

IST-2001-34340

D8.2 Security functional  
requirements mapping on  
modules

Distribution List:

Project Partners

Authors:

Christophe ANIER, Lionel VAN AERTRYCK **AQL**

Distribution List:

Project Partners

Authorised by:

Yann Fraval, **GIP-MDS**

Date of Issue:

January 15th, 2003

Issue:

1.00

File Name:

EUPKI-WP8-D8.2-1.00.DOC

Work Package:

WP8 Homologation issues and security guidelines

Deliverable Number:

D8.2

Deliverable Type:

Public

Deliverable Nature:

Total Number of Pages:

48

Contact Details for EUPKI:

Christophe ANIER  
mail: [Christophe.anier@aql.fr](mailto:Christophe.anier@aql.fr)

## Table Of Contents

<b>1</b>	<b>DOCUMENT CONTROL</b> .....	<b>3</b>
1.1	ABSTRACT .....	3
1.2	KEYWORDS .....	3
<b>2</b>	<b>MANAGEMENT OVERVIEW</b> .....	<b>4</b>
2.1	EXECUTIVE SUMMARY .....	4
2.2	SCOPE STATEMENT .....	4
<b>3</b>	<b>INTRODUCTION AND GLOSSARY</b> .....	<b>5</b>
3.1	INTRODUCTION .....	5
3.2	CORRESPONDENCE BETWEEN DESCRIPTION LEVELS .....	5
3.3	STRUCTURE OF THE DOCUMENT .....	6
3.4	GLOSSARY .....	7
<b>4</b>	<b>SECURITY FUNCTIONS</b> .....	<b>8</b>
4.1.1	<i>Certification Authority</i> .....	8
4.1.2	<i>Registration Authority</i> .....	10
4.1.3	<i>Central KGS</i> .....	12
4.1.4	<i>User KGS</i> .....	13
<b>5</b>	<b>SECURITY FUNCTIONAL REQUIREMENTS</b> .....	<b>14</b>
5.1	SFR FOR CERTIFICATION AUTHORITY .....	15
5.1.1	<i>Security Audit</i> .....	15
5.1.2	<i>Communication</i> .....	15
5.1.3	<i>Cryptographic support (CSP)</i> .....	16
5.1.4	<i>User data protection</i> .....	16
5.1.5	<i>Identification and authentication</i> .....	17
5.1.6	<i>Security management</i> .....	18
5.1.7	<i>Protection of the security functions</i> .....	19
5.1.8	<i>Trusted channels</i> .....	20
5.1.9	<i>Synthesis</i> .....	21
5.2	SFR FOR THE REGISTRATION AUTHORITY .....	22
5.2.1	<i>Security Audit</i> .....	22
5.2.2	<i>Communication</i> .....	23
5.2.3	<i>User data protection</i> .....	24
5.2.4	<i>Identification and authentication</i> .....	25
5.2.5	<i>Security management</i> .....	26
5.2.6	<i>Protection of the security functions</i> .....	27
5.2.7	<i>Trusted channels</i> .....	28
5.2.8	<i>Synthesis</i> .....	29
5.3	SFR FOR THE KEY GENERATION SYSTEM .....	30
5.3.1	<i>Security Audit</i> .....	30
5.3.2	<i>Communication</i> .....	30
5.3.3	<i>Cryptographic support</i> .....	31
5.3.4	<i>User data protection</i> .....	31
5.3.5	<i>Identification and authentication</i> .....	32
5.3.6	<i>Security management</i> .....	33
5.3.7	<i>Protection of the security functions</i> .....	34
5.3.8	<i>Trusted channels</i> .....	35
5.3.9	<i>Synthesis</i> .....	36

## 1 Document Control

<i>Issue</i>	<i>Date of Issue</i>	<i>Comments</i>
0.01	9 July, 2002	Creation
0.02	30 September, 2002	Mapping between SF and SFR
0.03	4 october, 2002	Technical check and complements
0.04	7 november, 2002	Internal modification
0.05	25 november, 2002	Integration of the modifications resulting from the documents D4.2 and D4.3

### 1.1 Abstract

The purpose of the deliverable D8.2 'Security functional requirements mapping' is to help the developers to establish the mapping between identified Security Functional Requirements and modules identified within task d4.1.

### 1.2 Keywords

EUPKI	EUPKI, the libre software Public Key Infrastructure (project name)
WP4	Work Package 4
GIP-MDS	Groupement d'Intérêt Public Modernisation des Déclarations Sociales
CGE&Y	Cap Gemini Ernst & Young
AQL	Alliance Qualité Logiciel

## 2 Management Overview

### 2.1 Executive Summary

This document provides information about security functional requirements ...

### 2.2 Scope Statement

PKI functionalities used to produce the present reports are those described in deliverable d4.1 "global architecture", Version 1.0.

This document refers to the following external documents:

Reference	Document
D3.6	Perimeter and requirements of the project
D4.1	Architectural Specification
[PP CRPKI]	<b>Cryptographic Resource for Public Key Infrastructure Protection Profile,</b> v2.6 <a href="http://www.scssi.gouv.fr/fr/confiance/documents/PPnc0003.pdf">www.scssi.gouv.fr/fr/confiance/documents/PPnc0003.pdf</a>
[PP PKI]	<b>Public Key Infrastructure Protection Profile,</b> v2.6 <a href="http://www.scssi.gouv.fr/fr/confiance/documents/PPnc0004.pdf">www.scssi.gouv.fr/fr/confiance/documents/PPnc0004.pdf</a>
[PP RA]	<b>Registration Authority Protection Profile,</b> v2.6 <a href="http://www.scssi.gouv.fr/fr/confiance/documents/PPnc0005.pdf">www.scssi.gouv.fr/fr/confiance/documents/PPnc0005.pdf</a>
[PP CA]	<b>Certification Authority Protection Profile,</b> v2.6 <a href="http://www.scssi.gouv.fr/fr/confiance/documents/PPnc0006.pdf">www.scssi.gouv.fr/fr/confiance/documents/PPnc0006.pdf</a>
[CC-01]	<b>Common Criteria for Information Technology Security Evaluation</b> CCIMB-99-031, Part 1: Introduction and general model, Version 2.1, August 1999.
[CC-02]	<b>Common Criteria for Information Technology Security Evaluation</b> CCIMB-99-032, Part 2: Security functional requirements, Version 2.1, August 1999.
[CC-03]	<b>Common Criteria for Information Technology Security Evaluation</b> CCIMB-99-033, Part 3: Security assurance requirements, Version 2.1, August 1999.

### 3 Introduction and Glossary

#### 3.1 Introduction

The approach that should have been followed to identify and select appropriate security functional requirements consists in defining a Security Target for the whole system (PKI) and a set of 3 Security Targets (one for each functional block of the PKI: CA, RA and KGS).

Within these Security Targets, the Security Functional Requirements defined at the higher level (PKI level) must be distributed onto the functional blocks composing the PKI (i.e. CA, RA and KGS). Although no such Security Target has been written yet, the work has been performed by AQL using available information (existing and available PPs for PKI and its associated components) and is presented in the present report.

#### 3.2 Correspondence between description levels

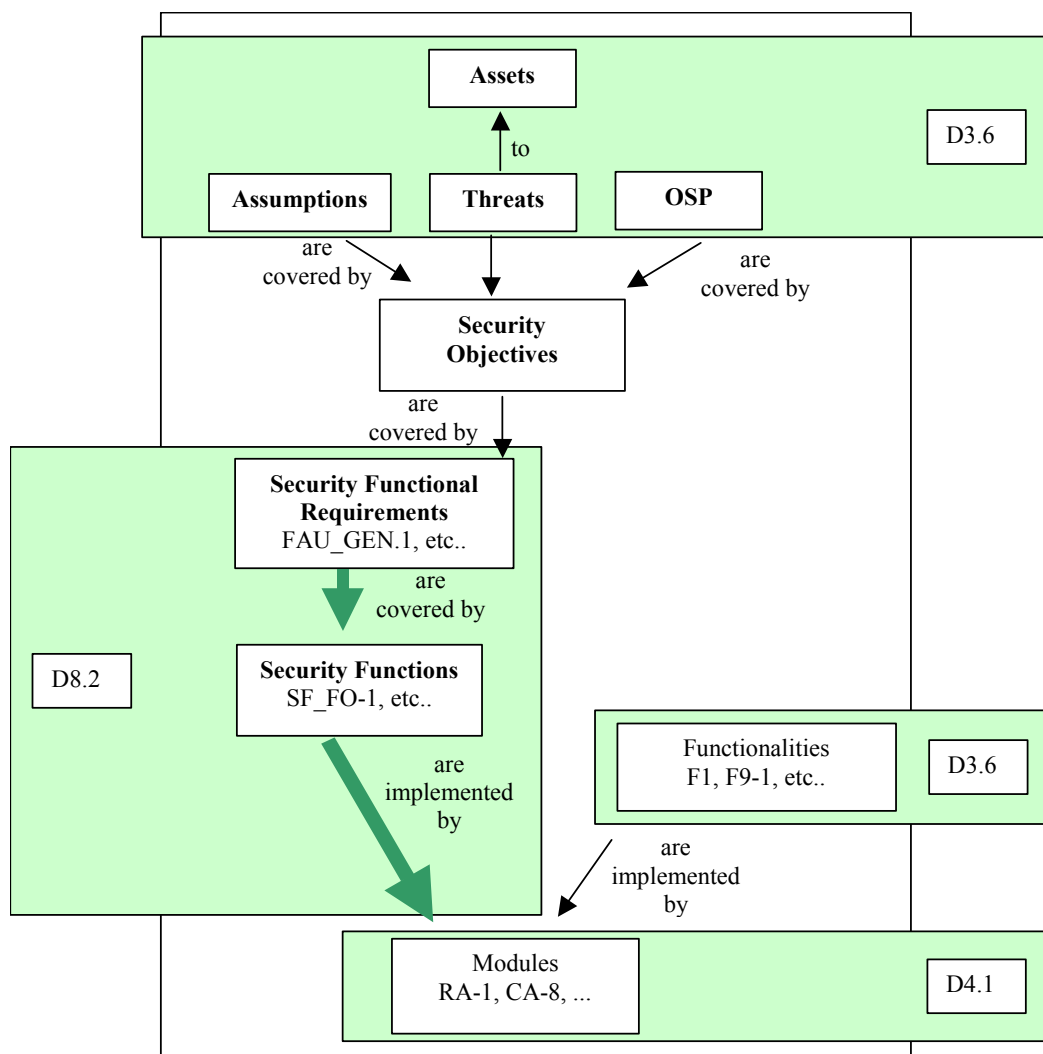


Figure 1: Correspondence links

Figure 1 presents the elements that are already defined or have to be defined to perform a complete security analysis. Elements that have to be considered in a security analysis as regard the Common Criteria are in bold face (assets, threats, security objectives, security requirements, etc...). Deliverables where the definition of the already defined elements can be found is also indicated.

The present document purpose is to select the security functional requirements appropriate to cover security needs for the components of the EUPKI project from those identified within existing Protection Profile about EUPKI (others can be added depending on security needs).

Nevertheless, the present state of the project is that the functionalities and their respective implementations (modules) are already defined (D3.6 and D4.1), whereas, in a fully compliant Common Criteria process, this should have been done after having identified a set of security objectives, themselves refined into a set of security functional requirements, themselves refined into a set of Security Functions. The functionalities described in D3.6 or not only related to security and thus can not be considered as Security Functions as expected in a CC process.

Consequently, in order to define a set of SFR, we have done a reverse analysis, starting from the module definitions to identify a set of Security Functions. Once defined, these security functions have been used to select the SFR that are suitable to the EUPKI project.

As it can be noticed in Figure 1, the security objectives definition is the missing link in our CC security analysis. We expect to write them in a second stage, as soon as the SF and the SFR will have been defined in a satisfactory way.

The present document is a draft in the sense that the coverage between SF, SFR and modules, and even the definition of the Security Functions do not pretend to be complete and exhaustive. Nevertheless, we think that this document, independently of its state, is a good starting point for the working group to complete the security analysis and define the security services covered by the EUPKI project.

Thus, the present report will evolve by adding new SF definitions, modification of existing SF definitions as a consequence of the analysis and completion of the coverage tables provided in the present document.

### **3.3 Structure of the document**

Section 4 presents the security functions identified from the module definitions. For each component of the EUPKI, we have proposed a set of security functions.

Section 5 presents the security functional requirements that are covered by the security functions identified in previous section. SFR and their links to the SF are presented for each component.

Annexe A gathers the SFR definitions.

*Comment: Please notice that we have use "Winword signets" to facilitate the navigation between the definitions of the SF, the SFR and the tables. This is particularly useful to validate the tables.*

### **3.4 Glossary**

CRM	Customer Relationship Management
HR	Human Resources
OCSF	On-line Certificate Status Protocol
TOE	Target Of Evaluation
SFR	Security Functional Requirements
PKI	Public Key Infrastructure
CA	Certification Authority
RA	Registration Authority
CRPKI	Cryptographic Resource for Public Key Infrastructure
TSP	TOE Security Functions — A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TSP	TOE Security Policy — A set of rules that regulate how assets are managed, protected and distributed within a TOE.
PP	Protection Profile
ST	Security Target
TSP	TOE Security Functions

## 4 Security Functions

This section presents a set of supposed security functions for each identified component of the EUPKI (as defined in d4.1: "global architecture"). These sets of functions has been a first step towards the security requirement assignment to block modules presented in the next section.

The identified components are the following:

- Certification Authority (CA)
- Cryptographic System Provider (CSP)
- Registration Authority - Front Office (FO)
- Registration Authority - Back Office (BO)
- Central Key Generation System (CKGS)
- User Key Generation System (UKGS)

NB.: In tables presented in this section, modules that are not associated to any function (see table in annex B for correspondence details) in the deliverables 4.1 or 4.3 are grey shaded. It has to be decided if a these modules are security enforcing or not, in order to identify the security functions really implemented. For example the security function SF\_CA\_OTP is mainly implemented by two modules that are not used to implement any CA functionality (according to d4.1). Consequently we may have to suppress the security function SF\_CA\_OTP. Finally, do we have to consider only used modules to identify security functions or do we have to consider the whole set of modules (which is the option that has been taken in the present version of the document) ?

### 4.1.1 Certification Authority

#### 4.1.1.1 Certification Authority Security Functions

SF_CA_Admin	The Certification Authority provides a set of administrative functions only available to administrators.
SF_CA_AccessControl	The Certification Authority provides an access control on managed elements.
SF_CA_SecCom	The Certification Authority is able to communicate sensitive information to other components of the PKI.
SF_CA_Audit	The Certification Authority provides ways to perform audit on actions performed.
SF_CA_CertMngt	The Certification Authority provides ways to manage Certificates List.
SF_CA_OTP	The Certification Authority provides a One Time Password generation system.

#### 4.1.1.2 *Certification Authority modules*

Block number	Modules	SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt
CA-1	User Request Handler						X
CA-2	Writemail						
CA-3	Log					X	
CA-5	Admin Interface	X					
CA-6	Admin API	X	X	X			
CA-8	Audit					X	
CA-9	OTP distributor				X		
CA-10	CA-API	X	X	X	X		X
CA-11	OTP Generator		X				
CA-12	OTP Authenticator		X				
CA-13	Communication to CSP				X		
CA-14	CA database						X
CA-15	Access Control			X			
CA-16	Publication				X		X
CA-17	Communication to KGS				X		
CA-18	CRL Factory						X
CA-20	Certificate Update Agent						X

#### 4.1.1.3 *Cryptographic System Provider Security Functions*

SF\_CSP\_Crypto                      The Cryptographic System Provider is able to perform cryptographic key generation.

SF\_CSP\_CertMngt                    The Cryptographic System Provider is able to sign Certificate and Certificate Revocation List in a secure manner.

#### 4.1.1.4 *Cryptographic System Provider modules*

Block number	Modules	SF_CSP_Crypto	SF_CSP_CertMngt
CSP-1	CSP-API	X	
CSP-2	Certificate Signer		X
CSP-3	CRL Signer		X
CSP-4	Crypto Engine	X	

#### 4.1.2 *Registration Authority*

##### 4.1.2.1 *Security Functions for RA-Front Office*

SF\_FO\_IdAuthUser      The Front Office part of the Registration Authority provides a user interface with login/authentication procedures.

SF\_FO\_SecureCom      The Front Office part of the Registration Authority provides a secure communication channel with the Back Office part of the Registration Authority.

##### 4.1.2.2 *RA-Front Office modules*

Block number	Modules	SF_FO_IdAuthUser	SF_FO_SecureCom
FO-1	User Interface	X	
FO-2	Communication to BO		X

##### 4.1.2.3 *Security Functions for RA-Back Office*

SF\_BO\_AccessControl      The Back Office part of the Registration Authority provides an access control on managed elements.

SF\_BO\_Audit      The Back Office part of the Registration Authority provides an audit functionality on actions performed.

SF_BO_IdAuthUser	Any functions performed using the Back Office part of the Registration Authority requested for an identification and authentication of the user.
SF_BO_Admin	The Back Office part of the Registration Authority provides administrative functions to authorised users.
SF_BO_SecureCom	The Back Office part of the Registration Authority provides a secure communication channel with the Front Office part of the Registration Authority and with the Certification Authority.
SF_BO_CertifMngt	The Back Office part of the Registration Authority provides secured functions to manage a list of certificates.

#### 4.1.2.4 RA- Back Office modules

Block number	Modules	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
RA-1	User Interface						
RA-2	Validation						X
RA-3	Log	X	X	X	X	X	X
RA-4	RA database						X
RA-5	Entry / Renewal						X
RA-7	Communication to CA					X	
RA-8	Audit		X				
RA-10	RA-API						X
RA-13	Revocation						X
RA-14	Entity/Cert Browser						X
RA-15	Access Control	X		X			
RA-16	Admin Interface				X		
RA-17	Admin API				X		
RA-18	RA PK Acceptor						X
RA-20	Communication to FO					X	

### 4.1.3 Central KGS

#### 4.1.3.1 Security Functions for Central KGS

SF_CKGS_AccessControl	The Central KGS provides an access control on managed elements.
SF_CKGS_Audit	The Central KGS provides an audit functionality on the cryptographic elements.
SF_CKGS_Crypto	The Central KGS provides a trusted key pair generation process.
SF_CKGS_IdAuthUser	Any functions performed using the KGS requested for an identification/authentication of the user.
SF_CKGS_Admin	The Central KGS provides administrative functions to authorised users.
SF_CKGS_Log	The Central KGS logs any operations performed.
SF_CKGS_CertStorage	The Central KGS stores in a secure way the certificates generated

#### 4.1.3.2 Central KGS modules

Block number	Modules	SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage
<b>KGS-3</b>	Log		X				X	
<b>KGS-5</b>	Admin Interface				X	X		
<b>KGS-6</b>	Admin API				X	X		
<b>KGS-8</b>	Audit		X					
<b>KGS-10</b>	KGS-API	X	X	X	X	X	X	X
<b>KGS-14</b>	Key Store							X
<b>KGS-15</b>	Access Control	X						
<b>KGS-21</b>	Key Pair Generator			X				
<b>KGS-22</b>	Certificate Storage							X
<b>KGS-26</b>	Key Pair Factory			X				

#### 4.1.4 User KGS

##### 4.1.4.1 Security Functions for User KGS

SF\_UKGS\_AccessControl The User KGS provides an access control on managed elements.

SF\_UKGS\_Crypto The User KGS provides a trusted key pair generation process.

SF\_UKGS\_ExportImport Export/import functions

##### 4.1.4.2 User KGS modules

Block number	Modules	SF_UKGS_AccessControl	SF_UKGS_Crypto	SF_UKGS_ExportImport
<b>KGS-14</b>	Key Store			
<b>KGS-21</b>	Key Pair Generator		X	
<b>KGS-23</b>	Export Certificate request			X
<b>KGS-24</b>	Import Certificate replies			X
<b>KGS-25</b>	User Interface	X		
<b>KGS-27</b>	User KGS API		X	
<b>KGS-28</b>	Access Control	X		

## 5 Security Functional Requirements

Conforming to the deliverable D3.6 (section 7.2), the TOE is composed of the following components:

- Certification Authority (CA including a CSP)
- Registration Authority (RA composed of a Front Office and a Back Office)
- Key Generation System (KGS) composed of a central part and a user part.

This section presents the security functional requirements taken from existing (but not certified yet) Protection Profiles for PKI components ([PP CA], [PP RA] and [PP CRPKI]) and for the whole PKI ([PP PKI]).

In section 5, we present tables summarising security functional requirements that have been selected in these Protection Profiles, and are extracted from Common Criteria Part 2 ([CC-02]) Security Functional Requirements (SFR). For each of them we have identified the security functions that implement them.

Nevertheless, links between SFR and modules, via Security Functions, are not always obvious. Consequently, we have included several questions for which we have not found an answer in other deliverables.

The SFR come from the PP (components ([PP CA], [PP RA] and [PP CRPKI]) and for the whole PKI ([PP PKI]) taken as input to this document. In the following tables, when a SFR is not covered by even one Security Function, it means that no modules implement it. This point has to be validated by the EUPKI's partners that have a better knowledge of the architecture and modules definitions than us.

The final goal is to write separate security targets for the following blocks of the EUPKI project:

- Global ST for the EUPKI
- Certification Authority (with CSP: Cryptographic Service Provider)
- Registration Authority (FO: Front Office and BO: Back Office)
- Key Generation System (Central KGS and User KGS)

## 5.1 SFR for Certification Authority

### 5.1.1 Security Audit

Security audit		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FAU_GEN.1	Audit data generation					X			
FAU_GEN.2	User identity association.					X			
FAU_SAR.1	Audit review.	X				X			
FAU_SAR.2	Restricted audit review	X				X			
FAU_SAR.3	Selectable audit review	X				X			
FAU_STG.2	Guarantees of audit data availability					X			
FAU_STG.4	Prevention of audit data loss					X			

Concerning daemons, as they're acting on behalf of the administrator, the user identity associated to the logged event is the administrator's one.

#### Audit:

The following actions should be auditable:

- Actions taken due to the audit storage failure.
- Reading of information from the audit records.
- Unsuccessful attempts to read information from the audit records.

### 5.1.2 Communication

Communication		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FCO_NRO.2	Enforced proof of origin	X	X		X				
FCO_NRR.2	Enforced proof of receipt	X	X		X				

#### Audit:

The following actions should be auditable:

- The invocation of the non-repudiation service.
- Identification of the information, the destination, and a copy of the evidence provided.

### 5.1.3 Cryptographic support (CSP)

Cryptographic support		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FCS_CKM.1	Cryptographic key generation		X				X		
FCS_CKM.2	Cryptographic key distribution	X	X		X		X	X	X
FCS_CKM.3	Cryptographic key access	X					X	X	
FCS_CKM.4	Cryptographic key destruction		X				X		
FCS_COP.1	Cryptographic operation		X				X		

#### Audit:

The following actions should be auditable:

- Success and failure of the activity.
- Success and failure, and the type of cryptographic operation.
- Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
- The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

### 5.1.4 User data protection

User data protection		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FDP_ACC.2	Complete access control			X					
FDP_ACF.1	Security attribute based access control	X		X					
FDP_IFC.2	Complete information flow control			X	X				
FDP_IFF.1	Simple security attributes			X					X
FDP_ITC.1	Import of user data without security attributes				X		X		X
FDP_ITT.1	Basic internal transfer protection						X		X
FDP_RIP.1	Subset residual information protection								X
FDP_UIT.1	Data exchange integrity				X		X		X

#### Audit:

The following actions should be auditable:

- Decisions to permit requested information flows.
- Successful import of user data, including any security attributes.

- Successful requests to perform an operation on an object covered by the SFP.
- Successful transfers of user data, including identification of the protection method used.
- The identity of any user or subject using the data exchange mechanisms.
- A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.
- All attempts to import user data, including any security attributes.
- All attempts to transfer user data, including the protection method used and any errors that occurred.
- All decisions on requests for information flow.
- All requests to perform an operation on an object covered by the SFP.
- Any identified attempts to block transmission of user data.
- The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorized to do so.

### 5.1.5 Identification and authentication

Identification and authentication		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FIA_ATD.1	User attribute definition			X					
FIA_UAU.2	User authentication before any action	X		X					
FIA_UAU.6	User re-authenticating			X					
FIA_UID.2	User identification before any action			X					
FIA_USB.1	User-subject Binding	X		X					

The FIA\_USB.1 requirement is used to established a link between a user (security attributes as a user identity) and a process acting on his behalf.

#### **Audit:**

The following actions should be auditable:

- Failure of re-authentication;
- Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).
- Unsuccessful use of the authentication mechanism;
- Unsuccessful use of the user identification mechanism, including the user identity provided;
- All re-authentication attempts.
- All use of the authentication mechanism.
- All use of the user identification mechanism, including the user identity provided.

- Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).

### 5.1.6 Security management

Security management		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FMT_MSA.1	Management of security attributes		X	X					
FMT_MSA.3	Static attribute initialisation	X	X				X		
FMT_MTD.1	Management of TSF data		X				X		X
FMT_MTD.3	Secure TSF data		X				X		X
FMT_SMR.2	Restrictions on security roles	X							

#### Audit:

The following actions should be auditable:

- All rejected values of TSF data.
- Modifications to the group of users that are part of a role;
- Unsuccessful attempts to use a role due to the given conditions on the roles;
- All modifications of the initial values of security attributes.
- All modifications of the values of security attributes.
- All modifications to the values of TSF data.
- Modifications of the default setting of permissive or restrictive rules.

### 5.1.7 Protection of the security functions

Protection of the TSF		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FPT_AMT.1	Abstract machine testing								
FPT_ITC.1	Inter-TSF confidentiality during transmission				X				
FPT_ITI.1	Inter-TSF detection of modification				X				
FPT_ITT.1	Basic internal TSF data transfer protection				X				
FPT_ITT.3	TSF data integrity monitoring.					X			
FPT_RVM.1	Non-bypassability of the TSP								
FPT_TDC.1	Inter-TSF basic TSF data consistency				X				
FPT_TRC.1	Internal TSF consistency						X		

The Security Functional Requirement FPT\_AMT.1 could be added in the Security Target document if some CA Security Functions use security functionalities of the abstract machine. In this case, a new Security function will be added to implement this Security Functional Requirement. This Security Functional Requirement is concerned with the TOE's environment.

#### Audit:

The following actions should be auditable:

- Restoring consistency upon reconnection.
- Successful use of TSF data consistency mechanisms.
- The detection of modification of transmitted TSF data.
- The detection of modification of TSF data;
- Detected inconsistency between TSF data.
- Detection of modified TSF data.
- Execution of the tests of the underlying machine and the results of the tests.
- Identification of which TSF data have been interpreted.
- The action taken following detection of an integrity error.
- The action taken upon detection of modification of transmitted TSF data.
- Use of the TSF data consistency mechanisms.

### 5.1.8 Trusted channels

Trusted path/channels		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FTP_ITC.1	Inter-TSF trusted channel				X				

#### Audit:

The following actions should be auditable:

- Failure of the trusted channel functions.
- Identification of the initiator and target of failed trusted channel functions.
- All attempted uses of the trusted channel functions.
- Identification of the initiator and target of all trusted channel functions.

**5.1.9 Synthesis**

		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FPT_ITC.1	Inter-TSF trusted channel				X				
FPT_AMT.1	Abstract machine testing								
FPT_ITC.1	Inter-TSF confidentiality during transmission				X				
FPT_ITI.1	Inter-TSF detection of modification				X				
FPT_ITT.1	Basic internal TSF data transfer protection				X				
FPT_ITT.3	TSF data integrity monitoring.					X			
FPT_RVM.1	Non-bypassability of the TSP								
FPT_TDC.1	Inter-TSF basic TSF data consistency				X				
FPT_TRC.1	Internal TSF consistency						X		
FMT_MSA.1	Management of security attributes		X	X					
FMT_MSA.3	Static attribute initialization	X	X						X
FMT_MTD.1	Management of TSF data		X				X		X
FMT_MTD.3	Secure TSF data		X				X		X
FMT_SMR.2	Restrictions on security roles	X							
FIA_ATD.1	User attribute definition			X					
FIA_UAU.2	User authentication before any action	X		X					
FIA_UAU.6	User re-authenticating			X					
FIA_UID.2	User identification before any action			X					
FIA_USB.1	User-subject Binding	X		X					
FDP_ACC.2	Complete access control			X					
FDP_ACF.1	Security attribute based access control	X		X					
FDP_IFC.2	Complete information flow control			X	X				
FDP_IFF.1	Simple security attributes			X					X
FDP_ITC.1	Import of user data without security attributes				X		X		X
FDP_ITT.1	Basic internal transfer protection						X		X
FDP_RIP.1	Subset residual information protection								X
FDP_UIT.1	Data exchange integrity				X		X		X
FCS_CKM.1	Cryptographic key generation		X					X	
FCS_CKM.2	Cryptographic key distribution	X	X		X		X	X	X
FCS_CKM.3	Cryptographic key access	X						X	X
FCS_CKM.4	Cryptographic key destruction		X					X	
FCS_COP.1	Cryptographic operation		X					X	

		SF_CA_Admin	SF_CA_OTP	SF_CA_AccessControl	SF_CA_SecCom	SF_CA_Audit	SF_CA_CertMngt	SF_CSP_Crypto	SF_CSP_CertMngt
FCO_NRO.2	Enforced proof of origin	X	X		X				
FCO_NRR.2	Enforced proof of receipt	X	X		X				
FAU_GEN.1	Audit data generation					X			
FAU_GEN.2	User identity association.					X			
FAU_SAR.1	Audit review.	X				X			
FAU_SAR.2	Restricted audit review	X				X			
FAU_SAR.3	Selectable audit review	X				X			
FAU_STG.2	Guarantees of audit data availability					X			
FAU_STG.4	Prevention of audit data loss					X			

## 5.2 SFR for the Registration Authority

### 5.2.1 Security Audit

Security audit		SF_BO_IdAuthUser	SF_BO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FAU_GEN.1	Audit data generation				X				
FAU_GEN.2	User identify generation.	X				X			
FAU_SAR.1	Audit review.				X				
FAU_SAR.2	Restricted audit review				X		X		
FAU_SAR.3	Selectable audit review				X		X		
FAU_STG.2	Guarantees of audit data availability				?				
FAU_STG.4	Prevention of audit data loss				?				

FAU\_STG.2: Is there a guarantee that audit data will always be available, or even a part of them ?

FAU\_STG.4: is there any module enforcing a protection against audit data lost ?

#### **Audit:**

The following actions should be auditable:

- Actions taken due to the audit storage failure.
- Reading of information from the audit records.
- Unsuccessful attempts to read information from the audit records.

**5.2.2 Communication**

<b>Communication</b>		<b>SF_FO_IdAuthUser</b>						
		<b>SF_FO_SecureCom</b>	X					
		<b>SF_BO_AccessControl</b>						
		<b>SF_BO_Audit</b>						
		<b>SF_BO_IdAuthUser</b>						
		<b>SF_BO_Admin</b>						
		<b>SF_BO_SecureCom</b>	X					
		<b>SF_BO_CertifMngt</b>						
FCO_NRO.2	Enforced proof of origin							

**Audit:**

The following actions should be auditable:

- The invocation of the non-repudiation service.
- Identification of the information, the destination, and a copy of the evidence provided.

### 5.2.3 User data protection

User data protection		SF_FO_IdAuthUser	SF_FO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FDP_ACC.2	Complete access control	X		X		X			
FDP_ACF.1	Security attribute based access control			X		X	X		
FDP_DAU.2	Data authentication with identity of guarantor	X				X			
FDP_IFC.2	Complete information flow control							X	
FDP_IFF.1	Simple security attributes					X	X		
FDP_ITC.1	Import of user data without security attributes		?					?	
FDP_ITT.1	Basic internal transfer protection		X					X	
FDP_RIP.1	Subset residual information protection								
FDP_UIT.1	Data exchange integrity							X	

FDP\_ITC.1: does any security function import separately security attributes associated to an user data and the corresponding user data ? Is it done such that the link can not be broken between the attributes and the data ?

#### Audit:

The following actions should be auditable:

- Decisions to permit requested information flows.
- Successful generation of validity evidence.
- Successful import of user data, including any security attributes.
- Successful requests to perform an operation on an object covered by the SFP.
- Successful transfers of user data, including identification of the protection method used.
- The identity of any user or subject using the data exchange mechanisms.
- A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.
- All attempts to import user data, including any security attributes.
- All attempts to transfer user data, including the protection method used and any errors that occurred.
- All decisions on requests for information flow.
- All requests to perform an operation on an object covered by the SFP.
- Any identified attempts to block transmission of user data.
- The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorized to do so.
- Unsuccessful generation of validity evidence.

### 5.2.4 Identification and authentication

Identification and authentication		SF_FO_IdAuthUser	SF_FO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FIA_ATD.1	User attribute definition	X				X			
FIA_UAU.2	User authentication before any action	X				X			
FIA_UID.2	User identification before any action	X				X			

#### Audit:

The following actions should be auditable:

- Unsuccessful use of the authentication mechanism;
- Unsuccessful use of the user identification mechanism, including the user identity provided;
- All use of the authentication mechanism.
- All use of the user identification mechanism, including the user identity provided.

### 5.2.5 Security management

Security management		SF_FO_IdAuthUser	SF_FO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FMT_MSA.1	Management of security attributes	X		X					
FMT_MSA.3	Static attribute initialization						?		
FMT_MTD.1	Management of TSF data						?		
FMT_MTD.3	Secure TSF data		?				?	?	
FMT_SMR.2	Restrictions on security roles			X			X		

FMT\_MSA.3: Which is the security function (i.e. the modules), if any, that implements the management of the security attributes and initialize them ?

FMT\_MTD.1: Which is the security function (i.e. the modules), if any, that implements the management of the TSF data ? Do the user have an access and a control on the security function data ?

FMT\_MTD.3: Is there a control on values that can be assigned to TSF data that insure that no safe state can be reach ?

#### Audit:

The following actions should be auditable:

- All rejected values of TSF data.
- Modifications to the group of users that are part of a role;
- Unsuccessful attempts to use a role due to the given conditions on the roles;
- All modifications of the initial values of security attributes.
- All modifications of the values of security attributes.
- All modifications to the values of TSF data.
- Modifications of the default setting of permissive or restrictive rules.

### 5.2.6 Protection of the security functions

Protection of the TSF		SF_FO_IdAuthUser	SF_FO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FPT_AMT.1	Abstract machine testing						X		
FPT_ITC.1	Inter-TSF confidentiality during transmission		X					X	
FPT_ITI.1	Inter-TSF detection of modification		X		X			X	
FPT_ITT.1	Basic internal TSF data transfer protection		X					X	
FPT_ITT.3	TSF data integrity monitoring				X				
FPT_RVM.1	Non-bypassability of the TSP	X	X	X		X		X	
FPT_TDC.1	Inter-TSF basic TSF data consistency		X					X	
FPT_TRC.1	Internal TSF consistency				X				
FPT_TST.1	TSF Testing						X		

#### Audit:

The following actions should be auditable:

- Restoring consistency upon reconnection.
- Successful use of TSF data consistency mechanisms.
- The detection of modification of transmitted TSF data.
- The detection of modification of TSF data;
- Detected inconsistency between TSF data.
- Detection of modified TSF data.
- Execution of the tests of the underlying machine and the results of the tests.
- Execution of the TSF self tests and the results of the tests.
- Identification of which TSF data have been interpreted.
- The action taken following detection of an integrity error.
- The action taken upon detection of modification of transmitted TSF data.
- Use of the TSF data consistency mechanisms.

### 5.2.7 Trusted channels

Trusted path/channels		SF_FO_IdAuthUser	SF_FO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FTP_ITC.1	Inter-TSF trusted channel		X					X	

#### Audit:

The following actions should be auditable:

- Failure of the trusted channel functions.
- Identification of the initiator and target of failed trusted channel functions.
- All attempted uses of the trusted channel functions.
- Identification of the initiator and target of all trusted channel functions.

### 5.2.8 Synthesis

		SF_FO_IdAuthUser	SF_FO_SecureCom	SF_BO_AccessControl	SF_BO_Audit	SF_BO_IdAuthUser	SF_BO_Admin	SF_BO_SecureCom	SF_BO_CertifMngt
FAU_GEN.1	Audit data generation				X				
FAU_GEN.2	User identify generation.	X				X			
FAU_SAR.1	Audit review.				X				
FAU_SAR.2	Restricted audit review				X		X		
FAU_SAR.3	Selectable audit review				X		X		
FAU_STG.2	Guarantees of audit data availability				?				
FAU_STG.4	Prevention of audit data loss				?				
FCO_NRO.2	Enforced proof of origin		X					X	
FDP_ACC.2	Complete access control	X		X		X			
FDP_ACF.1	Security attribute based access control			X		X	X		
FDP_DAU.2	Data authentication with identity of guarantor	X				X			
FDP_IFC.2	Complete information flow control							X	
FDP_IFF.1	Simple security attributes					X	X		
FDP_ITC.1	Import of user data without security attributes		?					?	
FDP_ITT.1	Basic internal transfer protection		X					X	
FDP_RIP.1	Subset residual information protection								
FDP_UIT.1	Data exchange integrity							X	
FIA_ATD.1	User attribute definition	X				X			
FIA_UAU.2	User authentication before any action	X				X			
FIA_UID.2	User identification before any action	X				X			
FMT_MSA.1	Management of security attributes	X		X					
FMT_MSA.3	Static attribute initialization						?		
FMT_MTD.1	Management of TSF data						?		
FMT_MTD.3	Secure TSF data		?				?	?	
FMT_SMR.2	Restrictions on security roles			X			X		
FPT_AMT.1	Abstract machine testing						X		
FPT_ITC.1	Inter-TSF confidentiality during transmission		X					X	
FPT_ITI.1	Inter-TSF detection of modification		X		X			X	
FPT_ITT.1	Basic internal TSF data transfer protection		X					X	
FPT_ITT.3	TSF data integrity monitoring				X				
FPT_RVM.1	Non-bypassability of the TSP	X	X	X		X		X	
FPT_TDC.1	Inter-TSF basic TSF data consistency		X					X	
FPT_TRC.1	Internal TSF consistency				X				
FPT_TST.1	TSF Testing						X		
FTP_ITC.1	Inter-TSF trusted channel		X					X	

## 5.3 SFR for the Key Generation System

### 5.3.1 Security Audit

Security audit		SF_CKGS_AccessControl											
		SF_CKGS_Audit	X										
		SF_CKGS_Crypto											
		SF_CKGS_IdAuthUser											
		SF_CKGS_Admin											
		SF_CKGS_Log	X										
		SF_CKGS_CertStorage											
		SF_UKGS_AccessControl											
		SF_UKGS_Crypto											
		Erreur! Source du renvoi											
		SF_UKGS_ExportImport											
FAU_GEN.1	Audit data generation		X					X					
FAU_STG.4	Prevention of audit data loss		X					X					

#### Audit:

The following actions should be auditable:

- Actions taken due to the audit storage failure.

### 5.3.2 Communication

Communication		SF_CKGS_AccessControl											
		SF_CKGS_Audit											
		SF_CKGS_Crypto											
		SF_CKGS_IdAuthUser											
		SF_CKGS_Admin											
		SF_CKGS_Log											
		SF_CKGS_CertStorage											
		SF_UKGS_AccessControl											
		SF_UKGS_Crypto											
		Erreur! Source du renvoi											
		SF_UKGS_ExportImport											X
FCO_NRR.2	Enforced proof of receipt											X	

#### Audit:

The following actions should be auditable:

- The invocation of the non-repudiation service.
- Identification of the information, the destination, and a copy of the evidence provided.

### 5.3.3 Cryptographic support

Cryptographic support		SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage	SF_UKGS_AccessControl	SF_UKGS_Crypto	Erreur!	Source	renvoi
FCS_CKM.1	Cryptographic key generation			X						X			
FCS_CKM.2	Cryptographic key distribution												X
FCS_CKM.3	Cryptographic key access	X		X		X		X	X	X	X		
FCS_CKM.4	Cryptographic key destruction			X				X		X	X		
FCS_COP.1	Cryptographic operation			X						X			

#### Audit:

The following actions should be auditable:

- Success and failure of the activity.
- Success and failure, and the type of cryptographic operation.
- Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
- The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

### 5.3.4 User data protection

User data protection		SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage	SF_UKGS_AccessControl	SF_UKGS_Crypto	Erreur!	Source	renvoi
FDP_IFF.5	No illicit information flow												X
FDP_ITC.1	Import of user data without security attributes												X
FDP_UIT.1	Data exchange integrity												X

#### Audit:

The following actions should be auditable:

- Decisions to permit requested information flows.
- Successful export of information.
- Successful import of user data, including any security attributes.
- The identity of any user or subject using the data exchange mechanisms.
- A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This could include security attributes associated with the user data.
- All attempts to export information.
- All attempts to import user data, including any security attributes.
- All decisions on requests for information flow.
- Any identified attempts to block transmission of user data.
- The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorised to do so.

### 5.3.5 Identification and authentication

Identification and authentication		SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage	SF_UKGS_AccessControl	SF_UKGS_Crypto	Erreur ! Source du renvoi	SF_UKGS_ExportImport
FIA_AFL.1	Authentication failure handling	X			X				X			
FIA_ATD.1	User attribute definition	X			X				X			
FIA_UAU.2	User authentication before any action				X							
FIA_UAU.6	User re-authenticating	X			X				X			
FIA_UID.2	User identification before any action				X							
FIA_USB.1	User-subject Binding				X							

#### Audit:

The following actions should be auditable:

- Failure of re-authentication;
- the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
- Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).
- Unsuccessful use of the authentication mechanism;
- Unsuccessful use of the user identification mechanism, including the user identity provided;
- All re-authentication attempts.
- All use of the authentication mechanism.

- All use of the user identification mechanism, including the user identity provided.
- Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).

### 5.3.6 Security management

Security management		SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage	SF_UKGS_AccessControl	SF_UKGS_Crypto	Erreur! Source du renvoi	SF_UKGS_ExportImport
FMT_MOF.1	Management of security functions behaviour					X						
FMT_MSA.1	Management of security attributes					X						
FMT_MSA.2	Secure security attributes					X						
FMT_SMR.1	Security Roles	X	X			X			X			

#### Audit:

The following actions should be auditable:

- All offered and rejected values for a security attribute;
- Modifications to the group of users that are part of a role;
- All modifications in the behavior of the functions in the TSF.
- All modifications of the values of security attributes.

### 5.3.7 Protection of the security functions

Protection of the TSF		SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage	SF_UKGS_AccessControl	SF_UKGS_Crypto	Erreur ! Source du renvoi	SF_UKGS_ExportImport
FPT_FLS.1	Failure with preservation of secure state					?						
FPT_ITC.1	Inter-TSF confidentiality during transmission											X
FPT_PHP.3	Resistance physical attack											
FPT_RVM.1	Non-bypassability of the TSP											
FPT_SEP.1	TSF domain separation					X						
FPT_TDC.1	Inter-TSF basic TSF data consistency											X
FPT_TRC.1	Internal TSF consistency											

FPT\_FLS.1: is there a security function (i.e. a module) that implements a preservation of a secure state of the CKGS or the UKGS ?

FPT\_PHP.3: are the CKGS or the UKGS protected against a physical attack ?

FPT\_RVM.1: is there a module dedicated to prevent any bypassing of the security function, insuring that any access control implemented will be perform ?

#### Audit:

The following actions should be auditable:

- Restoring consistency upon reconnection.
- Successful use of TSF data consistency mechanisms.
- Detected inconsistency between TSF data.
- Detection of modified TSF data.
- Failure of the TSF.
- Identification of which TSF data have been interpreted.
- Use of the TSF data consistency mechanisms.

### 5.3.8 Trusted channels

Trusted path/channels		SF_CKGS_AccessControl
		SF_CKGS_Audit
		SF_CKGS_Crypto
		SF_CKGS_IdAuthUser
		SF_CKGS_Admin
		SF_CKGS_Log
		SF_CKGS_CertStorage
		SF_UKGS_AccessControl
		SF_UKGS_Crypto
		Erreur! Source du renvoi
		<b>X</b> SF_UKGS_ExportImport
FTP_ITC.1	Inter-TSF trusted channel	

#### Audit:

The following actions should be auditable:

- Failure of the trusted channel functions.
- Identification of the initiator and target of failed trusted channel functions.
- All attempted uses of the trusted channel functions.
- Identification of the initiator and target of all trusted channel functions.

**5.3.9 Synthesis**

		SF_CKGS_AccessControl	SF_CKGS_Audit	SF_CKGS_Crypto	SF_CKGS_IdAuthUser	SF_CKGS_Admin	SF_CKGS_Log	SF_CKGS_CertStorage	SF_UKGS_AccessControl	SF_UKGS_Crypto	Erreur! Source du renvoi	SF_UKGS_ExportImport
FAU_GEN.1	Audit data generation		X				X					
FAU_STG.4	Prevention of audit data loss		X				X					
FCO_NRR.2	Enforced proof of receipt											X
FCS_CKM.1	Cryptographic key generation			X						X		
FCS_CKM.2	Cryptographic key distribution											X
FCS_CKM.3	Cryptographic key access	X		X		X		X	X	X	X	
FCS_CKM.4	Cryptographic key destruction			X				X		X	X	
FCS_COP.1	Cryptographic operation			X						X		
FDP_IFF.5	No illicit information flow											X
FDP_ITC.1	Import of user data without security attributes											X
FDP_UIT.1	Data exchange integrity											X
FIA_AFL.1	Authentication failure handing	X			X				X			
FIA_ATD.1	User attribute definition	X			X				X			
FIA_UAU.2	User authentication before any action				X							
FIA_UAU.6	User re-authenticating	X			X				X			
FIA_UID.2	User identification before any action				X							
FIA_USB.1	User-subject Binding				X							
FMT_MOF.1	Management of security functions behavior					X						
FMT_MSA.1	Management of security attributes					X						
FMT_MSA.2	Secure security attributes					X						
FMT_SMR.1	Security Roles	X	X			X			X			
FPT_FLS.1	Failure with preservation of secure state						?					
FPT_ITC.1	Inter-TSF confidentiality during transmission											X
FPT_PHP.3	Resistance physical attack											
FPT_RVM.1	Non-bypassability of the TSP											
FPT_SEP.1	TSF domain separation					X						
FPT_TDC.1	Inter-TSF basic TSF data consistency											X
FPT_TRC.1	Internal TSF consistency											
FTP_ITC.1	Inter-TSF trusted channel											X

**Annexe A: Security Functional Requirements Definitions**

<b>Security audit</b>	
FAU_GEN.1	<b>Audit data generation</b> Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.
FAU_GEN.2	<b>User identify association</b> The security functions shall associate auditable events to individual user identities.
FAU_SAR.1	<b>Audit review</b> Audit review provides the capability to read information from the audit records.
FAU_SAR.2	<b>Restricted audit review</b> Restricted audit review requires that there are no other users except those that have been identified in FAU_SAR.1 that can read the information.
FAU_SAR.3	<b>Selectable audit review</b> Selectable audit review requires audit review tools to select the audit data to be reviewed based on criteria.
FAU_STG.2	<b>Guarantees of audit data availability</b> Guarantees of audit data availability specifies the guarantees that the security functions maintains over the audit data given the occurrence of an undesired condition.
FAU_STG.4	<b>Prevention of audit data loss</b> Prevention of audit data loss specifies actions in case the audit trail is full.
<b>Communication</b>	
FCO_NRO.2	<b>Enforced proof of origin</b> Enforced proof of origin requires that the security functions always generate evidence of origin for transmitted information.
FCO_NRR.2	<b>Enforced proof of receipt</b> Enforced proof of receipt requires that the security functions always generate evidence of receipt for received information.

<b>Cryptographic support</b>	
FCS_CKM.1	<p><b>Cryptographic key generation</b> Cryptographic key generation requires cryptographic keys to be generated in accordance with a specified algorithm and key sizes which can be based on an assigned standard.</p>
FCS_CKM.2	<p><b>Cryptographic key distribution</b> Cryptographic key distribution requires cryptographic keys to be distributed in accordance with a specified distribution method which can be based on an assigned standard.</p>
FCS_CKM.3	<p><b>Cryptographic key access</b> Cryptographic key access requires access to cryptographic keys to be performed in accordance with a specified access method which can be based on an assigned standard.</p>
FCS_CKM.4	<p><b>Cryptographic key destruction</b> Cryptographic key destruction requires cryptographic keys to be destroyed in accordance with a specified destruction method which can be based on an assigned standard.</p>
FCS_COP.1	<p><b>Cryptographic operation</b> Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.</p>

<b>User data protection</b>	
FDP_ACC.2	<p><b>Complete access control</b></p> <p>Complete access control requires that each identified access control security function policy cover all operations on subjects (e.g. operators, user, administrator) and objects (e.g. key, certificate, user dat covered by that security function policy. It further requires that all objects and operations within scope of control of the TOE are covered by at least one identified access control security function policy.</p>
FDP_ACF.1	<p><b>Security attribute based access control</b></p> <p>Security attribute based access control allows the security functions to enforce access based upon security attributes and named groups of attributes. Furthermore, the security functions may have the ability to explicitly authorise or deny access to an object based upon security attributes. Examples of security attributes: login name, password.</p>
FDP_DAU.2	<p><b>Data authentication with identity of guarantor</b></p> <p>Data Authentication with Identity of Guarantor additionally requires that the security functions is capable of establishing the identity of the subject who provided the guarantee of authenticity.</p>
FDP_ETC.1	<p><b>Export of user data without security attributes</b></p> <p>Export of user data without security attributes requires that the security functions enforce the appropriate security function policies when exporting user data outside the security functions. User data that is exported by this function is exported without its associated security attributes</p>
FDP_IFC.2	<p><b>Complete information flow control</b></p> <p>Complete information flow control requires that each identified information flow control security function policy cover all operations on subjects and information covered by that security function policy. It further requires that all information flows and operations within the scope of control of the TOE are covered by at least one identified information flow control security function policy. In conjunction with the FPT_RVM.1 component, this gives the “always invoked” aspect of a reference monitor.</p>
FDP_IFF.1	<p><b>Simple security attributes</b></p> <p>Simple security attributes requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function, and describes how security attributes are derived by the function.</p>
FDP_IFF.5	<p><b>No illicit information flow</b></p> <p>No illicit information flows requires security function policy to cover the elimination of all illicit information flows.</p>

<b>User data protection</b>	
FDP_ITC.1	<b>Import of user data without security attributes</b> Import of user data without security attributes requires that the security attributes correctly represent the user data and are supplied separately from the object.
FDP_ITT.1	<b>Basic internal transfer protection</b> Basic internal transfer protection requires that user data be protected when transmitted between parts of the TOE.
FDP_RIP.1	<b>Subset residual information protection</b> Subset residual information protection requires that the security functions ensure that any residual information content of any resources is unavailable to a defined subset of the objects in the scope of control of the TOE upon the resource's allocation or de-allocation.
FDP_UCT.1	<b>Basic Data exchange confidentiality</b> Basic data exchange confidentiality, the goal is to provide protection from disclosure of user data while in transit.
FDP_UIT.1	<b>Data exchange integrity</b> Data exchange integrity addresses detection of modifications, deletions, insertions, and replay errors of the user data transmitted.

<b>Identification and authentication</b>	
FIA_AFL.1	<p><b>Authentication failure handing</b></p> <p>Authentication failure handing requires that the security functions be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the security functions be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs.</p>
FIA_ATD.1	<p><b>User attribute definition</b></p> <p>User attribute definition, allows user security attributes for each user to be maintained individually.</p>
FIA_UAU.2	<p><b>User authentication before any action</b></p> <p>User authentication before any action, requires that users authenticate themselves before any action will be allowed by the security functions.</p>
FIA_UAU.6	<p><b>User re-authenticating</b></p> <p>Re-authenticating, requires the ability to specify events for which the user needs to be re-authenticated.</p>
FIA_UID.2	<p><b>User identification before any action</b></p> <p>User identification before any action, require that users identify themselves before any action will be allowed by the security functions.</p>
FIA_USB.1	<p><b>User-subject Binding</b></p> <p>User-subject binding requires the maintenance of an association between the user's security attributes and a subject acting on the user's behalf.</p>

<b>Security management</b>	
FMT_MOF.1	<b>Management of security functions behavior</b> Management of security functions behavior allows the authorized users (roles) to manage the behavior of functions in the security functions that use rules or have specified conditions that may be manageable.
FMT_MSA.1	<b>Management of security attributes</b> Management of security attributes allows authorized users (roles) to manage the specified security attributes.
FMT_MSA.2	<b>Secure security attributes</b> Secure security attributes ensures that values assigned to security attributes are valid with respect to the secure state.
FMT_MSA.3	<b>Static attribute initialization</b> Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.
FMT_MTD.1	<b>Management of TSF data</b> Management of security functions data allows authorized users to manage security functions data.
FMT_MTD.3	<b>Secure TSF data</b> Secure security functions data ensures that values assigned to security functions data are valid with respect to the secure state.
FMT_SMR.1	<b>Security Roles</b> Security roles specifies the roles with respect to security that the security functions recognizes.
FMT_SMR.2	<b>Restrictions on security roles</b> Restrictions on security roles specifies that in addition to the specification of the roles, there are rules that control the relationship between the roles.

<b>Protection of the TSF</b>	
FPT_AMT.1	<p><b>Abstract machine testing</b> Abstract machine testing provides for testing of the underlying abstract machine. When a TOE is relying upon an abstract machine (that can be composed of hardware and software providing security services, testing of the underlying abstract machine, shall be performed, on start-up or when other conditions are met, in order to check before launching the TOE that the underlying abstract machine has not been modified or corrupted.</p>
FPT_FLS.1	<p><b>Failure with preservation of secure state</b> Failure with preservation of secure state requires that the security functions preserve a secure state in the face of the identified failures.</p>
FPT_ITC.1	<p><b>Inter-TSF confidentiality during transmission</b> Inter-security functions confidentiality during transmission requires that the security functions ensure that data transmitted between the security functions and a remote trusted IT product is protected from disclosure while in transit. Namely in EUPKI, data transmission between CA, RA, KGS or any remote trusted IT product (e.g. K shall be protected as regards confidentiality.</p>
FPT_ITI.1	<p><b>Inter-TSF detection of modification</b> Inter-security functions detection of modification, provides the ability to detect modification of security functions data during transmission between the security functions and a remote trusted IT product, under the assumption that the remote trusted IT product is cognisant of the mechanism used. Namely in EUPKI, data transmission between CA, RA, KGS or any remote trusted IT product (e.g. KA, OCSP) shall be protected as regards integrity.</p>
FPT_ITT.1	<p><b>Basic internal TSF data transfer protection</b> Basic internal security functions data transfer protection, requires that security functions data be protected when transmitted between separate parts of the TOE.</p>
FPT_ITT.3	<p><b>TSF data integrity monitoring</b> Security functions data integrity monitoring, requires that the security functions data transmitted between separate parts of the TOE is monitored for identified integrity errors.</p>
FPT_PHP.3	<p><b>Resistance physical attack</b> Resistance to physical attack, provides for features that prevent or resist physical tampering with security functions devices and security functions elements.</p>
FPT_RVM.1	<p><b>Non-bypassability of the TSP</b> Non-bypassability of the TSP requires non-bypassability for all security function policies in the TSP.</p>

<b>Protection of the TSF</b>	
FPT_SEP.1	<p><b>TSF domain separation</b></p> <p>Security functions domain separation, provides a distinct protected domain for the security functions and provides separation between subjects within the scope of control of the TOE.</p>
FPT_STM.1	<p><b>Reliable time stamps</b></p> <p>Reliable time stamps requires that the security functions provide reliable time stamps for security functions.</p> <p>Reliable time stamps is a requirement for a global PKI solution, but within the scope of the EUPKI project, the solution can rely on an external source for reliable time stamps.</p>
FPT_TDC.1	<p><b>Inter-TSF basic TSF data consistency</b></p> <p>Inter-security functions basic security functions data consistency requires that the security functions provide the capability to ensure consistency of attributes between security functions.</p>
FPT_TRC.1	<p><b>Internal TSF consistency</b></p> <p>Internal security functions consistency requires that the security functions ensure the consistency of security functions data that is replicated in multiple locations.</p>
FPT_TST.1	<p><b>TSF Testing</b></p> <p>Security functions testing, provides the ability to test the security functions correct operation. These tests may be performed at start-up, periodically, at the request of the authorized user, or when other conditions are met. It also provides the ability to verify the integrity of security functions data and executable code.</p>

<b>Trusted path/channels</b>	
FTP_ITC.1	<p><b>Inter-TSF trusted channel</b></p> <p>Inter-security functions trusted channel requires that the security functions provide a trusted communication channel between itself and another trusted IT product.</p> <p>Namely in EUPKI, data transmission between CA, RA, KGS or any remote trusted IT product (e.g. KA, OCSP) shall be protected as regards integrity or confidentiality, when security critical operations are performed.</p>

## Annex B: Modules and functions correspondences (as defined in d4.3)

These tables are being revised. They will be updated after the final version of D4.3

Function	Description
F1	Generate keys and certificate
F1.1	Generate keys
F1.2	Generate certificate
F2	Recover private encryption key
F3	Revoke certificate
F4	Repudiate keys
F5	Publish certificate in a directory
F6	Publish certificate in a CRL
F7	Suspend certificate
F8	Reactivate suspended certificate
F9	Update information in a certificate
F9.1	Renew certificate
F10	View event log
F10.1	Consult alarms
F11	Recover certificate
F12	Create a Certificate profile/template
F12.1	Sending the
F13	Key Ceremony
F13.1	CA/sub CA management
F13.2	Administrator management
F13.3	Secrets import/export
F15	Create and manage RA account
F16-19	Manage operator profiles and privileges

Module	Title	F1	F1.1	F1.2	F2	F3	F4	F5	F6	F7	F8	F9	F9.1	F10	F10.1	F11	F12	F12.1	F13	F13.1	F13.2	F13.3	F15	F16-19
<b>CA-01</b>	User Request Handler																							
<b>CA-02</b>	Writemail												<b>X</b>											
<b>CA-03</b>	Log	<b>X</b>				<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>	<b>X</b>		<b>X</b>	<b>X</b>	<b>X</b>		<b>X</b>		<b>X</b>				<b>X</b>	<b>X</b>
<b>CA-05</b>	Admin Interface																<b>X</b>		<b>X</b>				<b>X</b>	<b>X</b>
<b>CA-06</b>	Admin API																<b>X</b>		<b>X</b>				<b>X</b>	<b>X</b>
<b>CA-08</b>	Audit													<b>X</b>	<b>X</b>									
<b>CA-09</b>	OTP distributor																<b>X</b>		<b>X</b>				<b>X</b>	<b>X</b>
<b>CA-10</b>	CA-API	<b>X</b>				<b>X</b>	<b>X</b>			<b>X</b>	<b>X</b>		<b>X</b>											
<b>CA-11</b>	OTP Generator																<b>X</b>		<b>X</b>				<b>X</b>	<b>X</b>
<b>CA-12</b>	OTP Authenticator	<b>X</b>				<b>X</b>							<b>X</b>											
<b>CA-13</b>	Communication to CSP	<b>X</b>				<b>X</b>							<b>X</b>											
<b>CA-14</b>	CA database	<b>X</b>				<b>X</b>							<b>X</b>				<b>X</b>		<b>X</b>				<b>X</b>	<b>X</b>
<b>CA-15</b>	Access Control	<b>X</b>				<b>X</b>							<b>X</b>											
<b>CA-16</b>	Publication	<b>X</b>				<b>X</b>		<b>X</b>	<b>X</b>				<b>X</b>											
<b>CA-17</b>	Communication to KGS	<b>X</b>																						
<b>CA-18</b>	CRL Factory					<b>X</b>																		
<b>CA-20</b>	Certificate Update Agent												<b>X</b>											
<b>CSP-1</b>	CSP-API			<b>X</b>		<b>X</b>							<b>X</b>											
<b>CSP-2</b>	Certificate Signer			<b>X</b>									<b>X</b>											
<b>CSP-3</b>	CRL Signer					<b>X</b>																		
<b>CSP-4</b>	(Crypto Engine, sub module)			<b>X</b>		<b>X</b>							<b>X</b>											

Module	Title	F1	F1.1	F1.2	F2	F3	F4	F5	F6	F7	F8	F9	F9.1	F10	F10.1	F11	F12	F12.1	F13	F13.1	F13.2	F13.3	F15	F16-19
<b>FO-01</b>	User Interface	X				X						X												
<b>FO-02</b>	Communication to BO	X				X						X												
<b>KGS-03</b>	Log	X	X																					
<b>KGS-05</b>	Admin Interface		X																					
<b>KGS-06</b>	Admin API																							X
<b>KGS-08</b>	Audit													X										
<b>KGS-10</b>	KGS-API Job Scheduler	X	X																					
<b>KGS-14</b>	Key Store		X																					
<b>KGS-15</b>	Access Control (Central KGS)	X	X																					
<b>KGS-21</b>	Key Pair Generator		X																					
<b>KGS-22</b>	Certificate Storage		X																					
<b>KGS-23</b>	Export Certificate Request to CA	X	X																					
<b>KGS-24</b>	Import Certificate Replies from CA	X	X																					
<b>KGS-25</b>	User Interface		X																					
<b>KGS-26</b>	Key Pair Factory		X																					
<b>KGS-27</b>	User KGS API	X	X																					
<b>KGS-28</b>	Access Control (User KGS)		X																					
<b>KGS-29</b>	Export PKCS#12							X																
<b>RA-01</b>	User Interface	X				X						X												
<b>RA-02</b>	Validation	X																						
<b>RA-03</b>	RA-3	X				X						X												
<b>RA-04</b>	RA-4	X				X						X												
<b>RA-05</b>	RA-5	X										X												
<b>RA-07</b>	Communication to CA	X				X							X											

Module	Title	F1	F1.1	F1.2	F2	F3	F4	F5	F6	F7	F8	F9	F9.1	F10	F10.1	F11	F12	F12.1	F13	F13.1	F13.2	F13.3	F15	F16-19
<b>RA-08</b>	Audit													<b>X</b>	<b>X</b>									
<b>RA-10</b>	RA-API	<b>X</b>				<b>X</b>					<b>X</b>	<b>X</b>												
<b>RA-13</b>	Revocation					<b>X</b>				<b>X</b>														
<b>RA-14</b>	Entity/Cert Browser					<b>X</b>																		
<b>RA-15</b>	Access Control	<b>X</b>				<b>X</b>						<b>X</b>												
<b>RA-16</b>	Admin Interface																						<b>X</b>	<b>X</b>
<b>RA-17</b>	Admin API																						<b>X</b>	<b>X</b>
<b>RA-18</b>	RA PK Acceptor	<b>X</b>				<b>X</b>						<b>X</b>												
<b>RA-20</b>	Communication to FO	<b>X</b>				<b>X</b>						<b>X</b>												

Modules not used to implement identified functionalities are grey shaded in the table.