Architect of an Open World™

# Security Target

## MetaPKI

www.bull.com

# Status

| | |
|---|---|
| **Rédaction** | Sébastien Gelgon |
| **Validation** | Pierre-Jean Aubourg |
| **Classification** | Diffusion restreinte |
| **Statut du document** | Version finale |
| **Version actuelle** | 1.2 |
| **Référence** | EVALCC-MPKI-ST-01 |

# History of revisions

| Date | Version | Commentaire |
|---|---|---|
| 06/06/2010 | 0.1 | Création |
| 30/06/2010 | 0.2 | TOE overview complétée<br>Intégration des SFR |
| 25/09/2010 | 0.3 | Instanciation des SFR suite à réunion de travail |
| 29/10/2010 | 0.4 | Version revue pour diffusion au client |
| 25/11/2010 | 0.5 | Version revue pour diffusion ANSSI. |
| 13/01/2011 | 0.6 | Prise en compte des remarques de l'ANSSI.<br>Compléments dans les sections 7, 8 et 9. |
| 24/01/2011 | 0.7 | Version après validation interne |
| 11/02/2011 | 0.8 | Mise à jour<br>- PP Claim et argumentaire<br>- Ajout du rôle d'administrateur système (hors contrôle de la TOE) |
| 28/04/2011 | 0.9 | - Ajout des références HSM, client LDAP et SGBDs<br>- Ajout paragraphe 1.3.1.2 |
| 04/05/2011 | 0.9.1 | - prise en compte remarque évaluateur. |
| 10/05/2011 | 0.9.2 | Intégration d'une partie de IAIK dans la TOE (modification Fig. 3: TOE bundaries) |
| 23/06/2011 | 0.10 | Prise en compte des remarques suite à RE0 et RTE ASE :<br>- Add components identification and version of MetaPKI Pre-requisites<br>- IAIK component out of the scope of TOE<br>- supress Operator role<br>- TOE does not use TSF secret keys<br>- Certificate Rights are not automatically propagate when certificate renewal. |
| 28/09/2011 | 0.11 | - Mise à jour version MetaPKI et pré-requis<br>- Ajout de la fonctionnalité Syslog de MetaPKI hors périmètre de la TOE<br>- Ajout argumentaire de non applicabilité de FMT_MTD_CIMC.5 |
| 12/12/2011 | 1.0 | Version finale |
| 27/02/2012 | 1.1 | Modification version de la TOE |
| 29/11/2012 | 1.2 | Version finale pour diffusion publique |

# Contents

**1 SECURITY TARGET IDENTIFICATION ..... 5**

1.1 IDENTIFICATION ..... 5
1.2 TOE OVERVIEW ..... 5
1.2.1 Usage and Major Security Features ..... 6
1.2.2 TOE Type ..... 8
1.3 TOE DESCRIPTION ..... 9
1.3.1 Functional architecture ..... 9
1.3.2 Technical Architecture ..... 11
1.3.3 TOE Boundary ..... 12
1.3.4 Evaluated configuration ..... 12

**2 CONFORMANCE CLAIM ..... 15**

2.1 CC CONFORMANCE CLAIM ..... 15
2.2 PP CONFORMANCE CLAIM ..... 15
2.3 CONFORMANCE RATIONALE ..... 15

**3 SECURITY PROBLEM DEFINITION ..... 17**

3.1 SECURE USAGE ASSUMPTIONS ..... 17
3.1.1 Personnel ..... 17
3.1.2 Connectivity ..... 18
3.1.3 Physical ..... 18
3.2 THREATS ..... 19
3.2.1 Authorized users ..... 19
3.2.2 System ..... 19
3.2.3 Cryptography ..... 20
3.2.4 External attacks ..... 20
3.3 ORGANIZATIONAL SECURITY POLICIES ..... 20

**4 SECURITY OBJECTIVES ..... 21**

4.1 SECURITY OBJECTIVES FOR THE TOE ..... 21
4.1.1 Authorized users ..... 21
4.1.2 System ..... 21
4.1.3 Cryptography ..... 21
4.1.4 External attacks ..... 22
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT ..... 22
4.2.1 Non-IT security objectives for the environment ..... 22
4.2.2 IT security objectives for the environment ..... 23
4.3 SECURITY OBJECTIVES FOR BOTH THE TOE AND THE ENVIRONMENT ..... 24
4.4 SECURITY OBJECTIVES RATIONALE ..... 26

**5 EXTENDED COMPONENTS DEFINITION ..... 27**

**6 SECURITY REQUIREMENTS ..... 28**

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS ..... 28
6.1.1 Security Audit ..... 28
6.1.2 Roles ..... 32
6.1.3 Backup and recovery ..... 36
6.1.4 Access Control ..... 37
6.1.5 Identification and Authentication ..... 39
6.1.6 Remote Data Entry and Export ..... 41
6.1.7 Key Management ..... 43
6.1.8 Certificate Profile Management ..... 45

6.1.9 Certificate revocation list profile management ..... 46
6.1.10 Online Certificate Status Protocol (OCSP) Profile Management ..... 46
6.1.11 Certificate Registration ..... 47
6.1.12 Certificate Revocation ..... 48
6.2 TOE SECURITY ASSURANCE REQUIREMENTS ..... 49
6.3 SECURITY REQUIREMENTS RATIONALE ..... 50
6.3.1 SFR Dependencies ..... 50
6.3.2 SFR from PP CIMC unapplicable to this ST ..... 52

**7 TOE SUMMARY SPECIFICATIONS ..... 54**

7.1 TOE SECURITY FUNCTIONS ..... 54
7.1.1 Security Audit ..... 54
7.1.2 Roles ..... 54
7.1.3 Backup and recovery ..... 55
7.1.4 Access control ..... 55
7.1.5 Identification and authentication ..... 55
7.1.6 Remote Data Entry and Export ..... 55
7.1.7 Key Management ..... 56
7.1.8 Certificate Profile Management ..... 57
7.1.9 Information on Certificates statuses and Related Management ..... 57
7.1.10 Registration Authority ..... 57
7.2 TOE SUMMARY SPECIFICATIONS RATIONALE ..... 58

**8 ACCESS CONTROL POLICIES ..... 64**

8.1 CIMC IT ENVIRONMENT ACCESS CONTROL POLICY ..... 64
8.2 CIMC TOE ACCESS CONTROL POLICY ..... 64

**9 GLOSSARY OF TERMS AND ACRONYMS ..... 66**

9.1 GLOSSARY OF TERMS ..... 66
9.2 ACRONYMS ..... 70

# 1 Security Target Identification

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

## 1.1 Identification

| | |
|---|---|
| ST Title | Bull MetaPKI – Security Target |
| ST reference | EVALCC-MPKI-ST-01/v1.2 |
| TOE Identification | MetaPKI v9.2.5 |
| CC Conformance | Common Criteria for Information Technology Security Evaluation, Version 3.1 R3 |
| PP Conformance | Based on Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001 |
| Assurance Level | Evaluation Assurance Level 3 augmented with ALC_FLR.3 and AVA_VAN.3 |

## 1.2 TOE Overview

Information System (IS) security is an essential issue for organizations moving to paperless exchanges, whether for internal communications or for relationships with partners and customers. Electronic certificates respond to this need as they allow applications to support security services such as user authentication, non-repudiation of transactions, and confidentiality of data exchanges.

Bull, a European actor in IS security, provides MetaPKI, a complete solution to create electronic certificates and manage their life cycle.

### Keeping control of security

For all the use cases mentioned above, Users and applications are provided with one or more key pairs (a public key and a private key) and public key certificates, generated by a Certification Authority (CA), that associate the registered user or application with the public key.

MetaPKI supports one or more Certification Authorities, that may be independent, or subordinate CAs.

A whole range of certificates profiles is supported by MetaPKI. For each profile, the registration process may be adopted to the specific needs of the organization and integrated with the existing IS.

A workflow manager handles the registration process in order to minimize the time to produce and manage the certificates through the use of one or more Local Registration Authorities (LRA).

#### Accompanying growth

MetaPKI's modularity and sales conditions enable the smooth deployment of a solution according to the organisation's needs: new types of certificate, new management processes, new organisational units, new Certification Authorities may be added as required. The solution includes key escrow and key recovery for confidentiality keys.

#### Bull, European actor in IS security

Bull provides consultancy services for defining the best way to integrate MetaPKI into the IS, as well as for making use of certificates in applications (e.g. SSO-Single Sign On). Bull provides the training and the support.

MetaPKI components may be hosted in secure data centres managed by Bull.

### 1.2.1 Usage and Major Security Features

#### 1.2.1.1 TOE Usage

MetaPKI supports the following features:

- Certification authority: support of multiple certification authorities in a same instance of the PKI; support of multiple certificate profiles in a same CA
- Registration Authorities and/or Local Registration Authority (RA and/or LRA): customizable requests and validation workflows for certificate/renewal/revocation; web service interface; support of multiple RAs
- Publication Services: support of HTTP and LDAP/ActiveDirectory publication for CRLs and Certificates
- OSCP Responder
- Generation of key pairs in centralized or decentralized mode, depending on the usage of the associated certificates and on the client's need
- Key Escrow and Key Recovery Services
- Management services: management of the internal users of the PKI; management of the rights, management of the functional modules; management of the certificate profiles, …
- Audit

MetaPKI may optionally support the following entities (out of the scope of the TOE)

- Card Management System (GesCard)
- RFC3161 Time stamping server (MetaTIME)

#### 1.2.1.2 TOE security services

MetaPKI includes strong internal security mechanisms:

##### Security Audit (FAU)

Security Audit includes a chronological logging of events that occur in a system to act as a deterrent against security violations.

All actions related to the management of certificates are recorded in a database only accessible by authorized operators (Administrators, Officers or Auditors). All events are logged.

##### Communication (FCO)

Communications between functional entities and information stored in the database are all protected. Sensitive information is enciphered.

##### Cryptographic Support (FCS)

Private keys and public keys are protected (*i.e.*, generated and operated) using Hardware Security Modules (HSM). Bull supports different kinds of HSMs, either provided by Bull or by third parties.

##### User Data Protection (FDP)

User Data Protection relates to the protection of user data including certificate issuance, revocation, backup and recovery, and profile management of certificates, Certificate Revocation List (CRL), and Online Certificate Status Protocol (OCSP).

Access to all MetaPKI functional entities is controlled (see FIA bellow).

##### Identification and Authentication (FIA)

Identification and Authentication supports the administration and enforcement of the CIMC access control policies to unambiguously identify the person and/or entity performing functions in a CIMC.

Officers, Auditors and administrators must be authenticated using a X.509 certificate. Strong authentication is supported as far as the private key is held by a smart card or USB token.

##### Security Management (FMT)

Security Management specifies several aspects of management of security functions including distinct roles to maintain the security of the CIMC.

##### Protection of the TOE Security Functions (FPT)

Protection of the TOE Security Functions (TSF) includes functions that manage and protect the integrity, resp. the confidentiality, of TSF data from modification, resp. disclosure. This is carried out through the use of various means such as encryption, reliable time stamps, backup and recovery procedures, self-tests and audit logs.

The access to the TOE services is generally done through a front office server. The sensitive functions are isolated and performed on a separated back office server, only accessible from the front office server.

#### 1.2.1.3 Norms and standards supported for interfaces and protocols

- Certificate format compliance with ITUT X.509v3 and RFC 5280.
- Certificate profile compliance with ETSI TS 101 862, Netscape and Microsoft.
- Revocation information compliance with ITU-T X.509v2 CRL and OCSP Protocol (RFC 2560).
- Certification request format: PKCS#10, SPKAC.
- Key exchange format: PKCS#12.
- Connectivity: LDAP, HTTPS, SMTP.
- HSM interface: PKCS#11.

The TOE can be configured to be compliant with the certificates templates defined in Annex A14 of the French general frame of references for security of information systems (RGS)

### 1.2.2 TOE Type

Bull MetaPKI is a certificate issuance and management software (CIMS).

This software solution can be fully parameterized by the customer to implement any type of Public Key Infrastructure, from the simpler one to the most complex.

Bull MetaPKI can manage several certification authorities in a single occurrence of the software. Different types of certificates can be managed by MetaPKI in a same CA.

## 1.3 TOE Description

### 1.3.1 Functional architecture

The functional architecture of the TOE is depicted in the following figure:

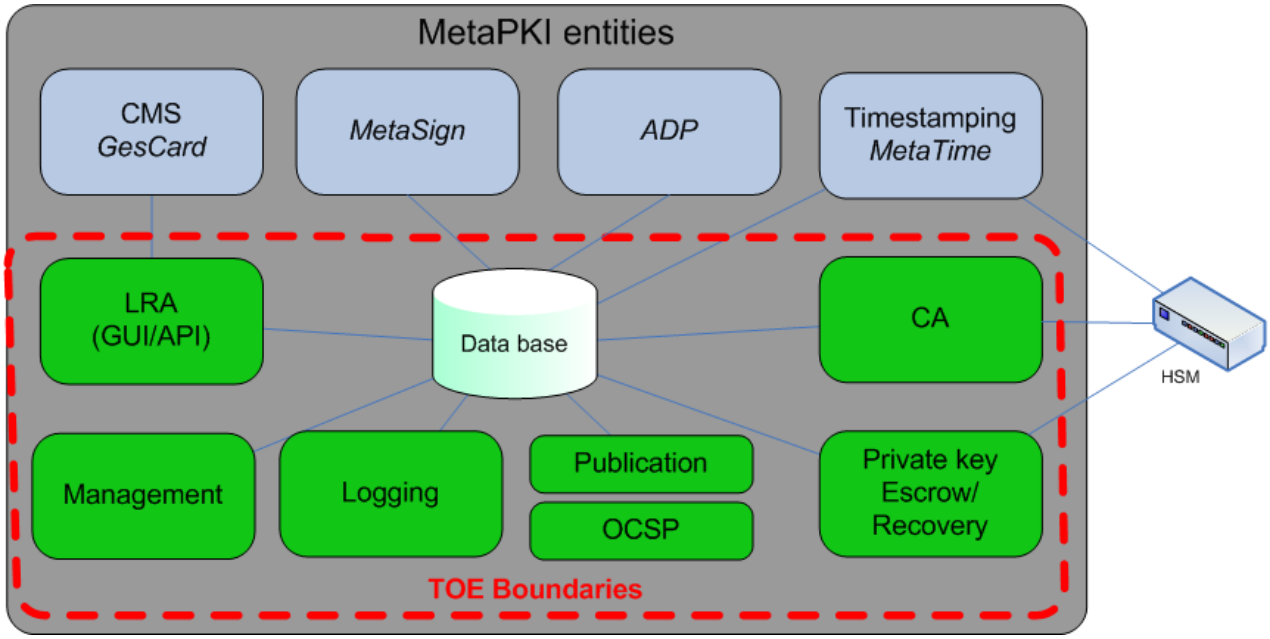


**Figure 1: TOE functional architecture**

#### 1.3.1.1 Functional entities included in TOE scope

##### CA - Certification Authority

A Certification Authority entity is in charge of the generation of the public key certificates based on predefined profiles in accordance with the corresponding certification policies.

A certification authority is also in charge of:

- the management of the certificates data base, including certificates life cycle (e.g., certificate status),
- the constitution (from identified certificate profiles), signature and automated publication of the user certificates
- the constitution, signature and automated publication of the CRLs

##### Registration Authority and/or Local Registration Authority (RA and/or LRA)

The Registration Authority and/or the Local Registration Authority (RA and/or LRA) takes in charge the registration of certificate holder. The RA or the LRA allows the management of a face to face meeting enabling the officer to verify the identity and the credentials of the certificate holder.

RA and LRA may be implemented either through a web interface, or through an API (Access2MetaPKI or Access2GescardCmd).

The registration authority may record different kinds of requests from the user (the final user or the RA Officer, depending on the certification policy.

The supported requests are certification, renewal and revocation requests; They requests are transmitted to the Certification Authority for treatment.

#### Publication Service

The Publication Service allows the distribution of certificate(s) (optionally the key pair, when it has been generated in centralized mode) to the holders. Optionally a publication service may make the certificate(s) available to Relying Parties (RP).

#### Key Escrow and Key Recovery Services

These two services allow:

- the escrow of the private keys associated to certificated used for confidentiality purposes (this service can be configured to be used automatically)
- the secure recovery of an escrowed private key:

The deployment of these services is optional.

#### Management services

These services allow managing the internal users of the PKI and their roles. Management services also allow managing the configuration of the different entities composing the TOE.

The access to the configuration of each functional entity is controlled through the use of roles.

#### Logging

The TOE supports logging services recording the certificate management and TOE configuration management events.

### 1.3.1.2 Optional functional entities

MetaPKI supports the following optional entities which are out of the scope of the TOE

#### Card Management System (GesCard)

Card Management System (GesCard) for managing smart cards: customization, PIN unblocking, etc...

#### MetaTime

MetaTime is a Time Stamp Service which delivers Timestamps conforming to the RFC3161.

#### MetaSign

MetaSign is offering functionalities to generate and to verify advanced electronic signatures conforming to the CAdES and XAdES standards.

#### ADP

ADP is a service which can be activated to store, to archive and to retrieve advanced electronic signatures.

### SysLog

MetaPKI integrates a Syslog service wich allows to redirect all logs produced by MetaPKI to Syslog server. This functionality is out of scope of TOE.

## 1.3.2 Technical Architecture

The TOE design is very modular and flexible, the functional entities may possibly be deployed on several physical or logical servers, for instance to allow a separation of the services between a back office and front office and to implement a highly available infrastructure.

The figure bellow depicts a possible deployment mode with two physical servers:

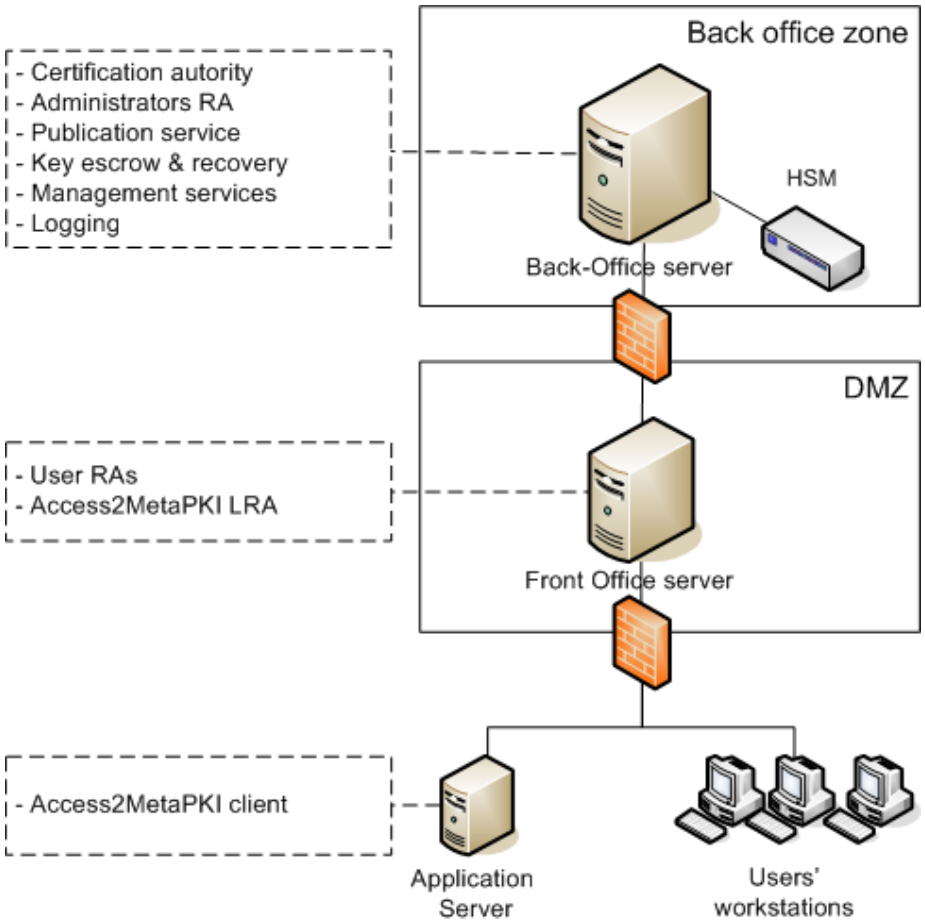


**Figure 2: MetaPKI sample technical architecture with two physical servers**

### 1.3.3 TOE Boundary

The following figure shows the different components needed for the TOE to operate. The green ones are part of the TOE boundary; the blue ones are open source software prerequisites that are out of the scope of the TOE.

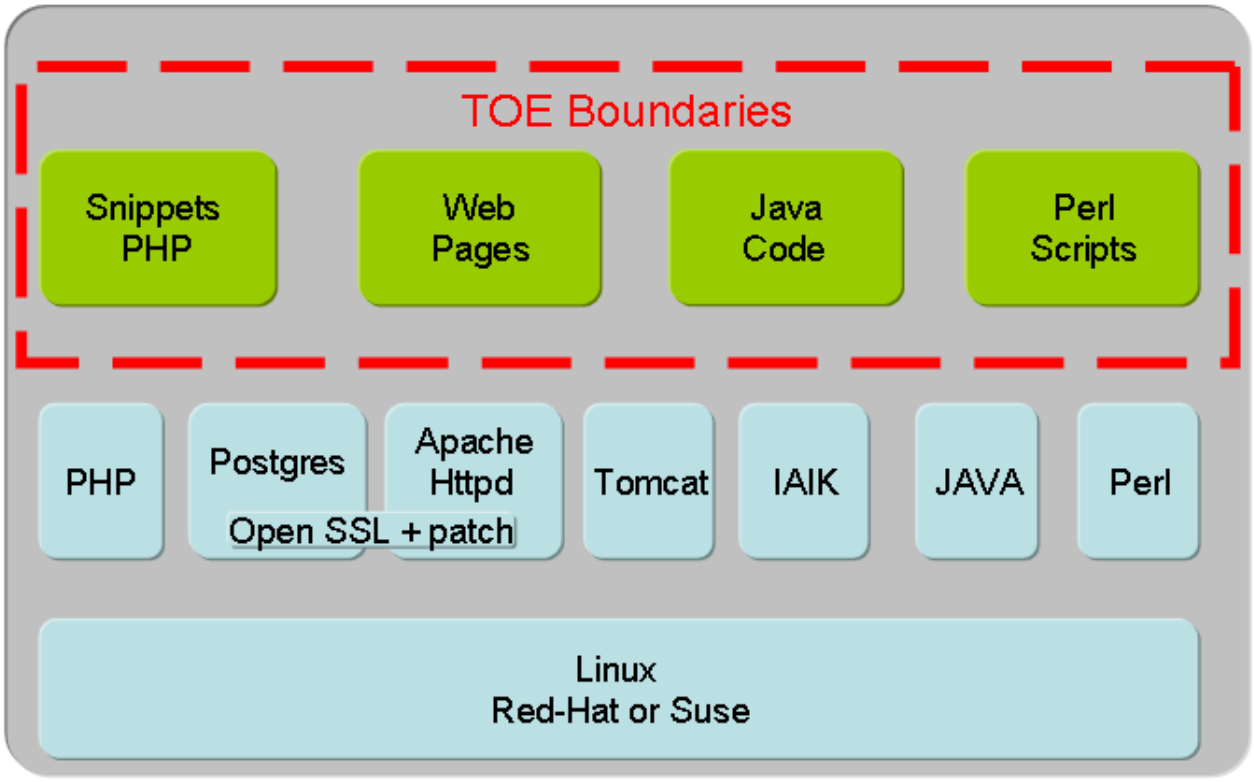


**Figure 3: TOE Boundaries**

### 1.3.4 Evaluated configuration

The evaluated configuration is a single server architecture composed of hardware and software parts. The evaluated configuration is described in the sections below.

#### 1.3.4.1 Server side

**Hardware**

| Component | Identification | Comment |
|---|---|---|
| Physical server | 32 or 64 bit platform with :<br>- at least 4 GB of RAM<br>- at least 10 GB disk available<br>- 2 Ethernet link adaptor | Minimum configuration for physical server where are hosting the virtual machine |
| HSM | TrustWay Box<br>Version S507-RSA 4096 | TrustWay box is using the enforced qualified "TrustWay PCI cryptographic card" |

### Software

The TOE is evaluated in a configuration including the following software:

| Component | Identification | Comment |
|---|---|---|
| **Virtual Machine for Front office functionalities** | VMWare virtual machine | |
| **Virtual Machine for Back office functionalities** | VMWare virtual machine | |
| **Operating system** | Red Hat 6 ES | Hardened version |
| **MetaPKI Pre-requistes** | 4.8.0 | Linux additional components requested for MetaPKI usage |
| **MetaPKI** | 9.2.5 | |
| **SGBDs** | PostgreSQL v9.0.6 | |
| **LDAP** | openldap client v2.4.29 | |

MetaPKI Pre-requisites include the following components:

| Identification | Version |
|---|---|
| apache-ant | 1.8.2 |
| ant-contrib | 1.0b3 |
| java_secure_channel | 0.1.46 |
| httpd | 2.2.22 |
| awstats | 7.0 |
| bison | 2.5 |
| curl | 7.24.0 |
| export_policy | |
| file | 5.10 |
| File_Find | 1.3.1 |
| flex | 2.5.35 |
| fpdf | 17 |
| freetype | 2.4.8 |
| jce_policy-6 | 6 |
| jdk | 6u31 |
| libjpeg | 6b |
| libpng | 1.5.9 |
| ibxml2 | 2.7.8 |
| local_policy | |
| mhash | 0.9.9.9 |
| mpki_p11_engine | |
| net_useragent_detect | 2.5.2 |
| opencryptoki | 2.4 |
| openldap | 2.4.29 |
| openssl | 1.0.0g |
| postgresql | 9.0.6 |
| php | 5.2.17 |

| | |
|---|---|
| readline | 6.2 |
| smarty | 3.1.8 |
| tomcat | 6.0.35 |
| xml_util | 1.2.1 |
| xml_parser | 1.3.4 |
| xml_serializer | 0.20.0 |

#### 1.3.4.2 Client side

**Client workstation configuration (out of the scope of the TOE)**

| Component | Identification | Comment |
|---|---|---|
| Operating system | Windows XP SP3 | |
| Browser | Internet explorer 8.0 | |
| Middleware | Classic Client 6.1_005 | |
| Smart card | Gemalto IAS ECC TPC | |

# 2 Conformance Claim

## 2.1 CC Conformance Claim

The TOE conforms to:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, part 2 extended.
- Common Criteria for Information Technology Security Evaluation, Version 3.1 R3 , part 3 conformant.
- Evaluation Assurance Level 3 augmented with AVA_VAN.3, and ALC_FLR.3.

Note: the EAL chosen for this security target is conformant with French Standard Qualification level.

## 2.2 PP Conformance Claim

This ST is based on the following Protection Profile (PP):

- Certificate Issuing and Management Components (CIMC) Security Level 3 PP, version 1.0, October 31, 2001.

## 2.3 Conformance Rationale

This ST is globally conformant with PP CIMC Level 3:

> This ST includes all of the assumptions, threats, policies, objectives and security requirements defined in CIMC PP to meet Security Level 3. The security requirements have been adapted for CC v3.1. Furthermore this ST does not include additional assumption, threat, policy or objective, except one assumption and one objective that are identified as changes in the text below.
>
> All operations performed on the security requirements for the TOE are within the bounds set by the CIMC PP for Security Level 3, except those mentioning the use of FIPS 140 validated HSMs that are changed by mentions to the French RGS. All the assignment and selection operations on security requirements are indicated in Section 6.1.

Some changes have been made regarding the referenced PP:

- An assumption (A.No Abusive System administrators) and a security objective (O.No Abusive System Administrators) from level 2 have been kept to cover system administrators' trustworthiness: this category of administrator is not under the scope of control of the TOE. A rationale for these additions is provided in section 4.4.

- The system backup role is fulfilled by the Administrator; the system recovery role is fulfilled by the system administrator.
- Some security functional requirements that were defined as SFRs for the environment in PP CIMC have been included as SFRs applicable to the TOE in this ST. The main reason is that these security requirements make the TSF more consistent and actually reinforce the product's security. These SFRs are:
    - FIA_ATD.1 User attribute definition
    - FMT_MSA.1 Management of security attributes
    - FMT_MSA.3 Static attribute initialisation
    - FMT_MTD.1 Management of TSF data
    - FMT_SMR.2 Restrictions on security roles
- The assurance level for this ST is EAL 3 augmented with ALC_FLR.3 and AVA_VAN.3. This assurance level is consistent with the French regulation for qualified IT products at Standard level.

# 3 Security Problem Definition

This section includes the following:

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

## 3.1 Secure Usage Assumptions

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

### 3.1.1 Personnel

**A.Auditors Review Audit Logs**

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

**A.Authentication Data Management**

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

**A.Competent Administrators, Officers and Auditors**

Competent Administrators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

**A.CPS**

All Administrators, 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, 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, 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. (Security Levels 1–3).

**A.No Abusive System administrators**

System administrators are trusted not to abuse their authority.

PP conformity note: This assumption is kept from PP CIMC for levels 1 and 2, and only addresses system administrators, meaning, administrators in charge of the management of the operating system and of the basic services on which the TOE relies. This assumption constitutes an addition with respect to PP CIMC Level 3. Other administrators and users mentioned in this ST operate through the TOE human interfaces.

### 3.1.2 Connectivity

**A.Operating System**

The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the appropriate Security Level identified in this family of PPs. Although the family of PPs does not specifically address the operating system, functions/requirements traditionally attributed to an operating system are distributed throughout this family of PPs in appropriate sections. PKIs incorporating CIMC components that rely on operating systems to provide/enforce these functions/requirements must utilize operating systems with features that counter the perceived threats for the appropriate Security Level identified in this family of PPs

### 3.1.3 Physical

**A.Communications Protection**

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

**A.Physical Protection**

The TOE hardware, software, and firmware critical to security policy enforcement will be protected 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, 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, Officers and Auditors commit errors or hostile actions**

An Administrator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur. (Addressed at Security Levels 3 and 4)

### 3.2.2 System

**T.Critical system component fails**

Failure of one or more system components results in the loss of system critical functionality.

**T.Malicious code exploitation**

An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.

**T.Message content modification**

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

**T.Flawed code**

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

### 3.2.3 Cryptography

**T.Disclosure of private and secret keys**

A private or secret key is improperly disclosed.

**T.Modification of private/secret keys**

A secret/private key is modified.

**T.Sender denies sending information**

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

### 3.2.4 External attacks

**T.Hacker gains access**

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

**T.Hacker physical access**

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

**T.Social engineering**

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

## 3.3 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.~~

Cryptographic functions used to perform all cryptographic operations shall be compliant to [RGS] requirements.

# 4 Security objectives

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

## 4.1 Security Objectives for the TOE

This section includes the security objectives for the TOE, divided among four categories:

- authorized users,
- system,
- cryptography, and
- external attacks.

### 4.1.1 Authorized users

**O.Certificates**

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

### 4.1.2 System

**O.Preservation/trusted recovery of secure state**

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

**O.Sufficient backup storage and effective restoration**

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

### 4.1.3 Cryptography

**O.Non-repudiation**

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

### 4.1.4 External attacks

**O.Control unknown source communication traffic**

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

## 4.2 Security Objectives for the Environment

This section specifies the security objectives for the environment.

### 4.2.1 Non-IT security objectives for the environment

**O.Administrators, Officers and Auditors guidance documentation**

Deter Administrator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.

**O.Auditors Review Audit Logs**

Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk

**O.Authentication Data Management**

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

**O.Communications Protection**

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

**O.Competent Administrators, Officers and Auditors**

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

**O.No Abusive System Administrators**

Use trustworthy System Administrators.

PP conformity note: This objective is kept from PP CIMC for levels 1 and 2, and only addresses system administrators. Please refer to §3.1.1 for more explanations of this particular role.

**O.CPS**

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

**O.Disposal of Authentication Data**

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

**O.Installation**

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

**O.Malicious Code Not Signed**

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

**O.Notify Authorities of Security Issues**

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

**O.Physical Protection**

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

**O.Social Engineering Training**

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

**O.Cooperative Users**

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

**O.Lifecycle security**

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

**O.Repair identified security flaws**

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

### 4.2.2 IT security objectives for the environment

**O.Cryptographic functions**

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

**O.Operating System**

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

**O.Periodically check integrity**

Provide periodic integrity checks on both system and software.

**O.Security roles**

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

**O.Validation of security function**

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

**O.Trusted Path**

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

## 4.3 Security Objectives for both the TOE and the Environment

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

**O.Configuration Management**

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

**O.Data import/export**

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

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

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

**O.Individual accountability and audit records**

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

**O.Integrity protection of user data and software**

Provide appropriate integrity protection for user data and software.

**O.Limitation of administrative access**

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

**O.Maintain user attributes**

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

**O.Manage behavior of security functions**

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

**O.Object and data recovery free from malicious code**

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

**O.Procedures for preventing malicious code**

Incorporate malicious code prevention procedures and mechanisms.

**O.Protect stored audit records**

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

**O.Protect user and TSF data during internal transfer**

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

**O.Require inspection for downloads**

Require inspection of downloads/transfers.

**O.Respond to possible loss of stored audit records**

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

**O.Restrict actions before authentication**

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

**O.Security-relevant configuration management**

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

**O.Time stamps**

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

**O.User authorization management**

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

**O.React to detected attacks**

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

## 4.4 Security Objectives Rationale

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

The only exceptions to this are the addition of the assumption *A.No Abusive System administrators* and of the corresponding security objective for the non-IT environment *O.No Abusive System Administrators*.

The rationale for the additional elements is the following:

*A.No Abusive System administrators* is fully covered by *O.No Abusive System Administrators*.

*A.No Abusive System administrators* establishes that system administrators have a great deal of authority. This is addressed by *O.No Abusive System Administrators*, which ensures that individuals hired to be system administrators are deemed to be trustworthy.

# 5 Extended Components Definition

Extended components have been defined in the CIMC Protection Profile.

Extended security requirements are explicitly identified in the table below:

| Component | Reference to the PP | Instantiation in this ST |
|---|---|---|
| FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin | §6.6 | §6.1.6 |
| FCO_NRO_CIMC.4 Advanced verification of origin | §6.6 | §6.1.6 |
| FCS_CKM_CIMC.5 CIMC private and secret key zeroization | §6.7.4 | §6.1.7.4 |
| FDP_ACF_CIMC.2 User private key confidentiality protection | §6.7.1 | §6.1.7.1 |
| FDP_ACF_CIMC.3 User secret key confidentiality protection | §6.7.3 | §6.1.7.3 |
| FDP_CIMC_BKP.1 CIMC backup and recovery | §6.3 | §6.1.3 |
| FDP_CIMC_BKP.2 Extended CIMC backup and recovery | §6.3 | §6.1.3 |
| FDP_CIMC_CER.1 Certificate Generation | §6.11 | §6.1.11 |
| FDP_CIMC_CRL.1 Certificate revocation list validation | §6.12.1 | §6.1.12 |
| FDP_CIMC_CSE.1 Certificate status export | §6.6.1 | §6.1.7.1 |
| FDP_CIMC_OCSP.1 OCSP basic response validation | §6.12.2 | §6.1.12.2 |
| FDP_ETC_CIMC.5 Extended user private and secret key export | §6.7.5 | §6.1.7.5 |
| FDP_SDI_CIMC.3 Stored public key integrity monitoring and action | §6.7.2 | §6.1.7.2 |
| FMT_MOF_CIMC.3 Extended certificate profile management | §6.8 | §6.1.8 |
| FMT_MOF_CIMC.5 Extended certificate revocation list profile management | §6.9 | §6.1.9 |
| FMT_MOF_CIMC.6 OCSP profile management | §6.10 | §6.1.10 |
| FMT_MTD_CIMC.4 TSF private key confidentiality protection | §6.7.1 | §6.1.7.1 |
| FMT_MTD_CIMC.5 TSF secret key confidentiality protection | §6.7.3 | §6.1.7.1 |
| FMT_MTD_CIMC.7 Extended TSF private and secret key export | §6.7.5 | §6.1.7.1 |
| FPT_CIMC_TSP.1 Audit log signing event | §6.1 | §6.1.1 |

# 6 Security Requirements

## 6.1 TOE Security Functional Requirements

### 6.1.1 Security Audit

**FAU_GEN.1 Audit data generation**

Hierarchical to: No other components.

Dependencies:

- FPT_STM.1 Reliable time stamps

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 the ***Table 1 – Auditable Events and Audit Data*** bellow.

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

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

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

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

| Section/Function | Component | Event | Additional Details |
|---|---|---|---|
| 6.1.1 Security Audit | FAU_GEN.1 Audit data generation | Any changes to the audit parameters, e.g., audit frequency, type of event audited | |
| | | Any attempt to delete the audit log | |
| | FPT_CIMC_TSP.1 Audit log signing event | Audit log signing event | Digital signature, keyed hash, or authentication code shall be included in the audit log. |

| Section/Function | Component | Event | Additional Details |
|---|---|---|---|
| Local Data Entry | | All security-relevant data that is entered in the system | The identity of the data entry individual if the entered data is linked to any other data (e.g., clicking an "accept" button). This shall be included with the accepted data. |
| Remote Data Entry | | All security-relevant messages that are received by the system | |
| Data Export and Output | | All successful and unsuccessful requests for confidential and security relevant information (Security Levels 2, 3, 4) | |
| Private Key Load | | The loading of Component private keys | |
| Private Key Storage | | All access to certificate subject private keys retained within the TOE for key recovery purposes | |
| 6.1.7.2: Public key storage | | All changes to the trusted public keys, including additions and deletions | The public certificate associated with the key |
| 6.1.7.3: Secret key storage | | The manual entry of secret keys used for authentication (Security Levels 3 and 4) | |
| 6.1.7.5: Private and secret key export | FDP_ETC_CIMC.5 Extended user private and secret key export<br>FMT_MTD_CIMC.7 Extended TSF private and secret key export | The export of private and secret keys (keys used for a single session or message are excluded) | |
| 6.1.11: Certificate Registration | FDP_CIMC_CER.1 Certificate Generation | All certificate requests | If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by Officer, etc.). |
| Certificate Status Change Approval | | All requests to change the status of a certificate | Whether the request was accepted or rejected. |
| CIMC Configuration | | Any security-relevant changes to the configuration of the TSF | |
| Certificate Profile Management | FMT_MOF_CIMC.3 Extended certificate profile management | All changes to the certificate profile | The changes made to the profile |

| Section/Function | Component | Event | Additional Details |
|---|---|---|---|
| 6.1.9: Certificate revocation list profile management | FMT_MOF_CIMC.5 Extended certificate revocation list profile management | All changes to the certificate revocation list profile | The changes made to the profile |
| 6.1.10: Online Certificate Status Protocol (OCSP) Profile Management | FMT_MOF_CIMC.6 OCSP profile management | All changes to the OCSP profile | The changes made to the profile |

**Table 1 – Auditable Events and Audit Data**

### FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies:

- FAU_GEN.1 Audit data generation

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.

### FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies:

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

FAU_SEL.1.1 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:

a) ***user identity, subject identity***

b) ***date, user's group, event status, message contents***

Application note:

Some of the terms used in this requirement have a specific meaning in the context of MetaPKI. The mapping between the CC term and the context of MetaPKI is the following:

- user identity = identifier of the user at the origin of the event
- user's group = identifier of the group to which the user belongs
- subject identity = identifier of the functional entity that generated the audit record
- event status = status of the event: success / fail

**FAU_STG.1 Protected audit trail storage**

Hierarchical to: No other components.

Dependencies:

- FAU_GEN.1 Audit data generation

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.

**FAU_STG.4 Prevention of audit data loss**

Hierarchical to:

- FAU_STG.3 Action in case of possible audit data loss

Dependencies:

- FAU_STG.1 Protected audit trail storage

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.

PP Conformity note: In the sentence above, the term "authorized user with special rights" is equivalent to "Auditor".

**FPT_STM.1 Reliable time stamps**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

**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 specified frequency at which the audit log signing event occurs shall be configurable.

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

### 6.1.2 Roles

The ability to perform many of the functions specified in this ST will be allocated to distinct roles to maintain the security of MetaPKI. This subsection defines a set of roles that will be used throughout this document when allocating responsibilities.

A single identity may be assigned multiple roles except where prohibited by the CIMC requirements. Multiple individuals may be assigned to a specific role, as required by the CIMC implementation.

The role definitions are listed below:

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

Application note: An additional role of "system administrator" is defined in section 3.1.1; this role is beyond the scope of control of the TOE.

It is important that one individual cannot perform all the functions specified for a CIMC. One mechanism to deter abuse of power is the separation of CA duties.

**FMT_SMR.2 Restrictions on security roles**

Hierarchical to: FMT_SMR.1 Security roles

Dependencies:

- FIA_UID.1 Timing of identification

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

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

FMT_SMR.2.3 The TSF shall ensure that the conditions **listed above** are satisfied.

a) no identity is authorized to assume both an Administrator and an Officer role ;

b) no identity is authorized to assume both an Auditor and an Officer role; and

c) no identity is authorized to assume both an Administrator and an Auditor role.

Coverage rationale of PP CIMC: this SFR was applicable to the TOE environment in PP CICM. For consistency reasons, it has been included as applicable to the TOE in this ST.

### FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.2 Restrictions on security roles

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in ***Table 2 – Authorized Roles for Management of Security Functions Behavior*** to the authorized roles as specified in ***Table 2 – Authorized Roles for Management of Security Functions Behavior***.

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

| Section/Function | Component | Function/Authorized Role |
|---|---|---|
| ~~Data export and output~~ | | ~~Private key export shall be performed by the Administrator (Security Levels 1 and 2).~~<br><br>~~The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer, Auditor, or Operator. (Security Levels 3 and 4)~~ |
| Certificate Status Change Approval | | Only ~~Officers~~ *Administrators* [1]shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate.<br>~~Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.~~[2] |
| CIMC Configuration | | The capability to configure any TSF functionality shall be restricted to Administrators. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.) |
| Certificate Profile Management | FMT_MOF_CIMC.3 Extended certificate profile management | The capability to modify the certificate profile shall be restricted to Administrators. |
| ~~Revocation Profile Management~~ | | ~~The capability to modify the revocation profile shall be restricted to Administrators.~~[3] |
| Certificate Revocation List Profile Management | FMT_MOF_CIMC.5 Extended certificate revocation list profile management | The capability to modify the certificate revocation list profile shall be restricted to Administrators. |
| Online Certificate Status Protocol (OCSP) Profile Management | FMT_MOF_CIMC.6 OCSP profile management | The capability to modify the OCSP profile shall be restricted to Administrators. |

**Table 2 – Authorized Roles for Management of Security Functions Behavior**

Coverage rationale of PP CIMC: in table above some rows have been kept but have been bared in this ST since they are not applicable to this TOE (MetaPKI does not allow the export of CIMC private keys, and only support one revocation profile).

[1] The ability to configure validation process of the revocation requests is restricted to the Administrators, through the configuration of the validation workflows.
[2] The status of a certificate cannot be set to “on hold", MetaPKI does not support this functionality.
[3] The notion of "revocation profile" does not exist in MetaPKI.

**FMT_MSA.1 Management of security attributes**

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_SMR.2 Restrictions on security roles
- *FMT_SMF.1 Specification of Management Functions*

FMT_MSA.1.1 The TSF shall eSnforce the **CIMC TOE Access Control Policy** to restrict the ability to ***change_default***, ***query***, ***modify***, ***delete*** the security attributes ***entities, users, certificate profiles, workflows*** to **Administrators.**

Coverage rationale of PP CIMC: this SFR was applicable to the TOE environment in PP CICM. For consistency reasons, it has been included as applicable to the TOE in this ST.

**FMT_MSA.3 Static attribute initialisation**

Hierarchical to: No other components.

Dependencies:

- FMT_MSA.1 Management of security attributes
- FMT_SMR.2 Restrictions on security roles

FMT_MSA.3.1 The TSF shall enforce the **CIMC TOE Access Control Policy** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **Administrators** to specify alternative initial values to override the default values when an object or information is created.

Coverage rationale of PP CIMC: this SFR was applicable to the TOE environment in PP CICM. For consistency reasons, it has been included as applicable to the TOE in this ST.

**FMT_MTD.1 Management of TSF data (Iteration 1)**

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.2 Restrictions on security roles
- *FMT_SMF.1 Specification of Management Functions*

FMT_MTD.1.1 The TSF shall restrict the ability to **query**, **modify**, **delete**, ***import / export*** the ***entities, users, certificate profiles*** to ***Administrators***.

Coverage rationale of PP CIMC: this SFR was applicable to the TOE environment in PP CICM. For consistency reasons, it has been included as applicable to the TOE in this ST.

**FMT_MTD.1 Management of TSF data (Iteration 2)**

Hierarchical to: No other components.

Dependencies:

- FMT_SMR.2 Restrictions on security roles
- *FMT_SMF.1 Specification of Management Functions*

FMT_MTD.1.1 The TSF shall restrict the ability to **query**, **delete and export** the **audit logs** to ***Auditors***.

Coverage rationale of PP CIMC: this SFR was applicable to the TOE environment in PP CICM. For consistency reasons, it has been included as applicable to the TOE in this ST.

### 6.1.3 Backup and recovery

*Backup and recovery* includes reconstructing a system in the event of a system failure or other serious error.

In order to be able to recover from failures and other unanticipated undesired events, CIMCs must be able to back up the system. The backup will be used to restore the CIMC to an operational status at a previous point in time. The frequency of performing backups (e.g., hourly, daily, or weekly) is based on the criticality of the application or system.

**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.

### 6.1.4 Access Control

**FDP_ACC.1 Subset access control**

Hierarchical to: No other components.

Dependencies:

- FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the **CIMC TOE Access Control Policy** on.

**Subjects (human users / external entities)**

- Administrators
- Officers
- Auditors
- Final user / certificate holder

Security attributes for subjects: subject identifier, subject internal reference number, membership to a group

**Objects**

- Certificates (operations: request for a certificate, revocation of a certificate, publication / export of a certificate)
- Private Key (operations: request for the generation of a key pair, private key escrow/recovery)
- CRLs (operations: request generation and export/publication (=1 op))
- Audit logs (operations: view/export, delete)

**FDP_ACF.1 Security attribute based access control**

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control

- FMT_MSA.3 Static attribute initialisation

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

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***rules specified in Table 3 – Access control rules***.

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

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

| Section/Function | Component | Event |
|---|---|---|
| Certificate Request Remote and Local Data Entry | | The entry of certificate request data shall be restricted to Officers and the subject of the requested certificate. |
| Certificate Revocation Request Remote and Local Data Entry | | The entry of certificate revocation request data shall be restricted to Officers and the subject of the certificate to be revoked. |
| Data Export and Output | | The export or output of confidential and security-relevant data shall only be at the request of authorized users. |
| Key Generation | | The capability to request the generation of Component keys (used to protect data in more than a single session or message) shall be restricted to Administrators. |
| Private Key Load | | The capability to request the loading of Component private keys into cryptographic modules shall be restricted to Administrators. |
| Private Key Storage | | ~~The capability to request the decryption of certificate subject private keys shall be restricted to Officers.~~<br>The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures.<br>~~At least two Officers or one Officer and an Administrator, Auditor, or Operator shall be required to request the decryption of a certificate subject private key.~~ |
| Trusted Public Key Entry, Deletion, and Storage | | The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administrators. |
| Secret Key Storage | | The capability to request the loading of CIMC secret keys into cryptographic modules shall be restricted to Administrators. |

| Section/Function | Component | Event |
|---|---|---|
| Private and Secret Key Destruction | | The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administrators. |
| Private and Secret Key Export | | The capability to export a component private key shall be restricted to Administrators.<br>The capability to export certificate subject private keys shall be restricted to Officers.<br>The export of a certificate subject private key shall require the authorization of at least two Officers or one Officer and an Administrator or Auditor. |
| Certificate Status Change Approval | | ~~Only Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold.~~<br>~~Only Officers shall be capable of removing a certificate from on hold status.~~<br>~~Only Officers shall be capable of approving the placing of a certificate on hold.~~<br>Only Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate.<br>Only Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate. |

**Table 3 – Access control rules**

### FPT_RVM.1 Non-bypassability of the TSP

This requirement does not exist anymore in CC V3.1; it is covered by assurance component ADV_ARC.1

## 6.1.5 Identification and Authentication

### FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies:

- FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow ***download the CRL, CA and code signing certificates download and OCSP request processing*** on behalf of the user to be performed before the user is authenticated.

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

### FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow ***the download of the CRL, CA and code signing certificates and OCSP request processing*** on behalf of the user to be performed before the user is identified.

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

### FIA_USB.1 User-subject binding

Hierarchical to: No other components.

Dependencies:

- FIA_ATD.1 User attribute definition

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

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***no rules***].

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:

***Upon renewal of the user certificate, the new certificate does not automatically grant the same rights than the previous one; if it is still valid and non-revoked, the former certificate is kept and continues granting the same rights. The same rights have to be propagated by an Administrator.***

### FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- ***Identifier***
- ***Certificate Hash***
- ***Reference number (optional)***
- ***Role***

Application note: MetaPKI implements roles through groups of rights.

Coverage rationale of PP CIMC: this SFR was applicable to the TOE environment in PP CICM. For consistency reasons, it has been included as applicable to the TOE in this ST.

### 6.1.6 Remote Data Entry and Export

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

Hierarchical to: FCO_NRO.2

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 [**no other attributes**] of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

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

**FDP_ITT.1 Basic internal transfer protection**

Hierarchical to: No other components.

Dependencies:

- FDP_ACC.1 Subset access control

FDP_ITT.1.1 The TSF shall enforce the **CIMC TOE Access Control Policy** to prevent the **disclosure and modification** of user data when it is transmitted between physically-separated parts of the TOE.

Coverage rationale of PP CIMC: PP CIMC which was drafted in CC version 2.1 includes two iterations of FDP_ITT.1. The present formulation of the requirement covers these two former iterations:

- iteration 1 : was intended to prevent modification of security relevant user data
- iteration 2 : was intended to prevent disclosure of confidential user data

Coverage rationale of PP CIMC: This requirement is only kept in this ST for the record. It is not applicable to the TOE since the TOE is not made of physically-separated parts.

**FDP_UCT.1 Basic data exchange confidentiality**

Hierarchical to: No other components.

Dependencies:

- [FPT_ITC.1 Inter-TSF confidentiality during transmission, or *FTP_TRP.1 Trusted path*]
- FDP_ACC.1 Subset access control

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

**FPT_ITC.1 Inter-TSF confidentiality during transmission**

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

Refinement: This requirement applies both to the *Core configuration* and the *Enhanced configuration* of the TOE and concerns the Access2MetaPKI interface.

**FPT_ITT.1 Basic internal TSF data transfer protection**

Hierarchical to: No other components.

Dependencies: No dependencies.

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

**FCO_NRO_CIMC.4 Advanced verification of origin**

Hierarchical to: No other components.

Dependencies:

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

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

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

#### 6.1.6.1 Certificate Status Export

**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 [ST 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)~~*].

Application note: The ST should specify the format used to supply certificate status information. If a standard format is not used, then the ST shall include a description of the format.

### 6.1.7 Key Management

This section defines requirements on key management.

Numerous requirements in this section mention "FIPS 140-1 validated cryptographic modules". However, since FIPS 140-1 (and following versions) is not applicable in the French regulation context, this term is changed in the requirements' text by "RGS conformant cryptographic module", meaning cryptographic modules conformant to [RGS] requirements.

#### 6.1.7.1 Private key storage

**FDP_ACF_CIMC.2 User private key confidentiality protection**

Hierarchical to: No other components

Dependencies: No dependencies

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

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

**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~~ *RGS conformant 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~~ *RGS conformant cryptographic module*.

#### 6.1.7.2 Public key storage

**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~~ *RGS conformant 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 any action involving the corrupted public key to be performed**

- **generate a record of this failure in the audit logs]**

Refinement: public keys are only accessed upon the following events:

- Reception of certification requests for a public key being generated outside the TOE (PKCS#10, Acces2MPKI, XKMS)
- Certificate signature by the CA
- Export (publication) of a certificate

#### 6.1.7.3 Secret key storage

**FDP_ACF_CIMC.3 User secret key confidentiality protection**

Hierarchical to: No other components

Dependencies: No dependencies

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

Refinement: The TOE does not store user secret keys but user pass-phrases used in the generation of PKCS#12 encryption keys. This requirement is applicable to these sensitive user data.

**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~~ RGS conformant cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the ~~FIPS 140-1 validated~~ RGS conformant cryptographic module.

Application note : This requirement is not applicable because all TSF secret keys stored within the TOE are stored in RGS conformant cryptographic module.

#### 6.1.7.4 Private and secret key destruction

**FCS_CKM_CIMC.5 CIMC private and secret key zeroization**

Hierarchical to: No other components.

Dependencies:

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

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

Application note: This requirement is applicable to the HSM, which is part of the TOE IT environment. It is ensured by the RGS qualification of the HSM.

#### 6.1.7.5 Private and secret key export

**FDP_ETC_CIMC.5 Extended user private and secret key export**

Hierarchical to: FDP_ETC_CIMC.4

Dependencies: No dependencies

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

**FMT_MTD_CIMC.7 Extended TSF private and secret key export**

Hierarchical to: FMT_MTD_CIMC.6.

Dependencies: No dependencies

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

Refinement: The TOE only exports TSF private keys upon backup of its data base. These keys are stored in the database in an encrypted form.
The TSF secret keys export is not applicable to TOE because it does not use this kind of key.

### 6.1.8 Certificate Profile Management

**FMT_MOF_CIMC.3 Extended certificate profile management**

Hierarchical to: FMT_MOF_CIMC.2

Dependencies:

- FMT_MOF.1 Management of security functions behavior
- FMT_SMR.2 Restrictions on 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.

### 6.1.9 Certificate revocation list profile management

**FMT_MOF_CIMC.5 Extended certificate revocation list profile management**

Hierarchical to: FMT_MOF_CIMC.4

Dependencies:

- FMT_MOF.1 Management of security functions behavior
- FMT_SMR.2 Restrictions on 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.

### 6.1.10 Online Certificate Status Protocol (OCSP) Profile Management

**FMT_MOF_CIMC.6 OCSP profile management**

Hierarchical to: No other components.

Dependencies:

- FMT_MOF.1 Management of security functions behavior
- FMT_SMR.2 Restrictions on 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.

### 6.1.11 Certificate Registration

#### 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 [~~ST 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~~ RGS-approved or recommended algorithm.

### 6.1.12 Certificate Revocation

#### 6.1.12.1 Certificate Revocation List Validation

**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:

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

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

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

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

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

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

#### 6.1.12.2 OCSP Basic Response Validation

**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:

1. The **version** field shall contain a 0.

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

3. The **signatureAlgorithm** field shall contain the OID for a RGS-approved digital signature algorithm.

4. The **thisUpdate** field shall indicate the time at which the status being indicated is known to be correct.

5. The **producedAt** field shall indicate the time at which the OCSP responder signed the response.

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

## 6.2 TOE Security Assurance Requirements

The selected assurance level for this security target is Evaluation Assurance Level 3 augmented with ALC_FLR.3 and AVA_VAN.3 (indicated in bold in the table below).

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

## 6.3 Security Requirements Rationale

### 6.3.1 SFR Dependencies

The following table lists the dependences between SFRs.

| Component | Dependency | Rationale |
|---|---|---|
| FAU_GEN.1 Audit data generation | FPT_STM.1 Reliable time stamps | Statisfied |
| FAU_GEN.2 User identity association | FAU_GEN.1 Audit data generation | Satisfied |
| FAU_SEL.1 Selective audit | FAU_GEN.1 Audit data generation | Satisfied |
| | FMT_MTD.1 Management of TSF data | Satisfied and reinforced by the following specific management SFRs : FMT_MTD_CIMC.4 TSF private key confidentiality protection, FMT_MTD_CIMC.5 TSF secret key confidentiality protection and FMT_MTD_CIMC.7 Extended TSF private and secret key export |
| FAU_STG.1 Protected audit trail storage | FAU_GEN.1 Audit data generation | Satisfied |
| FAU_STG.4 Prevention of audit data loss | FAU_STG.1 Protected audit trail storage | Satisfied |
| FPT_STM.1 Reliable time stamps | No dependencies | |
| FPT_CIMC_TSP.1 Audit log signing event | FAU_GEN.1 Audit data generation | Satisfied |
| | FMT_MOF.1 Management of security functions behavior | Satisfied |
| FMT_SMR.2 Restrictions on security roles | FIA_UID.1 Timing of identification | Satisfied |
| FMT_MOF.1 Management of security functions behavior | FMT_SMR.2 Restrictions on security roles | Satisfied |
| FMT_MSA.1 Management of security attributes | FDP_ACC.1 Subset access control | Satisfied |
| | FMT_SMR.2 Restrictions on security roles | Satisfied |
| | *FMT_SMF.1 Specification of Management Functions* | Dependency not satisfied, but satisfied by the inclusion of FMT_MOF_CIMC.3 Extended certificate profile management, FMT_MOF_CIMC.5 Extended certificate revocation list profile management and FMT_MOF_CIMC.6 OCSP profile management |
| FMT_MSA.3 Static attribute initialisation | FMT_MSA.1 Management of security attributes | Satisfied |

| Component | Dependency | Rationale |
|---|---|---|
| | FMT_SMR.2 Restrictions on security roles | Satisfied |
| FMT_MTD.1 Management of TSF data | FMT_SMR.2 Restrictions on security roles | Satisfied |
| | *FMT_SMF.1 Specification of Management Functions* | Dependency not satisfied, but satisfied by the inclusion of FMT_MOF_CIMC.3 Extended certificate profile management, FMT_MOF_CIMC.5 Extended certificate revocation list profile management and FMT_MOF_CIMC.6 OCSP profile management |
| FDP_CIMC_BKP.1 CIMC backup and recovery | FMT_MOF.1 Management of security functions behavior | Satisfied |
| FDP_CIMC_BKP.2 Extended CIMC backup and recovery | FDP_CIMC_BKP.1 CIMC backup and recovery | Satisfied |
| FDP_ACC.1 Subset access control | FDP_ACF.1 Security attribute based access control | Satisfied |
| FDP_ACF.1 Security attribute based access control | FDP_ACC.1 Subset access control | Satisfied |
| | FMT_MSA.3 Static attribute initialisation | Satisfied |
| FPT_RVM.1 Non-bypassability of the TSP | | Requirement kept from the PP for compatibility reasons. |
| FIA_UAU.1 Timing of authentication | FIA_UID.1 Timing of identification | Satisfied |
| FIA_UID.1 Timing of identification | No dependencies | |
| FIA_USB.1 User-subject binding | FIA_ATD.1 User attribute definition | Satisfied |
| FIA_ATD.1 User attribute definition | No dependencies | |
| FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin | FIA_UID.1 Timing of identification | Satisfied |
| FDP_ITT.1 Basic internal transfer protection | FDP_ACC.1 Subset access control | Satisfied |
| FDP_UCT.1 Basic data exchange confidentiality | FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path | Satisfied by FPT_ITC.1 Inter-TSF confidentiality during transmission |
| | FDP_ACC.1 Subset access control | Satisfied |
| FPT_ITC.1 Inter-TSF confidentiality during transmission | No dependencies | |
| FPT_ITT.1 Basic internal TSF data transfer protection | No dependencies | |

| Component | Dependency | Rationale |
|---|---|---|
| FCO_NRO_CIMC.4 Advanced verification of origin | FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin | Satisfied |
| FDP_CIMC_CSE.1 Certificate status export | No dependencies | |
| FDP_ACF_CIMC.2 User private key confidentiality protection | No dependencies | |
| FMT_MTD_CIMC.4 TSF private key confidentiality protection | No dependencies | |
| FDP_SDI_CIMC.3 Stored public key integrity monitoring and action | No dependencies | |
| FDP_ACF_CIMC.3 User secret key confidentiality protection | No dependencies | |
| FMT_MTD_CIMC.5 TSF secret key confidentiality protection | No dependencies | |
| FCS_CKM_CIMC.5 CIMC private and secret key zeroization | *FCS_CKM.4 Cryptographic key destruction* | Not satisfied. Requirement applicable to the RSG conformant HSM. |
| | *FDP_ACF.1 Security attribute based access control* | Not satisfied. Requirement applicable to the RSG conformant HSM. |
| FDP_ETC_CIMC.5 Extended user private and secret key export | No dependencies | |
| FMT_MTD_CIMC.7 Extended TSF private and secret key export | No dependencies | |
| FMT_MOF_CIMC.3 Extended certificate profile management | FMT_MOF.1 Management of security functions behavior | Satisfied |
| | FMT_SMR.2 Restrictions on security roles | Satisfied |
| FMT_MOF_CIMC.5 Extended certificate revocation list profile management | FMT_MOF.1 Management of security functions behavior | Satisfied |
| | FMT_SMR.2 Restrictions on security roles | Satisfied |
| FMT_MOF_CIMC.6 OCSP profile management | FMT_MOF.1 Management of security functions behavior | Satisfied |
| | FMT_SMR.2 Restrictions on security roles | Satisfied |
| FDP_CIMC_CER.1 Certificate Generation | No dependencies | |
| FDP_CIMC_CRL.1 Certificate revocation list validation | No dependencies | |
| FDP_CIMC_OCSP.1 OCSP basic response validation | No dependencies | |

### 6.3.2 SFR from PP CIMC unapplicable to this ST

The table below provides a rationale for the SFR that where defined in the PP and that are considered as not applicable to this ST.

| Component | Status | Rationale |
| --- | --- | --- |
| FDP_ITT.1 Basic internal transfer protection | Not applicable | This SFR only applies to TOEs involving physically separated parts. The evaluated configuration only includes one server. |

# 7 TOE Summary Specifications

## 7.1 TOE Security Functions

### 7.1.1 Security Audit

#### Operations logging

The TOE generates logs upon occurrence of actions performed by a user through the application interface (application log)

For each traced operation, the TOE records:

- the identity of the subject been at the origin of the logged operation
- the date and time the operation occurred

The time reference of the TOE is the system time of the back-office server.

#### Log selection

The TOE provides a user interface allowing to select the logs to be displayed.

#### Log integrity protection

The protection of the logs integrity is ensured by a twofold mechanism:

1) Each TOE log entry is chained with all preceding entries (hash computation).
2) The TOE log entries are periodically signed. This log signing mechanism is triggered periodically. This period is configurable under control of an authorized administrator.

#### Prevention of data loss

The TOE performs a supervision of the remaining disk space.

When a configurable threshold is reached, the TOE stops itself its operations and alerts the administrators.

### 7.1.2 Roles

The TOE provides a role management function allowing the definition of distinct roles.

The roles supported by the TOE are composed of one or several privileges.

These privileges grant the user the authorization to perform a given action on the TOE including administration actions and TOE configuration actions.

A given user can be bound to a unique role.

When creating a new user the TOE provides a restrictive value to the user's attributes in the sense the user is not assigned to any role. His role must be explicitly specified by an Administrator.

### 7.1.3 Backup and recovery

The TOE implements a backup/restore function accessible to the Administrators.

The output data of the backup function is ciphered and its integrity is protected by a MAC.

The recovery can only be performed upon a successful check of this MAC.

### 7.1.4 Access control

TOE access control is implemented using a RBAC model involving each functional entity of the TOE and roles.

Access Rules will be achieved by:

- an appropriate configuration of the allowed actions for each functional entity and
- a proper role definition specifying the accessible entities for that role
- the assignment of a role to a user.

### 7.1.5 Identification and authentication

The TOE performs the identification and authentication of users (i.e. the binding of a user to a subject) as follows:

- For a user having an operational authentication certificate: using the hash of the subject's certificate to retrieve the user's unique identifier. The issuing CA of that certificate must either be a PKI's internal user's CA, or belong to the list of trusted third party CAs.
- For other users: using the holder identifier (authentication is then done through a mechanism of answer to personal questions)

The only operations allowed to a user without authentication nor identification are:
- download of the CRL
- CA and code signing certificates download
- OCSP request processing

The authorized Administrators may manage the users' profiles (creation, update and deletion) through a proper interface.

Along with the user's identity, the TOE maintains the following security attributes:

- identifier
- authentication certificate hash
- reference number (which is not applicable for third party CA issued authentication certificates)
- role

### 7.1.6 Remote Data Entry and Export

#### Protection of internal and external interfaces

All communications between the TOE and external IT systems are protected in confidentiality and integrity using TLS protected communication channels.

Export of subjects certificates statuses (that are public information) are performed through an HTTP communication channel (excepted OCSP and CRL data exchanges).

All communications between the TOE components are protected in confidentiality and integrity using TLS protected communication channels.

#### Proof of origin of imported data

The TLS protocol in full handshake mode ensures the proof of the message origin by a combination of:

- Authentication of the requesting user
- Integrity protection of the message transferred.

This provides a proof of origin of transferred data.

Certificate status information and other relevant security data can only be updated by authenticated users. The identity of that user (proved by the authentication) is bound to the operation performed by that user which ensures the proof of origin of the action.

#### Proof of origin of exported data

The TOE is compliant with RFC 5280 (for X.509 PKI Certificate and CRL) and the RFC 2560 (for OCSP protocol), therefore it provides proof of the origin of the certificates, CRLs and OCSP responses.

### 7.1.7 Key Management

#### Subject private key escrow and recovery

The TOE implements a key escrow and recovery function involving a specific Long Term Private Key Protection Key that is operated in an RGS conformant HSM.

The TOE ensures the export of private keys that have been generated centrally under an encrypted form.

This export can be done through a key withdrawal interface or through the escrow recovery interface.

The withdrawal interface that supports two encryption mechanisms, depending on the media that will hold the key:

- PKCS#12 files: the private key is encrypted using a user secret (from which a secret encryption key is derived, according to PKCS#5);
- Smart card: the private key is exported wrapped by the HSM using a specific transport public key, the corresponding private key having been generated in the smartcard.

The escrow recovery interface supports only the PKCS#12 format.

#### Integrity check of stored public keys

The public keys stored within the TOE are protected against undetected modification using a MAC, the key used for the MAC is stored and operated in a RGS conformant HSM.

A verification of that MAC is performed prior to use the public key or authorize its transfer to another entity. Any failed verification causes the generation of an audit trail.

#### Protection of secret and private keys and user sensitive data

The TOE relies on a RGS compliant HSM to protect the secret keys (TSF secret keys) involved in the protection of internal and user sensitive data.

The private keys used for the internal protection of the TOE are held and operated in a by an RGS conformant HSM.

The TOE implements a mechanism to protect the secrets involved in the generation of PKCS#12 files. The user pass-phrases that are stored within the TOE are encrypted by the means of a RGS compliant HSM.

The TOE relies on a RGS compliant HSM to provide the ability to zeroize plaintext secret and private keys.

Note: The TSF private and secret keys stored in the HSM are backuped using the trusted HSM backup recovery function. The protection of that backup is HSM dependent (beyond the scope of this ST).

### 7.1.8 Certificate Profile Management

The TOE provides the Administrators with an interface allowing them to manage the certificate profiles.

### 7.1.9 Information on Certificates statuses and Related Management

The TOE generates

- CRLs in accordance with RFC 5280
- OCSP responses in accordance with IETF RFC 2560.

The TOE provides the Administrators with an interface allowing them to manage:

- The certificate revocation profiles (CRL publication period).
- The OCSP responders configuration

### 7.1.10 Registration Authority

The TOE generates certificates compliant with ANSI X509 and RFC-5280 according to the chosen certificate profile.

The TOE accepts PKCS#10 and SPKAC certification requests that include a proof of possession of the private key.

## 7.2 TOE Summary Specifications Rationale

| Security functional requirement | Security Function | Rationale |
|---|---|---|
| FAU_GEN.1 Audit data generation | Security Audit | The TOE generates logs upon occurrence of actions performed by a user : through the application interface (application log)<br>Since the system administrators of the TOE are assumed to be non-threatened agents, system logs are not considered in the rest of this rational |
| FAU_GEN.2 User identity association | Security Audit | For each action, the subject's identity is bound to the corresponding log entry. |
| FAU_SEL.1 Selective audit | Security Audit | The TOE provides a user interface allowing to select the logs to be displayed. |
| FAU_STG.1 Protected audit trail storage | Security Audit | Each TOE log entry is chained with all preceding entries (hash computation).<br>The TOE log entries are periodically signed. |
| FAU_STG.4 Prevention of audit data loss | Security Audit | The TOE performs a supervision of the remaining disk space.<br>When a configurable threshold is reached, the TOE stops itself its operations and alerts the administrators. |
| FPT_STM.1 Reliable time stamps | Security Audit | Each TOE log entry is time stamped using the operating system time of the back office hosting machine.<br>The trust in this system time relies on system administrator trustworthiness. |
| FPT_CIMC_TSP.1 Audit log signing event | Security Audit | The TOE log signing mechanism is triggered periodically. This period is configurable under control of an authorized administrator. |
| FMT_SMR.2 Restrictions on security roles | Roles | The TOE implements a role management function allowing the definition of distinct roles.<br>A user can be bound to a unique role. |
| FMT_MOF.1 Management of security functions behavior | Roles | The roles supported by the TOE are composed of one or several privileges.<br>These privileges grant the user the authorization to perform a given action on the TOE including administration actions and TOE configuration actions. |
| FMT_MSA.1 Management of security attributes | Roles | The roles supported by the TOE are composed of one or several privileges.<br>These privileges grant the user the authorization to perform a given action on the TOE including administration actions and TOE configuration actions. |
| FMT_MSA.3 Static attribute initialisation | Roles | When creating a new user the TOE provides a restrictive value to the user's attributes in the sense the user is not assigned to any role. His role must be explicitly specified by an Administrator. |
| FMT_MTD.1 Management of TSF data | Roles | One of the privileges **eligible** to roles is the capability to change TOE configuration data that includes TSF. data |

| Security functional requirement | Security Function | Rationale |
|---|---|---|
| FDP_CIMC_BKP.1 CIMC backup and recovery | Backup and recovery | The TOE implements a backup/restore function accessible to the Administrators. |
| FDP_CIMC_BKP.2 Extended CIMC backup and recovery | Backup and recovery | The output data of the backup function is ciphered and its integrity is protected by a MAC.<br>The recovery can only be performed upon a successful check of this MAC. |
| FDP_ACC.1 Subset access control | Access control | TOE access control is implemented using a RBAC model involving each functional entity of the TOE and roles.<br>Subjects are authorized to perform actions on objects though the functions allowed by functional entities they gain access to, according to the role the subjects belongs. |
| FDP_ACF.1 Security attribute based access control | Access control | TOE. access control is implemented using a RBAC model involving each functional entity of the TOE and roles.<br>Subjects are authorized to perform action on objects though the functions allowed by functional entities they gain access to according to the role the subjects belongs.<br>Access Rules will be achieved by<br>1) an appropriate configuration of the allowed actions for each functional entity and<br>2) a proper role definition specifying the accessible entities for that role<br>3) the assignment of a role to a user. |
| FPT_RVM.1 Non-bypassability of the TSP | | This requirement from PP CIMC does not exit anymore in CC V3.1. |
| FIA_UAU.1 Timing of authentication | Identification and authentication | The only operations allowed to a user without authentication are:<br>- download of the CRL<br>- CA and code signing certificates download<br>- OCSP request processing |
| FIA_UID.1 Timing of identification | Identification and authentication | The only operations allowed to a user without identification are:<br>- download of the CRL<br>- CA and code signing certificates download<br>- OCSP request processing |

| Security functional requirement | Security Function | Rationale |
|---|---|---|
| FIA_USB.1 User-subject binding | Identification and authentication | The binding of a user to a subject is done :<br>- For a user having an operational authentication certificate: using the hash of the subject's certificate to retrieve the user's unique identifier. The issuing CA of that certificate must either be a PKI's internal user's CA, or belong to the list of trusted third party CAs.<br>- For other users: using the holder identifier (authentication is then done through a mechanism of answer to personal questions) |
| FIA_ATD.1 User attribute definition | Identification and authentication | Along with the user's identity, the TOE maintains the following security attributes to enforce the SFRs:<br>- identifier<br>- authentication certificate hash<br>- reference number (optional)<br>- role<br>These attributes are managed through the functions of the TOE for user creation, update and deletion.<br>Note : the reference number is not applicable for third party CA issued authentication certificates. |
| FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin | Remote Data Entry and Export | Certificate status information and other relevant security data can only be updated by authenticated users. The identity of that user (proved by the authentication) is bound to the operation performed by that user which ensures the proof of origin of the action. |
| FDP_ITT.1 Basic internal transfer protection | Remote Data Entry and Export | All communications between the TOE components are protected in confidentiality and integrity using TLS protected communication channels. |
| FDP_UCT.1 Basic data exchange confidentiality | Remote Data Entry and Export | All communications between the TOE components are protected in confidentiality and integrity using TLS protected communication channels.<br>All communications between the TOE and external IT systems are protected in confidentiality and integrity using TLS protected communication channel, excepted OCSP and CRL data exchanges which rely on HTTP but do not contain user confidential data. |
| FPT_ITC.1 Inter-TSF confidentiality during transmission | Remote Data Entry and Export | All communications between the TOE and external IT systems are protected in confidentiality and integrity using TLS protected communication channel, excepted OCSP and CRL data exchanges, that rely on HTTP but do not contain TSF data. |
| FPT_ITT.1 Basic internal TSF data transfer protection | Remote Data Entry and Export | All communications between the TOE components are protected in confidentiality and integrity using TLS protected communication channels. |

| Security functional requirement | Security Function | Rationale |
|---|---|---|
| FCO_NRO_CIMC.4 Advanced verification of origin | Remote Data Entry and Export | The external interfaces used to send the initial certificates registrations are protected using the TLS protocol in full handshake mode . This protocol ensures the proof of the message origin by a combination of:<br>- Authentication of the requesting user Integrity protection of the message transferred.<br>The identity of the user (proved by the authentication) is bound to the operation performed by that user. This ensures the proof of origin of the transferred data |
| FDP_CIMC_CSE.1 Certificate status export | Certificate Status Export | As required in this SFR, the TOE is compliant with RFC 5280 (for X.509 PKI Certificate and CRL Profile management) and the RFC 2560 (for OCSP protocol). |
| FDP_ACF_CIMC.2 User private key confidentiality protection | Key Management | The TOE implements a key escrow and recovery function involving a specific Long Term Private Key Protection Key that is operated in an RGS conformant HSM. |
| FMT_MTD_CIMC.4 TSF private key confidentiality protection | Key Management | The private keys used for the internal protection of the TOE are held and operated in a by an RGS conformant HSM. |
| FDP_SDI_CIMC.3 Stored public key integrity monitoring and action | Key Management | The public keys stored within the TOE are protected against undetected modification using an MAC, the key used for the MAC is stored and operated in a RGS conformant HSM.<br>A verification of that MAC is performed prior to use the public key or authorize its transfer to another entity.<br>Any failed verification causes the generation of an audit trail. |
| FDP_ACF_CIMC.3 User secret key confidentiality protection | Key Management | The TOE implements a mechanism to protect the secrets involved in the generation of PKCS#12 files.<br>The user pass-phrases that are stored within the TOE are encrypted by the means of a RGS compliant HSM. |
| FMT_MTD_CIMC.5 TSF secret key confidentiality protection | Key Management | The TOE relies on a RGS compliant HSM to protect the secret keys (TSF secret keys) involved in the protection of internal and user sensitive data. |
| FCS_CKM_CIMC.5 CIMC private and secret key zeroization | Key Management | The TOE relies on a RGS compliant HSM to provide the ability to zeroize plaintext secret and private keys. |

| Security functional requirement | Security Function | Rationale |
|---|---|---|
| FDP_ETC_CIMC.5 Extended user private and secret key export | Key Management | The TOE ensures the export of private keys that have been generated centrally under an encrypted form. This export can be done through a key withdrawal interface or through the escrow recovery interface.<br><br>The withdrawal interface that supports two encryption mechanisms, depending on the media that will held the key:<br>- PKCS#12 files: the private key is encrypted using a user secret (from which a secret encryption key is derived, according to PKCS#5);<br>- Smart card: the private key is exported wrapped by the HSM using a specific transport public key, the corresponding private key having been generated in the smartcard.<br>The escrow recovery interface supports only the PKCS#12 format. |
| FMT_MTD_CIMC.7 Extended TSF private and secret key export | Key Management | The TSF private and secret keys stored in the HSM are backuped using the trusted HSM backup recovery function. The protection of that backup is HSM dependent (beyond the scope of this ST).<br>Other keys can only be exported along with the backup/recovery function which is ciphered by an HSM protected secret key. |
| FMT_MOF_CIMC.3 Extended certificate profile management | Certificate Profile Management | The TOE provides the Administrators with an interface allowing to manage the certificate profiles. |
| FMT_MOF_CIMC.5 Extended certificate revocation list profile management | Information on Certificates statuses and Related Management | The TOE provides the Administrators with an interface allowing them to manage the certificate revocation profiles (CRL publication period). |
| FMT_MOF_CIMC.6 OCSP profile management | Information on Certificates statuses and Related Management | The TOE provides the Administrators with an interface allowing them to manage the configuration of the OCSP responders.<br>(note: the term OSCP profile is kept in the requirement for PP CIMC conformance) |
| FDP_CIMC_OCSP.1 OCSP basic response validation | Information on Certificates statuses and Related Management | The TOE generates OCSP responses in accordance with IETF RFC 2560 |
| FDP_CIMC_CER.1 Certificate Generation | Registration Authority | The TOE generates certificates compliant with ANSI X509 and RFC-5820 according to the chosen certificate profile. The TOE accepts PKCS#10 and SPKAC certification requests that include a proof of possession of the private key. |
| FDP_CIMC_CRL.1 Certificate revocation list validation | Registration Authority | The TOE generates CRLs in accordance with ANSI X509 and IETF RFC 5280 |

# 8 Access Control Policies

## 8.1 CIMC IT Environment Access Control Policy

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

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

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

Subject identification includes:

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

Access type, with explicit allow or deny:

- Read
- Write
- Execute

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

## 8.2 CIMC TOE Access Control Policy

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

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

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

Subject identification includes:

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

Access type, with explicit allow or deny:

- Read
- Write
- Execute

# 9 Glossary of Terms and Acronyms

## 9.1 Glossary of Terms

Most of the terms in this glossary are come from PP CIMC, and some are specific to this ST. The terms that are specific to this ST are indicated in italic.

**Authentication code**

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

**Certificate subject private keys**

Private keys corresponding to the public keys contained in certificates issued by the CIMC where:

- the private key is held by the CIMC solely to enable key recovery; or
- the CIMC generates a public/private key pair and the private key is only held by the CIMC until the certificate subject has received it.

**CIMC**

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

**CIMC boundary**

An explicitly defined contiguous perimeter that establishes the physical bounds of a CIMC.

**Component keys**

Keys, other than CIMS personnel keys, which are used by the CIMC. CIMCs shall use Component keys to sign certificates and certificate status information. Component public/private key pairs may also be used in key agreements, for signing audit logs and system backups and for ensuring the integrity of transmitted or stored data. Component secret keys may be used to encrypt CIMC stored or transmitted data and to compute authentication codes.

**Compromise**

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

**Confidentiality:**

The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

**Critical security parameter**

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

**Cryptographic key (key)**

A parameter used in conjunction with a cryptographic algorithm that determines:

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

**Cryptographic key component (key component)**

A parameter used in conjunction with other key components in a RGS-approved or recommended security method to form a plaintext cryptographic key or perform a cryptographic function.

**Digital signature**

A non-forgeable transformation of data that allows proof of the source (with nonrepudiation) and verification of the integrity of that data.

**Encrypted key**

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

**Error detection code**

A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

**RGS-Approved or recommended mode of operation**

A mode that employs only the operation of RGS approved or recommended security methods.

**RGS-approved or recommended security method**

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

**Firmware**

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

**Hardware**

The physical equipment used to process programs and data in a CIMC.

**Integrity**

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

**Key encrypting key**

A cryptographic key that is used for the encryption or decryption of other keys.

**Key management**

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

**Password**

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

**Personal Identification Number (PIN)**

A 4 or more character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

**Physical protection**

The safeguarding of a CIMC, cryptographic keys, or other CSPs using physical means.

**Plaintext key**

An unencrypted cryptographic key.

**Private key**

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

**Protection Profile**

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

**Public key**

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

**Public key certificate**

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

**Public key (asymmetric) cryptographic algorithm**

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

***RGS conformant cryptographic module***

A cryptographic module conformant to [RGS] requirements for the security level expected for the CIMC. The security levels are defined in the certification policies templates (Politique de certification type

**Secret key**

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

**Secret key (symmetric) cryptographic algorithm**

A cryptographic algorithm that uses a single, secret key for both encryption and decryption.

**Security policy**

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

**Software**

The programs and associated data that can be dynamically written and modified.

**Split knowledge**

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

**Target of Evaluation (TOE)**

An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

**TOE Security Functions (TSF)**

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

**TOE Security Policy (TSP)**

A set of rules that regulate how assets are managed, protected and distributed within a TOE.

**Trusted path**

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

**User**

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

**Zeroization**

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

## 9.2 Acronyms

The acronyms specified below are mainly originated from CIMC PP. The acronyms that are specific to this ST are indicated in *italic*.

| | |
|---|---|
| *API* | *Application Programming Interface* |
| *ANSSI* | *Agence Nationale pour la Sécurité des Systèmes d'Information – French Network and Information Security Agency* |
| ANSI | American National Standards Institute |
| CA | Certification Authority |
| CC | Evaluation Criteria for Information Technology Security (Common Criteria) |
| CIMC | Certificate Issuing and Management Component |
| CIMS | Certificate Issuing and Management System |
| *CM* | *Configuration Management* |
| CP | Certificate Policy |
| CPS | Certification Practices Statement |
| CRL | Certificate Revocation List |
| *DMZ* | *Demilitarized zone* |

| | |
|---|---|
| EAL | Evaluation Assurance Level |
| *ETSI* | *European Telecommunication Standards Institute* |
| *HSM* | *Hardware Security Module* |
| *HTTP* | *HyperText Transmission Protoco* |
| *HTTPS* | *HyperText Transmission Protocol with Security* |
| I&A | identification and authentication |
| IEC | International Electrotechnical Commission |
| *IETF* | *Internet Engineering Task Force* |
| IS | Information Security |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITU | International Telecommunication Union |
| ITU-T | ITU Telecommunication Standardization Sector |
| *LDAP* | *Lightweight Directory Access Protocol* |
| *LRA* | *Local Registration Authority* |
| *MAC* | *Message Authentication Code* |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| *PKCS* | *Public Key Cryptographic Standards* |
| PP | Protection Profile |
| RA | Registration Authority |
| RFC | Request For Comment |
| *RP* | *Relying Parties* |
| *SFR* | *Security Functional Requirement* |
| SFP | Security Function Policy |
| *SMTP* | *Simple Mail Transfer Protocol* |
| *SPKAC* | *Signed Public Key And Challenge* |
| *SSO* | *Single Sign On* |
| ST | Security Target |
| TOE | Target of Evaluation |
| *TS* | *Technical Standard* |

| | |
| --- | --- |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| *XKMS* | *XML Key Management Specification* |

End of the document