificates and CRLs) in the repositories.

Table 9: Coverage of identification and authentication related SFRs

Requirements	Titles	Rationales
FIA_UAU.1	Timing of authentication	Authentication is required to access the services offered by the TOE (except to view repositories).
FIA_UID.1	Timing of identification	Identification is required to access the services offered by the TOE (except to view repositories).
FIA_USB.1	User-subject binding	Each user who connects is assigned a user profile.

6.1.5. Role management

TrustyKey enables the profiles to which rights will be assigned to be managed (see 7.1.2).

Table 10: Coverage of role management related SFRs

Requirements	Titles	Rationales
FMT_SMR.1	Security roles	Rights are managed via user profiles, each user is assigned a user profile.
FMT_MOF.1	Management of security functions behavior	The configuration function access is restricted to specific roles via the user profiles.

6.1.6. Access control

The TOE provides users only with the services authorized by their profile.

Table 11: Coverage of access control related SFRs

Requirements	Titles	Rationales
FDP_ACC.1	Subset access control	Users can only access functions to which their rights profile gives access.
FDP_ACF.1	Security attribute based access control	Users can only access functions to which their rights profile gives access.

6.1.7. Key management

TrustyKey saves public keys (included in certificates) and user information in a database and stores private keys in an HSM.

Certification Authority private keys and TSF private keys are generated and stored in the TrustyKey CA HSM and cannot be exported.

Table 12: Coverage of key management related SFRs

Requirements	Titles	Rationales
FMT_MTD_CIMC.4	TSF private key confidentiality protection	The private keys of the applications are stored in the HSM.
FDP_SDI_CIMC.3	Stored public key integrity monitoring and action	Certificate integrity is verified before use.

FMT_MTD_CIMC.5	TSF secret key confidentiality protection	The secret keys of the applications are stored in the HSM.

6.1.8. Audit

TrustyKey CA records events in a database (log). Each log record is linked with the authenticated user who performed the action traced.

TrustyKey provides a log consultation (viewer) interface with search and filtering functions.

Log integrity is ensured by sealing each record with an authentication code. This code is computed using the record data and the previous record seal, and a secret key of the application.

Table 13: Coverage of audit related SFRs

Requirements	Titles	Rationales
FAU_GEN.1	Audit data generation	Events are recorded in the database.
FAU_GEN.2	User identity association	Each record is linked with a user.
FAU_SEL.1	Selective audit	There is a consultation (viewer) interface.
FAU_STG.1	Protected audit trail storage	Log integrity is ensured by record signature mechanisms.
FAU_STG.4	Prevention of audit data loss	The system engineer regularly checks that the database has the disk space it requires to operate. If an event write operation fails, the function affected returns an error and the application stops.
FPT_CIMC_TSP.1	Audit log signing event	Log integrity is ensured by record signature mechanisms.

6.1.9. Communication protection

The confidentiality and integrity of the communications between the CA server and RA and operators are protected.

TrustyKey CA provides this protection by TLS/SSL type mechanisms in mutual-authentication mode.

Table 14: Coverage of communication protection related SFRs

Requirements	Titles	Rationales
FCO_NRO_CIMC.3	Enforced proof of origin and verification of origin	operators are authenticated in SSL mode and sign certificate and revocation requests. The RA and CA sign the messages exchanged between the two components.
FPT_ITC.1	Inter-TSF confidentiality during transmission (internal data export)	CA communications with operators are protected by a TLS/SSL tunnel.
FDP_ITT.1 (user data integrity)	Basic internal transfer protection	Communications between the CA and the CA applet is protected by a TLS/SSL tunnel.

FDP_ITT.1 (user data confidentiality)	Basic internal transfer protection	Communications between the CA and the CA applet is protected by a TLS/SSL tunnel.
FPT_ITT.1 (internal data integrity)	Basic internal transfer protection	Communications between the CA and the CA applet is protected by a TLS/SSL tunnel.
FPT_ITT.1 (internal data confidentiality)	Basic internal transfer protection	Communications between the CA and the CA applet is protected by a TLS/SSL tunnel.

6.1.10. Backup and Recovery

TrustyKey CA provides a backup and recovery functionality, that ensures integrity and confidentiality, using a backup utility and the database built-in functions.

Table 15: Coverage of communication protection related SFRs

Requirements	Titles	Rationales
FDP_CIMC_BKP.1	CIMC backup and recovery	TrustyKey provides a tool to encrypt/decrypt backup data using a password, and the administrator guide describes the related procedure. HSM backup shall be performed according to HSM provider procedures.
FDP_CIMC_BKP.2	Extended CIMC backup and recovery	The TrustyKey backup/restore tool verifies integrity and confidentiality. Key backup integrity and confidentiality is ensured by the HSM provider backup procedures.

6.2. RATIONALES

The functional requirement coverage rationales are given directly in the descriptions of the security functions.

7. ANNEXES

7.1. ACCESS CONTROL POLICY

7.1.1. TrustyKey CA Administration

Access control policy is based on:

- Rights,
- Profile rights,
- CA Administration authorization.

7.1.1.1. Rights

A **right** is an authorization, granted to a user, to use a TrustyKey software function.

The complete list of the rights available for TrustyKey CA is given below:

Type of rights	Right
CA Administration	Declare a root authority
	Declare a child authority
	Configure an authority
	Request an authority certificate
	Generate an authority certificate
	Import an authority certificate
	Revoke sub-authority certificates
	Revoke certificates signed by an authority
	Declare revocation of an authority certificate
	Publish certificates
	Publish revocation lists
	Generate a technical certificate
	Revoke a technical certificate
	Manage RA, PIC and RC certificates
Server management rights	Manage CGPs and RGPs
	Manage publication repositories
	Request a server certificate
	Import a server certificate
Operator management rights	Manage operator profiles
	Manage operators
Supervision rights	View audit log

7.1.1.2. Rights profiles

To enable rights to be rapidly assigned to an operator, rights profiles are used.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40

A right profile is a collection of rights, defined by TrustyKey CA operators. Some default right profiles are created during TrustyKey CA initialization.

For example, an operator who is in charge to manage the Certification Authorities certificates is granted a profile containing all CA Administration rights, whereas a supervision operator is granted a profile with only the right to view audit log.

7.1.1.3. Authorization of CA Management

Besides the right profile, an operator is authorized to manage only a subset of Certification Authorities declared on a TrustyKey CA instance. Each CA Administration operation is hence authorized only if the operator is granted a right for this particular operation, and moreover is authorized to manage the specific associated authority.

For example, on operator is granted a CA Administration profile with all CA Administration rights, and is authorized to manage only the root CA. This operator can renew the root CA certificate, generate certificate for sub-authorities, but cannot request a certificate for any sub-authority.

7.1.2. TrustyKey CA CMP Services

The registration authorities authorized to submit certificate requests (generation and revocation) must be declared by the CA Administrator for the particular targeted CA.

When a CMP message is received, the authenticated sender is searched among the list of declared RA on the server. The request is refused is the RA is not found. Then for each request included in the CMP message, the sender is searched among the list of declared RA for the associated CA (certificate issuer). The specific request is not processed if the check is negative.

7.1.3. TrustyKey CA OCSP Responder

The OCSP responder accepts requests without any access control.

7.2. IDENTIFICATION AND AUTHENTICATION

Identification and authentication mechanisms depend on target TrustyKey CA application.

7.2.1. TrustyKey CA Administration

The operator connects to TrustyKey CA Administration application via his Web browser, by establishing an SSL link with mutual authentication.

The Distinguished Name of the operator's authentication certificate is used by TrustyKey CA to identify the operator.

operator authentication is ensured by the fact that only the token owner (who is the only person to know the token PIN code) is able to establish the mutual SSL connection.

Once the operator has been authenticated, his profile is read in the database and the corresponding rights assigned to him. The TrustyKey CA applet executed by the browser establishes an SSL link with the server using the same credentials.

7.2.2. TrustyKey CA CMP Services

As an operator, a registration application must establish a SSL mutual authentication connection with TrustyKey CA CMP services application to be able to send certificate requests (generation and revocation). This ensures the identification and authentication (as certificate owner) of the sender.

Moreover, the CMP requests are signed by the registration application and the signing certificate identifier is included in the request.

7.2.3. TrustyKey CA OCSP Responder

OCSP clients are not identified.

7.3. EXTENDED COMPONENTS DEFINITION

7.3.1. Definition of the Family FPT_CIMC_TSP

To define the security functional requirements of the TOE an additional family (FPT_CIMC_TSP) of the Class FPT (protection of the TSF) is defined here.

Family behavior:

This family defines the signature of the audit logs.

Component leveling:

There is only one component in this family:

- FPT_CIMC_TSP.1 Signature of audit logs.

Management: FPT_CIMC_TSP.1

There are no management activities foreseen.

Audit: FPT_CIMC_TSP.1

There are no actions defined to be auditable.

FPT_CIMC_TSP.1 Audit log signing event

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation, FMT_MOF.1 Management of security functions behavior

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

7.3.2. Definition of the Family FCO_NRO_CIMC

To define the security functional requirements of the TOE an additional family (FCO_NRO_CIMC) of the Class FCO (Communication) is defined here.

Family behavior:

This family defines the signature of the certificate status information.

Component leveling:

There is only one component in this family:

- FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin.

Management: FCO_NRO_CIMC.3

There are no management activities foreseen.

Audit: FCO_NRO_CIMC.3

There are no actions defined to be auditable.

FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

Hierarchical to: FCO_NRO.2

Dependencies: FIA_UID.1 Timing of identification

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 [assignment: 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.

7.3.3. Definition of the Family FDP_CIMC_BKP

To define the security functional requirements of the TOE an additional family (FDP_CIMC_BKP) of the Class FDP (User Data protection) is defined here.

Family behavior:

This family defines the CIMC backup and recovery.

Component leveling:

There are two components in this family, without hierarchical relation:

- FDP_CIMC_BKP.1 CIMC backup and recovery
- FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Management: FDP_CIMC_BKP.1, FDP_CIMC_BKP.2

There are no management activities foreseen.

Audit: FDP_CIMC_BKP.1, FDP_CIMC_BKP.2

There are no actions defined to be auditable.

FDP_CIMC_BKP.1 CIMC backup and recovery

Hierarchical to: No other components.

Dependencies: FMT_MOF.1 Management of security functions behavior

FDP_CIMC_BKP.1.1 The TSF shall include a backup function.

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

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

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

b) a stored copy of the backup data;

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

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

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

FDP_CIMC_BKP.2 Extended CIMC backup and recovery

Hierarchical to: No other components.

Dependencies: FDP_CIMC_BKP.1 CIMC backup and recovery

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

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

7.3.4. Definition of the Family FDP_CIMC_CER

To define the security functional requirements of the TOE an additional family (FDP_CIMC_CER) of the Class FDP (User Data protection) is defined here.

Family behavior:

This family defines the certificate generation.

Component leveling:

There is only one component in this family:

- FDP_CIMC_CER.1 Certificate generation

Management: FDP_CIMC_CER.1

There are no management activities foreseen.

Audit: FDP_CIMC_CER.1

There are no actions defined to be auditable.

FDP_CIMC_CER.1 Certificate Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_CIMC_CER.1.1 The TSF shall only generate certificates whose format complies with [assignment: the X.509 standard for public key certificates, other standard (ST shall specify the standard and ST author shall ensure that a description of the format is available), or ST specified format (ST shall include a description of the format)].

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.

7.3.5. Definition of the Family FDP_CIMC_CRL

To define the security functional requirements of the TOE an additional family (FDP_CIMC_CRL) of the Class FDP (User Data protection) is defined here.

Family behavior:

This family defines the certificate revocation list validation.

Component leveling:

There is only one component in this family:

- FDP_CIMC_CRL.1 Certificate revocation list validation

Management: FDP_CIMC_CRL.1

There are no management activities foreseen.

Audit: FDP_CIMC_CRL.1

There are no actions defined to be auditable.

FDP_CIMC_CRL.1 Certificate revocation list validation

Hierarchical to: No other components.

Dependencies: No dependencies

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:

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

7.3.6. Definition of the Family FDP_CIMC_CSE

To define the security functional requirements of the TOE an additional family (FDP_CIMC_CSE) of the Class FDP (User Data protection) is defined here.

Family behavior:

This family defines the export of the certificate status information.

Component leveling:

There is only one component in this family:

- FDP_CIMC_CSE.1 Certificate status export

Management: FDP_CIMC_CSE.1

There are no management activities foreseen.

Audit: FDP_CIMC_CSE.1

There are no actions defined to be auditable.

FDP_CIMC_CSE.1 Certificate status export

Hierarchical to: No other components

Dependencies: No dependencies

FDP_CIMC_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with [assignment: the X.509 standard for CRLs, the OCSP standard as defined by RFC 2560, other standard (ST shall specify the standard and ST author shall ensure that a description of the format is available), or ST specified format (ST shall include a description of the format)].

7.3.7. Definition of the Family FDP_CIMC_OCSP

To define the security functional requirements of the TOE an additional family (FDP_CIMC_OCSP) of the Class FDP (User Data protection) is defined here.

Family behavior:

This family defines the OCSP response validation.

Component leveling:

There is only one component in this family:

- FDP_CIMC_OCSP.1 OCSP basic response validation

Management: FDP_CIMC_OCSP.1

There are no management activities foreseen.

Audit: FDP_CIMC_OCSP.1

There are no actions defined to be auditable.

FDP_CIMC_OCSP.1 OCSP basic response validation

Hierarchical to: No other components.

Dependencies: No dependencies

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:

- The version field shall contain a 0.

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

7.3.8. Definition of the Family FMT_MOF_CIMC

To define the security functional requirements of the TOE an additional family (FMT_MOF_CIMC) of the Class FMT (Security Management) is defined here.

Family behavior:

This family defines the protection of the TSF private key confidentiality.

Component leveling:

There are three components in this family without hierarchical relation:

- FMT_MOF_CIMC.3 Extended certificate profile management
- FMT_MOF_CIMC.5 Extended certificate revocation list profile management
- FMT_MOF_CIMC.6 OCSP profile management

Management: FMT_MOF_CIMC.3, FMT_MOF_CIMC.5, FMT_MOF_CIMC.6

There are no management activities foreseen.

Audit: FMT_MOF_CIMC.3, FMT_MOF_CIMC.5, FMT_MOF_CIMC.6

There are no actions defined to be auditable.

FMT_MOF_CIMC.3 Extended certificate profile management

Hierarchical to: No other components

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

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

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

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

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

- keyUsage;
- basicConstraints;
- certificatePolicies

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

FMT_MOF_CIMC.5 Extended certificate revocation list profile management

Hierarchical to: No other components

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

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

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

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

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

FMT_MOF_CIMC.6 OCSP profile management

Hierarchical to: No other components.

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

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.

7.3.9. Definition of the Family FMT_MTD_CIMC

To define the security functional requirements of the TOE an additional family (FMT_MTD_CIMC) of the Class FMT (Security Management) is defined here.

Family behavior:

This family defines the protection of the TSF private and secret keys confidentiality.

Component leveling:

There are two components in this family with hierarchical relation:

- FMT_MTD_CIMC.4 TSF private key confidentiality protection
- FMT_MTD_CIMC.5 TSF secret key confidentiality protection

Management: FMT_MTD_CIMC.4, FMT_MTD_CIMC.5

There are no management activities foreseen.

Audit: FMT_MTD_CIMC.4, FMT_MTD_CIMC.5

There are no actions defined to be auditable.

FMT_MTD_CIMC.4 TSF private key confidentiality protection

Hierarchical to: No other components

Dependencies: No dependencies

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

FMT_MTD_CIMC.5 TSF secret key confidentiality protection

Hierarchical to: No other components

Dependencies: No dependencies

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.

7.3.10. Definition of the Family FDP_SDI_CIMC

To define the security functional requirements of the TOE an additional family (FDP_SDI_CIMC) of the Class FDP (User Data Protection) is defined here.

Family behavior:

This family defines the monitoring of stored public key integrity.

Component leveling:

There is only one component in this family:

- FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

Management: FDP_SDI_CIMC.3

There are no management activities foreseen.

Audit: FDP_SDI_CIMC.3

There are no actions defined to be auditable.

FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

Hierarchical to: No other components

Dependencies: No dependencies

FDP_SDI_CIMC.3.1 Public keys stored within the CIMC, but not within a FIPS 140-1 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_CIMC.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall [assignment: action to be taken if the verification fails, with the ST rationale showing why this completion is consistent with maintenance of security].

LIST OF REVISIONS

Rev.	Date	Issued by	Checked by	Approved by	Reason
7.1	March 28th 2011	G. Tétu	S. Blonde	JF Wiorek	"iteration 1 and 2" replaced by user/internal data integrity and user/internal data confidentiality
7.0	March 21st 2011	G. Tétu	S. Blonde	JF Wiorek	Correction of version number FAU_STG.4.1 updated
6.0	March 21st 2011	S. Vergnes/ C. Blad	G. Tétu, JF Wiorek	JF Wiorek	OE removed or updated: - OE.Administrators, operator[CIMC]s, Officers and Auditors guidance documentation. - OE.Lifecycle_security. - OE.Repair_identified_security_flaws. - OE.Prevent malicious code. -OE.Cryptographic functions. FAU_STG.1 label fixed in FAU_STG.4 definition Security objective coverage : "iteration 1 and 2" removed when useless, OT.Limitation of administrative access coverage completed.
5.0	November 3rd 2010	S. Vergnes / C. Blad	JF Wiorek	JF Wiorek	TOE overview (§1.3.2) rewritten Extended component definition FPT_STM.1 removed (environment objective) FPT_CIMC_TSP.1.3 removed Objectives on TOE and environment dispatched on TOE or environment CC Reference fixed
4.0	October 14th 2010	S. Vergnes	G. Tétu	JF Wiorek	Authentic Web Pack version updated Luna HSM type updated for root instance Roles correspondence updated Administrator role defined for FMT_MOF_CIMC.3, FMT_MOF_CIMC.5 and FMT_MOF_CIMC.6
3.0	October 5th 2010	S. Vergnes / C. Blad	JF Wiorek	JF Wiorek	Roles description Fix correctness issues
2.0	June 30th 2010	S. Vergnes	JF Wiorek	JF Wiorek	Scope reduced to TrustyKey CA Backup and Restore function description SFR updated Update of rights and audited functions Fix remarks on CIMC profile O.Detect modifications of firmware, software, and backup data is an environment objective
1.0	November 04th 2008	S. Vergnes	JF Wiorek	JF Wiorek	Version submitted for the evaluation file.

FILES

Software	*User files*
Windows XP	
Word 2003	*Template:* Normal.dot *Document:* TrustyKey6.0_EN_Security_Target_rev7.0.doc

DISTRIBUTION

Initial Name	*Entity*	*Initial Name*	*Entity*

This document is available on the server in electronic form.

It is not officially issued in paper form.

If you are using a printed copy of this document, please consult the server to make sure that you have the most recent applicable revision.

22, avenue Galilée – 92350 Le Plessis Robinson – France – Tél. : +33 (0)1 41 28 40 00 – Fax : +33 (0)1 41 28 40 40