



IST-2001-34340
D3.5 Draft of the definition of the
perimeter of the project

Distribution List :	Project Partners
Author :	Minaradjy Pascal & Pierre-Olivier Baudot, CGE&Y
Distribution List :	Project Partners
Authorised by :	Yann Fraval, GIP-MDS
Date of Issue :	28 June 2002
Issue :	1.0
File Name :	EUPKI-WP3-D3.5-1.0.doc
Work Package :	WP3 Requirements
Deliverable Number :	D 3.5
Deliverable Type :	Public
Deliverable Nature :	Draft of the final WP3 report
Total Number of Pages :	23
Contact Details for EUPKI :	Project Coordinator Yann Fraval GIP-MDS mail : yann.fraval@gip-mds.fr web site : www.eupki.org

0 Table Of Contents

0	TABLE OF CONTENTS	2
1	DOCUMENT CONTROL	4
1.1	ABSTRACT	4
1.2	KEYWORDS	4
2	MANAGEMENT OVERVIEW	5
2.1	EXECUTIVE SUMMARY	5
2.2	SCOPE STATEMENT	5
3	INTRODUCTION AND GLOSSARY.....	6
3.1	GLOSSARY	6
4	PERIMETER OF THE EUPKI PROJECT	7
4.1	PERIMETER	7
4.2	PKI BUSINESSES AND SERVICES	7
0.1	8
5	USERS OF THE PKI	10
6	PKI FUNCTIONS REQUIREMENTS.....	11
6.1	LIST OF THE PKI FUNCTIONS	11
6.2	SOME FUNCTIONS OUT OF THE SCOPE OF THE EUPKI PROJECT	13
6.3	FUNCTIONS REQUIREMENTS.....	13
6.3.1	<i>Overview of the main process</i>	<i>14</i>
6.3.2	<i>Requirements of function F1 – Generate keys and certificate.....</i>	<i>15</i>
6.3.3	<i>Requirements of function F1.1 – Generate keys.....</i>	<i>15</i>
6.3.4	<i>Requirements of function F1.2 – Generate certificate</i>	<i>16</i>
6.3.5	<i>Requirements of function F2 – Recover private encryption key.....</i>	<i>17</i>
6.3.6	<i>Requirements of function F3 – Revoke certificate.....</i>	<i>17</i>
6.3.7	<i>Requirements of function F4 – Repudiate keys</i>	<i>18</i>
6.3.8	<i>Requirements of function F5 – Publish certificate in white list.....</i>	<i>18</i>
6.3.9	<i>Requirements of function F6 – Publish certificate in black list (CRL).....</i>	<i>18</i>
6.3.10	<i>Requirements of function F7 – Suspend certificate</i>	<i>18</i>
6.3.11	<i>Requirements of function F8 – Reactivate suspended certificate</i>	<i>18</i>
6.3.12	<i>Requirements of function F9 – Update certificate.....</i>	<i>18</i>
6.3.13	<i>Requirements of function F9.1 – Update expiration date of certificate for renewal</i>	<i>18</i>
6.3.14	<i>Requirements of function F10 – View event log</i>	<i>18</i>
6.3.15	<i>Requirements of function F11 – Recover certificate.....</i>	<i>19</i>
6.4	EXAMPLES OF EXISTING USE OF PKI	19
7	SECURITY REQUIREMENTS.....	20
8	LEGAL ISSUES	21
8.1	LICENSE	21
8.2	ELECTRONIC SIGNATURE	21
8.3	PERSONAL DATA PROTECTION	21
9	OTHER REQUIREMENTS.....	22
9.1	VOLUMETRY	22
9.2	BUDGET	22
9.3	PKI ADMINISTRATION	22
9.4	FUNCTIONAL ARCHITECTURE REQUIREMENTS	23
9.4.1	<i>Platforms.....</i>	<i>23</i>
9.4.2	<i>Protocols and standards.....</i>	<i>23</i>
9.4.3	<i>External devices</i>	<i>23</i>

9.4.4 *Modularity*..... 23
9.4.5 *Priorities for the build of PKI modules* 23
9.4.6 *List of other needs* 23
9.4.7 *Compatibility with examples of existing use of the PKI* 23

1 Document Control

<i>Issue</i>	<i>Date of Issue</i>	<i>Comments</i>
0.1	14 June 2002	Creation
0.2	21 June 2002	Amend and complete version 0.1
1.0	28 June 2002	Amend and complete version 0.2 To be validated on 04/06/2002 (draft review meeting)

1.1 Abstract

The purpose of the deliverable D3.5 'Draft of the definition of the perimeter of the project' is to communicate the results achieved during the three brainstorming meetings of the Work Package 3 to all members of the consortium.

The deliverables D3.2, D3.3 and D3.4 are merged into the deliverable D3.5 in order to determine the requirements for the EUPKI project.

1.2 Keywords

EUPKI	EUPKI, the libre software Public Key Infrastructure (project name)
WP3	Work Package 3
D3.1	Reference to the deliverable 'D3.1 Brainstorming requirements analysis'
D3.2	Reference to the deliverable 'D3.2 Report of the first meeting'
D3.3	Reference to the deliverable 'D3.3 Report of the second meeting'
D3.4	Reference to the deliverable 'D3.4 Report of the third meeting'
PKI	Public Key Infrastructure
GIP-MDS	Groupement d'Intérêt Public Modernisation des Déclarations Sociales
CGE&Y	Cap Gemini Ernst & Young

2 Management Overview

2.1 Executive Summary

This document contains the results achieved during the three brainstorming meetings of the Work Package 3. The outputs of the deliverables D3.2, D3.3 and D3.4 are included into the draft D3.5. The final version of the draft will be referred to as the deliverable D3.6 and will contain all requirements of the EUPKI project which will be the inputs of the Work Package 4.

2.2 Scope Statement

The scope of this document is to capture the results achieved during the three brainstorming meetings of the Work Package 3.

This document refers to the following external documents :

Reference	Document
D3.1	Brainstorming requirements analysis
D3.2	Report of the first meeting
D3.3	Report of the second meeting
D3.4	Report of the third meeting

3 Introduction and Glossary

3.1 Glossary

CRM	Customer Relationship Management
HR	Human Resources
OCSP	On-line Certificate Status Protocol

4 Perimeter of the EUPKI project

4.1 Perimeter

The use of the PKI as defined in the EUPKI project shall be possible in the following sectors :

- Public Services
- Financial Services
- Telco
- Utilities
- Health

All companies could make use of this PKI, whatever their size is (see §9.1 for volumetry).

The following examples of existing PKIs must be supported :

- Net-Entreprises
- Vital smart card
- Capkey, CGE&Y example of internal PKI
- Banking
- FT example
- FINSIEL example of pension fund PKI

The PKI functions which are within the scope of the EUPKI project are listed in §6 'PKI functions requirements'.

4.2 PKI Businesses and services

The PKI business and service scope is listed below.

Businesses	Services	Authentication	Signature	Encryption
e-Government scenarios	e-Voting	X		
	Electronic identity card	X		
	Secure identity	X		
	Social Security declarations		X	X
	Secure payments		X	X
	Secure e-Declarations		X	X
	Identification of subject	X		
	Administrative e-procedure		X	
	Tax declaration		X	X
	e-Procurement	X	X	X

Businesses	Services	Authentication	Signature	Encryption
Financial Services	Internet banking	X	X	X
	Internet insurance	X	X	X
	Secure banking	X	X	X
	Authentication in payments	X	X	X
	Operations of compensation	X	X	X
	Home banking	X	X	X
	Professional banking	X	X	X
	On-line insurance	X	X	X
Home Networking	Customer Home Networking (access to domestic control portal, to home computers ...)	X		
	Service Provider Home Networking (remote administration, remote maintenance ...)	X		
Telco	Secure access to Back-Office (network admin)	X		
	VPN	X		X
	Mobile services	X		
Utilities	Monitoring	X		
Health	Medical "paper" treatment	X	X	X
	Clinical essays	X		X
	Secure document exchange (secure mailing)		X	X
Internal PKI	Company dedicated PKI	X		
	Internal PKI	X		
	Work from home	X		
	EDI, ebXML		X	
	e-Procedures	X		
	Secure access to Information System (IS)	X		
	Secure e-mail		X	X
	Telecom infrastructure (VPN)	X		X
Grid computing	X	X		

Businesses	Services	Authentication	Signature	Encryption
Transverse	Electronic forms		X	X
	Electronic declarations		X	X
	Tele-declaration		X	X
	Code signing		X	
	Secure mailing		X	X
	e-Declaration (B2B)		X	X
	Secure access to IS		X	
	e-Order		X	X
	e-Billing		X	X
	e-Payment		X	X
	Contract Management		X	X

5 Users of the PKI

- **User**

The user is the subject of the certificate, whose identity and public key are implicitly bound together in the public key certificate.
The user may be :

 - a person
 - a citizen (public PKI)
 - an employee (internal PKI of a company)
 - a customer or a supplier (external PKI of a company)
 - a member of a community PKI (ON-X example : Openevidence)
 - an application
 - a server

- **Sponsor**

The sponsor is the entity which represents a set of PKI users.
The sponsor may be an application (HR application, CRM application).

- **Server administrator**

The server administrator is the sponsor of an application and/or of a server.

- **Auditor**

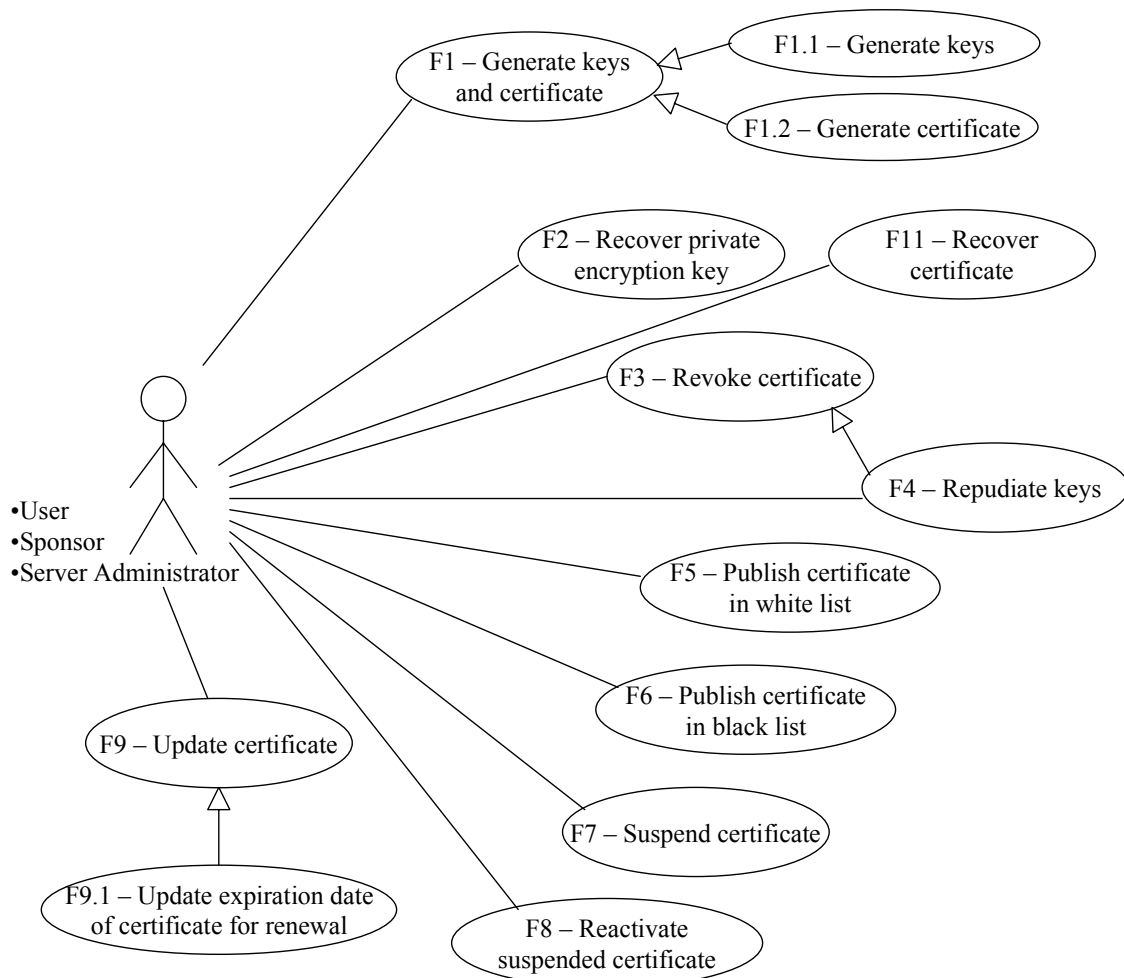
The auditor is the entity who is authorised to view event logs.

6 PKI functions requirements

This chapter lists a set of PKI functions requirements from an end user point of view rather than from an implementation point of view.

6.1 List of the PKI functions

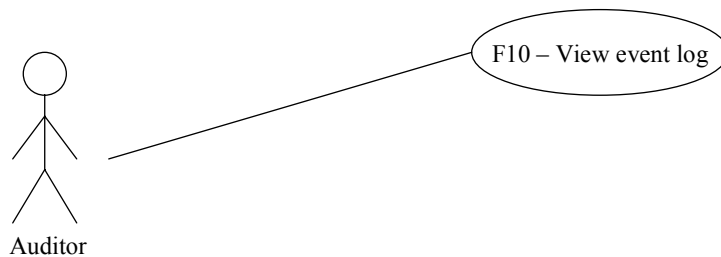
The PKI must provide the following functions to the user, sponsor and server administrator :



Functions	Description	User	Sponsor	Server Administrator
F1	Generate keysⁱ and certificate The following actions can be performed : <ul style="list-style-type: none"> • the keys generation only (F1.1), • the certificate generation only (F1.2), • the keys generation and the certificate generation in a row (F1.1 and F1.2). 	X	X	X
F1.1	Generate keys The generation of the private and the public keys can be performed for encryption and/or signature.	X	X	X
F1.2	Generate certificate The certificate can be used for encryption and/or signature.	X	X	X
F2	Recover private encryption key	X	X	X
F3	Revoke certificate The revocation can be performed for the certificate which is used for encryption and/or signature.	X	X	X
F4	Repudiate keys	X	X	X
F5	Publish certificate in white list The white list contains the certificates used for encryption and/or signature.	X	X	X
F6	Publish certificate in black list (CRL) The black list contains the certificates which were revoked, whether there are used for encryption only, for signature only or for both.	X	X	X
F7	Suspend certificate The certificate used for encryption and/or signature can be suspended.	X	X	X
F8	Reactivate suspended certificate The certificate which were suspended and which were used for encryption and/or signature can be reactivated.	X	X	X
F9	Update certificate Any information contained in a certificate can be updated, including the expiration date of the certificate (F9.1).	X	X	X
F9.1	Update expiration date of certificate for renewal The expiration date of the certificate used for encryption and/or signature can be updated so that the certificate can be used for a longer period of time.	X	X	X
F11	Recover certificate	X	X	X

ⁱ As these keys are mentioned without specific characteristics, these keys are the private key and the public key.

The PKI must provide the following functions to the auditor :



Functions	Description	Auditor
F10	View event log The auditor can view the event log which must be timed with a reliable time source (in French : 'horodatage'). The auditor can filter this log to view the events related to a specific community within a specific period of time.	X

6.2 Some functions out of the scope of the EUPKI project

The following functions are outside the scope of the EUPKI project :

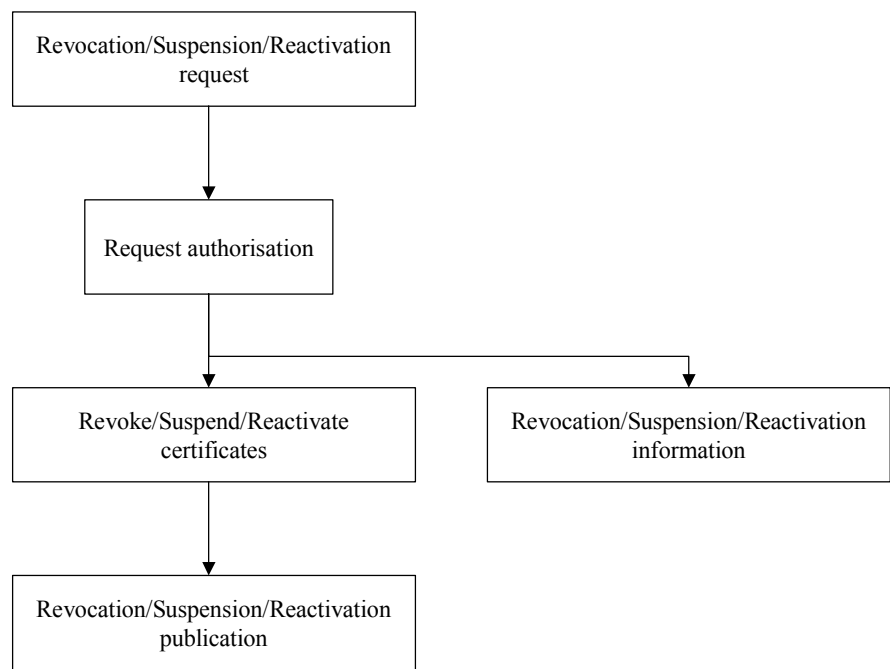
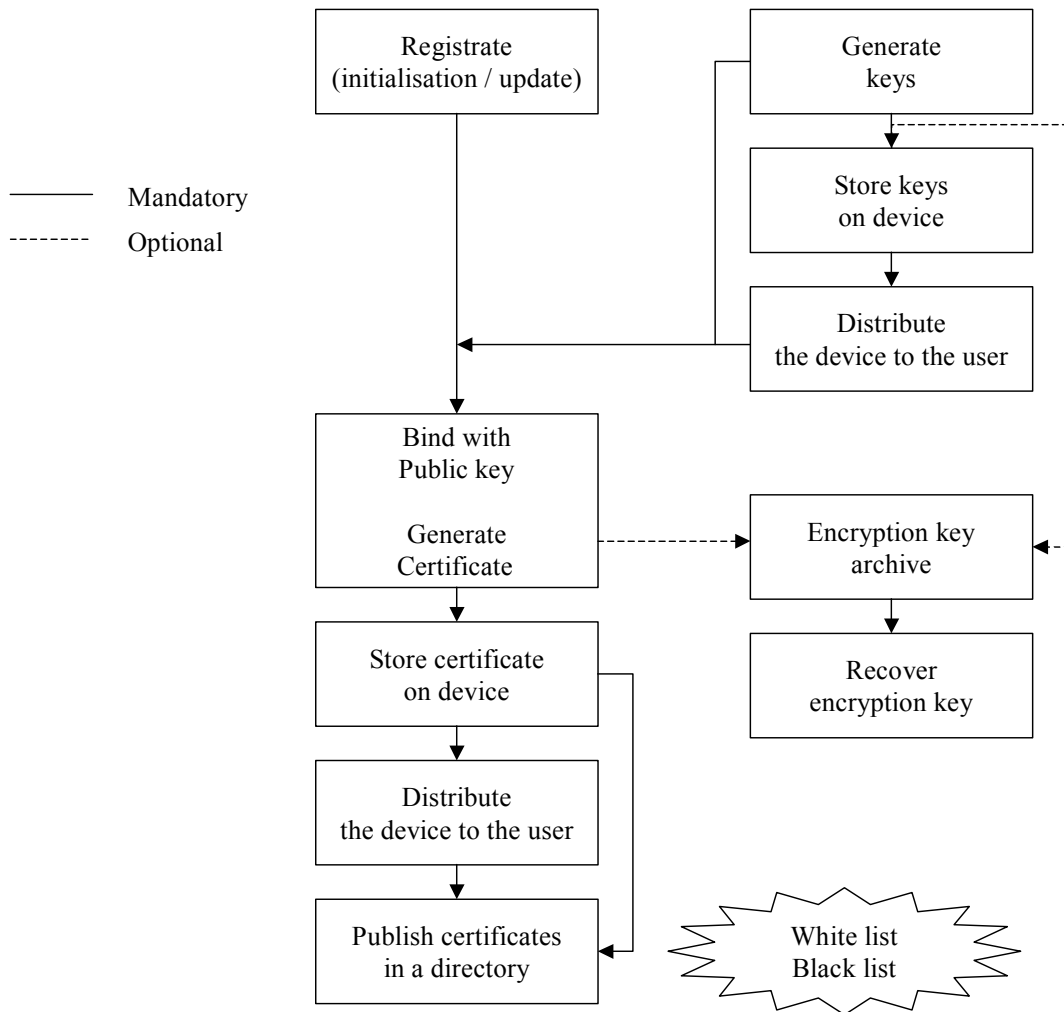
- Time-stamping service
 - Definition of time-stamping : the use of date and time within the digital signature.
- The build of the reliable time source used for the event log is outside of the scope of the EUPKI project.
 - Time-stamping and 'horodatage' are two different services. 'Horodatage' is within the scope of the EUPKI project (the use of the reliable time source but not the build of it) while time-stamping is not.
- Certificate validation service based on On-line Certificate Status Protocol (OCSP).

6.3 Functions requirements

This paragraph provides some additional requirements of the PKI functions which are listed in §6.1 'List of the PKI functions'.

Chapters §6.3.2.to §6.3.13 refer to the main process described in chapter §6.3.1 'Overview of the main process'.

6.3.1 Overview of the main process



6.3.2 Requirements of function F1 – Generate keys and certificate

Functions F1.1 (see §6.3.3) and F1.2 (see §6.3.4) can be performed separately or can be triggered by the function F1.

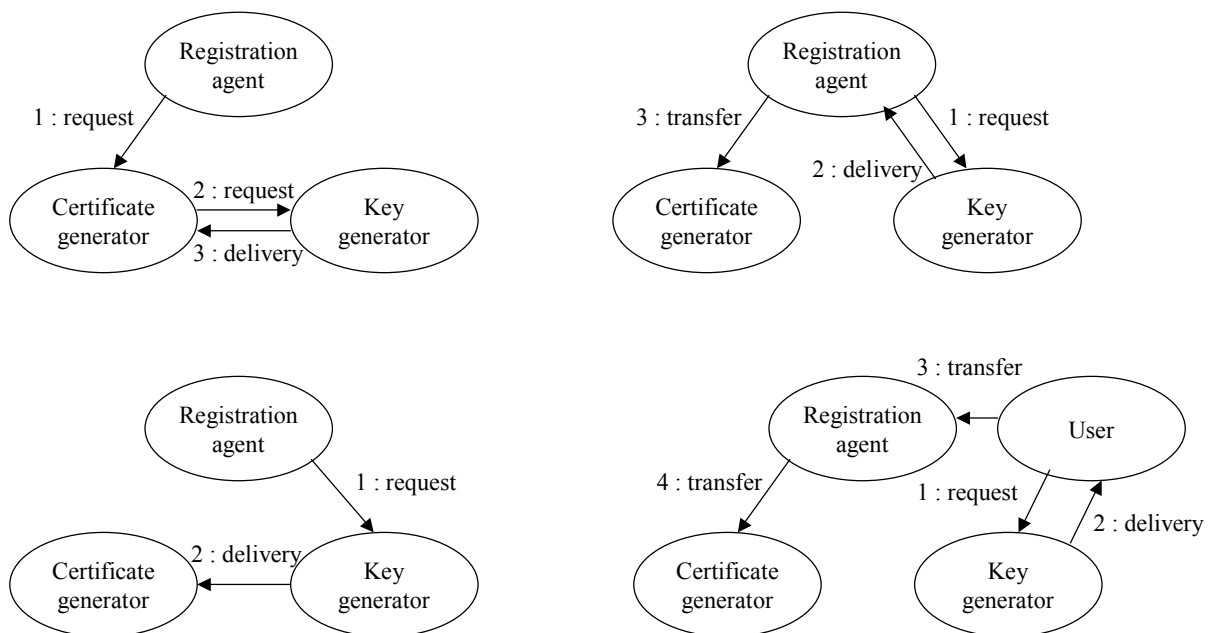
6.3.3 Requirements of function F1.1 – Generate keys

The PKI must allow the generation of keys on smart cards. The key generation can be performed either by the PKI or by the user.

The only client-side component which is mandatory to deliver is the software key generator which would therefore replace the Internet browser key generator. The reason for this is that, despite the wide use of Internet Explorer, its key generator is not an open source key generator.

The client-side key generator must be easy to install/uninstall with an automatic installation procedure. It must be compatible with Internet Explorer and Netscape.

The keys generation can be processed in different ways as shown below :



The lower-right scheme in the above processes uses a key generator which is either a centralised key generator or a client-side key generator.

The private key of the user must be protected so that it can be used only by the user it belongs to.

There are mainly three ways of protecting the private key :

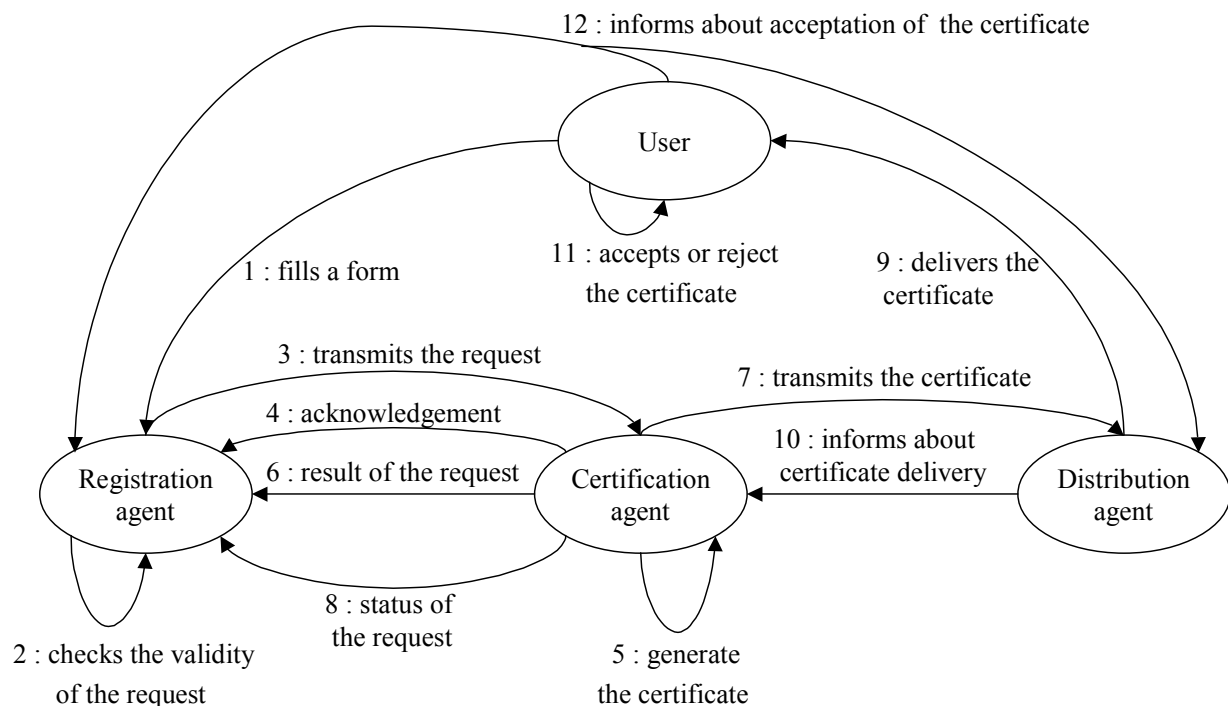
- password chosen by the user,
- pin code provided by the key generator,
- public key of the registration agent.

The PKI must force any user public key to be unique, which implies that two users cannot have the same public key :

- Only centralised key generation allows full control of the unicity of public keys.
- To facilitate the transition period when renewing one's certificate, the PKI must allow a user to have two certificates with his/her same public key.

6.3.4 Requirements of function F1.2 – Generate certificate

The certificate generation from the user request through the delivery of the certificate can be processed as follows :



The user fills a form to generate a certificate.

- Context : The user already generated his/her keys (public and private) the user provides his public key to the registration agent,
- or
- Context : The user has NOT generated his/her keys (public and private) the user requests to have his/her keys generated - the private key can be optionally protected by a password chosen by the user.

The registration agent checks the validity of the request, which status can be :

- pending,
- accepted,
- rejected.

The registration agent transmits the request (with the user information needed by the PKI and the user public key) to the certification agent after having signed it :

- manually (electronic forms),
- or
- automatically (batch or real-time).

The user accepts or rejects the certificate and informs at least one of the actors (distribution agent and/or registration agent and/or certification agent) of his/her decision.

According to RFC 2510, the proof of possession of the private key can occur either at the very beginning of the process (2 : checks the validity of the request) or at the acceptance of the certificate (11 : accepts or reject the certificate).

The certificate generation can also be automatically processed e.g. in a company : the staff database can be accessed by the PKI application.

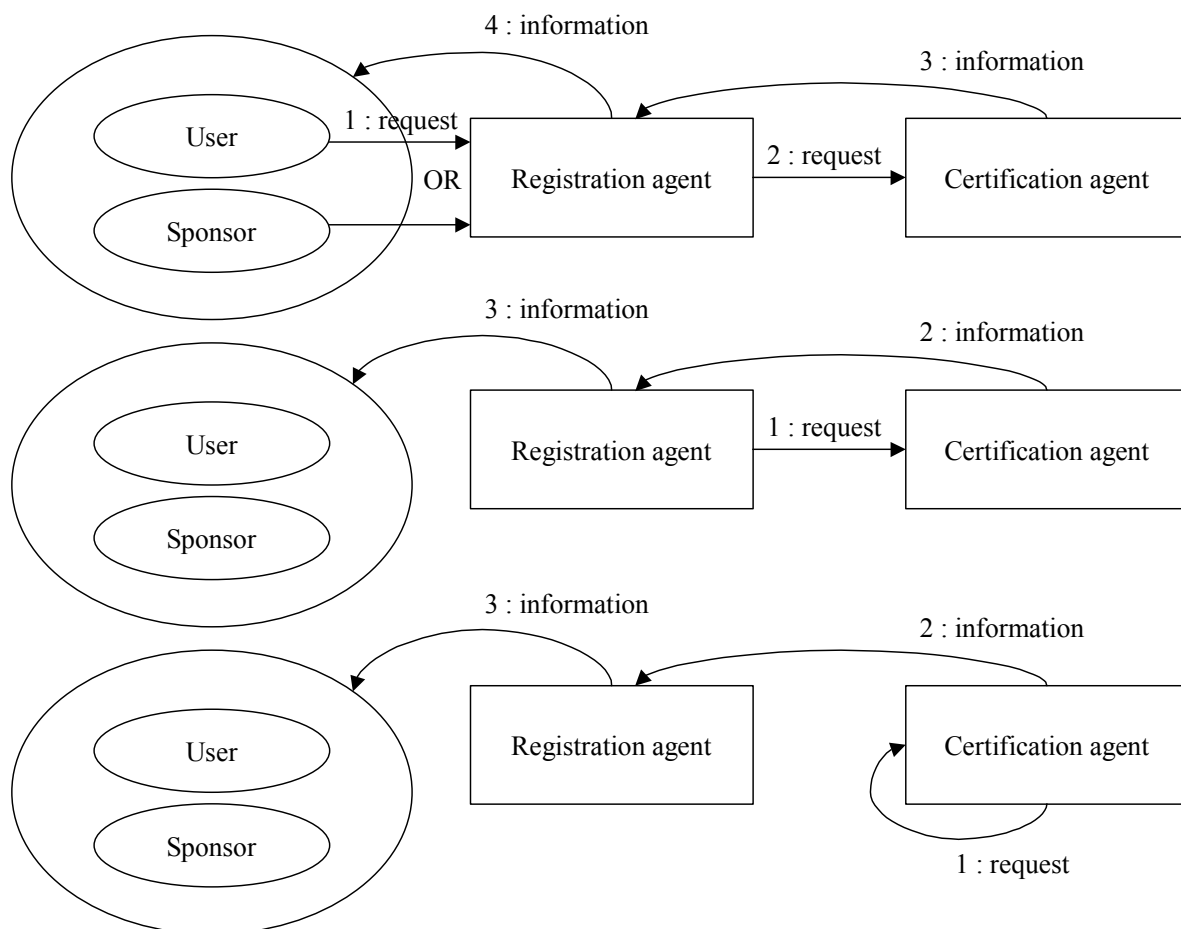
6.3.5 Requirements of function F2 – Recover private encryption key

The recovery of the private encryption key is a PKI function that is definitely needed for most applications, including medical applications.

The key archive system is important.

6.3.6 Requirements of function F3 – Revoke certificate

Certificates can be revoked in various ways as shown below :



The actors can revoke certificates depending on their rights.

6.3.7 Requirements of function F4 – Repudiate keys

The repudiation of keys also triggers the revocation of the corresponding certificate (see §6.3.9).

6.3.8 Requirements of function F5 – Publish certificate in white list

Generally speaking, the publishing of any certificate shall provide as little information as possible about its owner in order to avoid any commercial abuse.

There is no legal obligation to publish the white list, as opposed to obligation of publishing the black list. Anyway the PKI must allow the publishing of the white list since owners or group of owners of certificates (e.g. company) can decide whether his/her certificate can be published. For example, it is up to a company to decide who can view the white list of its employees certificates (e.g. whether the white list can be viewed only by its employees or also by the public).

6.3.9 Requirements of function F6 – Publish certificate in black list (CRL)

The publication of the black list (Certificate Revocation List) is mandatory according to the law.

6.3.10 Requirements of function F7 – Suspend certificate

Certificates which have been suspended are listed in the black list.

6.3.11 Requirements of function F8 – Reactivate suspended certificate

Certificates which have been reactivated must be removed from the black list.

6.3.12 Requirements of function F9 – Update certificate

The update action can be performed in order to change any information stored within the certificate such as the name of the owner of the certificate, the expiration date, the keys.

6.3.13 Requirements of function F9.1 – Update expiration date of certificate for renewal

The function F9 can perform the same action than the function F9.1.

6.3.14 Requirements of function F10 – View event log

The PKI must have a secure event log mechanism in terms of :

- Availability,
- Integrity,
- Confidentiality,
- Management of rights.

The event log outputs must be easily re-used (e.g. event logs with standard format can be easily processed by auditors) and therefore must use a non-proprietary format of storage.

The PKI must allow the information related to a specific community within a period of time to be easily extracted from the event log.

All logged events must be timed using a reliable time source.

This PKI function performs not only the storage of evidences but also the storage of the details of the person to whom the certificate was issued and the reasons why it was issued.

6.3.15 Requirements of function F11 – Recover certificate

Any certificate can be recovered when lost by the owner.

This function can be very useful when the white list is not published.

6.4 Examples of existing use of PKI

The list below maps existing PKIs with EUPKI functions. s

Functions → ↓ Examples	F1	F1.1	F1.2	F2	F3	F4	F5	F6	F7	F8	F9	F9.1	F10	F11
Capkey	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	No	No	No	Yes	No
France Telecom														
Italian Pension Fund	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	No	No	No	Yes	
Net-Enterprises														
Vital														

7 Security requirements

The following security requirements are made from the AQL proposal :

Assets	Confidentiality	Integrity	High Availability	Comments
Keys	Protect the private key, the pin code and the password. Distribute the keys to the right actor.	X		The authorised actor can : <ul style="list-style-type: none"> • Generate keys (public and private) • Recover encryption key • Repudiate keys
Certificate	Protect the personal data (identity, evidences) Distribute the certificate to the right actor.	X		The authorised actor can : <ul style="list-style-type: none"> • Generate certificate • Update certificate • Suspend certificate • Reactivate certificate • Revoke certificate
White List	Protect information contained in the white list	X		The authorised actor can : <ul style="list-style-type: none"> • Publish his/her/its certificate(s) • View the white list
Black List		X	X	
Event Log	Protect information contained in the event log	X		The authorised actor can : <ul style="list-style-type: none"> • View the event log

Nota. – The Availability column contains the needs for high availability ('X' means highly available, while a blank means standard availability).

8 Legal issues

8.1 License

The EUPKI project will use Mozilla and lesser GPL instead of GPL (GNU Public License) so that the code which will be produced in the EUPKI project or in any project using the code produced by the EUPKI project will not become some GPL code.

8.2 Electronic signature

The Italian law identifies 3 distinct levels of security, ordered by increase :

- electronic documents,
- digital signature and certificate (smart card is not mandatory),
- key and certificate generated on smart card (example : Italian public services).

Our PKI must also be able to deliver qualified certificates, which therefore enable the delivery of non-qualified certificates.

8.3 Personal data protection

- The PKI must have at least the same obligations than those of any Information System which deals with personal data.
- Higher level protection of personal data may be needed in the health sector.
- A European directive forces the use of a pseudonym but the way to implement it in France is not yet defined.

9 Other requirements

9.1 Volumetry

The following deployment requirements in terms of volumetry constraints are identified :

- Millions of users for :
 - e-Government,
 - Social services,
 - Home Networking,
 - Telco,
 - Utilities;
- Thousands of users for :
 - Financial Services,
 - Internal PKI;
- Hundreds of users for :
 - Small companies;
- Batch processes

9.2 Budget

The following requirements related to budget constraints are identified :

- Software/client browser certificates,
- Centralised generated certificates HSM,
- Software certificates generated by a applet which is downloaded,
- Type and quality of the registration (e.g. face-to-face registration),
- Certificates stored on a physical device (e.g. SM, token, etc.),
- Life time validity of certificates,
- Number of PC used,
- Number of RA,
- Number of Operators,
- Level of service for all PKI modules,
- Request and delivery of a certificate happen during the same session,
- Time to deliver,
- Key length,
- Number of certificates that can be stored on the same device,
- Diversity of certificates,
- Level of certificate.

9.3 PKI Administration

The following needs for the administration of a PKI have been identified :

- Initialisation,
- Key ceremony,
- Key recovery,
- Split responsibilities,
- Event log (see function F10 "View event log" in §6.1 and §6.3.14),
- Administration of roles.

9.4 Functional architecture requirements

The functional architecture of the PKI is part of the WP3 while the technical architecture of the PKI is not, but part of the WP4.

9.4.1 Platforms

The PKI must be platform independent.

The PKI must allow a very easy and cost effective portability to the following platforms : Linux, Unix and Windows NT.

9.4.2 Protocols and standards

The PKI must use open standards in order to :

- store any PKI data,
- facilitate the migration of PKI data.

The PKI must use open high level protocols and standards.

9.4.3 External devices

The PKI can use a Hardware Storage Module for the key generation and the cryptographic processes.

9.4.4 Modularity

The PKI shall make full use of modularity.

9.4.5 Priorities for the build of PKI modules

High priority has been defined on the following PKI modules :

- Registration Authority
- Certification Authority
- Protocols

9.4.6 List of other needs

The following needs are identified :

- Localisation (language specificities such as accents, etc.),
- Connexion to external sources (external databases, etc.),
- Documentation,
- Ease of installation,
- Maintainability & maintenance,
- Ease of administration,
- Key ceremony (generating process),
- Ease of renewal process.

9.4.7 Compatibility with examples of existing use of the PKI

The PKI must be designed so that it can be used within the examples described in §6.4 'Example of existing use of PKI'.