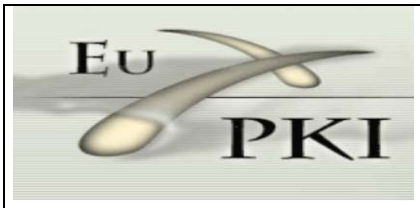


IST-2001-34340
D3.6 Definition of the perimeter of the project and requirements

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 February 2003
Issue :	1.5
File Name :	EUPKI-WP3-D3.6-1.5.doc
Work Package :	WP3 Requirements
Deliverable Number :	D 3.6
Deliverable Type :	Public
Deliverable Nature :	Approved WP3 report
Total Number of Pages :	52
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

1 Document Control

Issue	*Date of Issue*	*Comments*
0.1	12 July 2002	Creation
1.0	19 July 2002	Amendments from FINSIEL, FT and GIP-MDS. Input on security requirements from AQL
1.1	30 August 2002	Amendments from ON-X. Input on administration requirements from Certinomis
1.2	16 September 2002	Amendments from CGE&Y Add the answers to the EUPKI questionnaire
1.3	18 September 2002	Amendments from CGE&Y on administration functions
1.4	26 September 2002	Amendments determined in the 2nd steering meeting
1.5	28 February 2003	Amendments from CGE&Y Add legal issues

1.1 Abstract

This deliverable D3.6 'Definition of the perimeter of the project and requirements' is produced from the deliverable D3.5 'Draft of the definition of the perimeter of the project' and the amendments determined in the Draft review meeting held on 04/07/2002 in Munich.

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'
D3.5 Reference to the deliverable 'D3.5 Draft of the definition of the perimeter of the project'
PKI Public Key Infrastructure
GIP-MDS Groupement d'Intérêt Public Modernisation des Déclarations Sociales
CGE&Y Cap Gemini Ernst & Young
FT France Telecom

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 were included into the draft D3.5. This deliverable D3.6 is the final version of the draft and contains all requirements of the EUPKI project which will be the inputs of the Work Package 4. It was approved in the 2nd Board meeting held on 24/09/2002 in Paris.

2.2 Scope Statement

The scope of this document is to capture the results achieved during the three brainstorming meetings and the Draft review meeting 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
D3.5	Draft of the definition of the perimeter of the project

3 Introduction and Glossary

3.1 Glossary

B2B	Business to Business
CRL	Certificate Revocation List
CRM	Customer Relationship Management
EDI	Electronic Data Interchange
HR	Human Resources
IS	Information System
OCSP	On-line Certificate Status Protocol
SM	Smart Card
VPN	Virtual Private Network
XML	Extended Mark-Up Language

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 §10.1 scalability).

The following examples of existing PKIs must be supported :

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

CGE&Y, FINSIEL and FT examples are described in §11.

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

5.1.1 External users

- **End 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.

5.1.2 Internal users

- **PKI administrator**
  The PKI administrator is responsible for establishing, distributing, maintaining, promoting and enforcing certificate and security policies.
  He may be :
  - a public service in a public PKI
  - a company in an internal or external PKI, for example a bank with his customers.

- **PKI operator**
  The PKI operator is an entity authorized or accredited by the PKI administrator to perform a PKI functional role under the established policies.
  He may be :
  - a registration agent
  - a certification agent
  - a distribution agent.

6 PKI functions requirements for external users

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 keys[i] and certificate** The following actions can be performed : • 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 a directory** The directory contains the certificates used for encryption and/or signature.	x	x	x
F6	**Publish certificate in Certificate Revocation List** The CRL contains the certificates which were revoked and suspended, 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

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

F9	**Update information in a certificate** Any information contained in a certificate can be updated, including the expiration date of the certificate.	x	x	x
F9.1	**Renew certificate** Generate a new certificate with updated informations.	x	x	x
F11	**Recover certificate** The owner needs to recover his certificate when he has lost it.	x	x	x

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 :

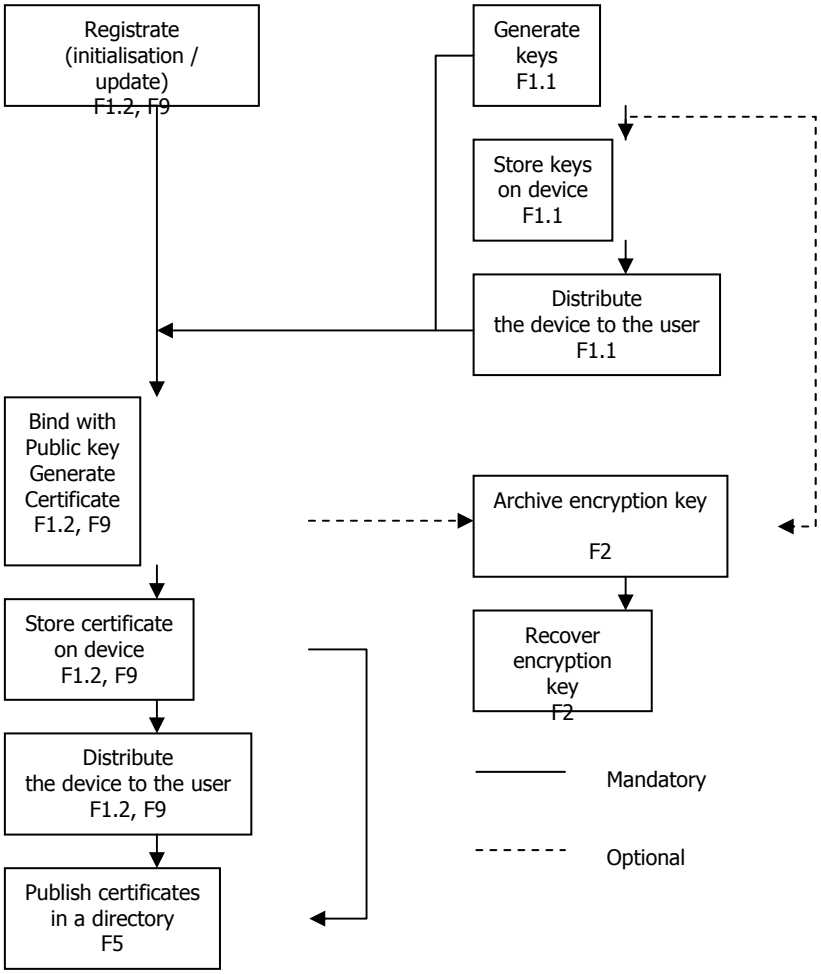
- Time-stamping service
  - Definition of time-stamping : the use of date and time within the digital signature.
- The build of the reliable time source used for the event log is outside of the scope of the EUPKI project.
  - Time-stamping and 'horodatage' are two different services. 'Horodatage' is 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) or any other protocol.

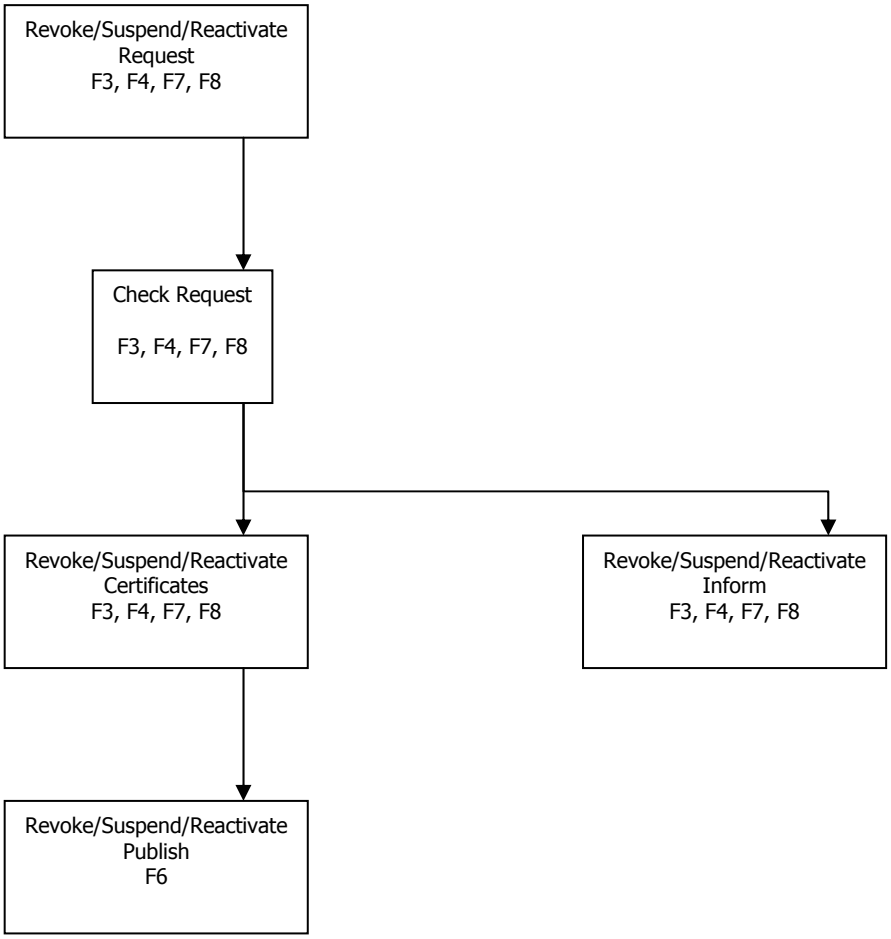
6.3 Functions requirements

This paragraph provides some additional requirements of the PKI functions that 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 mapped with PKI functions




Revoke/Suspend/Reactivate Request
F3, F4, F7, F8
Check Request
F3, F4, F7, F8
Revoke/Suspend/Reactivate Certificates
F3, F4, F7, F8
Revoke/Suspend/Reactivate Inform
F3, F4, F7, F8
Revoke/Suspend/Reactivate Publish
F6

6.3.2 Requirements of function F1 – Generate keys and certificate

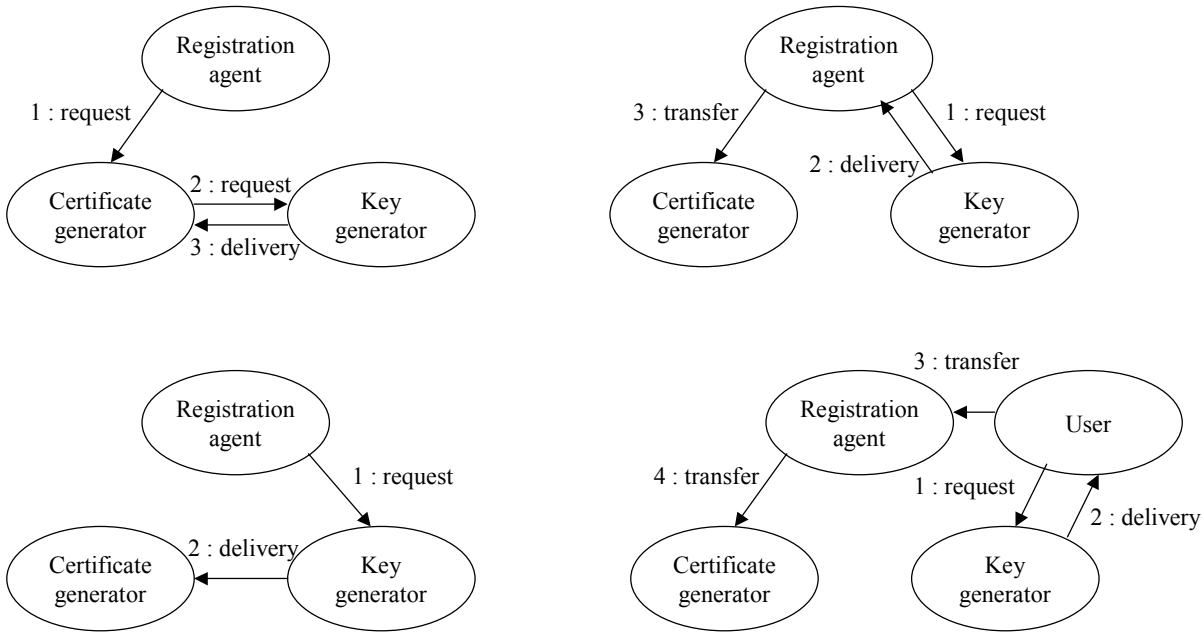
Functions F1.1 (see §6.3.3) and F1.2 (see §6.3.4) can be performed separately or can be triggered by the function F1.

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 use of this client-side key generator is not compulsory for a EUPKI user.

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. In this case, the private key will be stored and distributed on a device to the user.
In the other cases, it can be stored with the certificate on the same device or on a separate device.

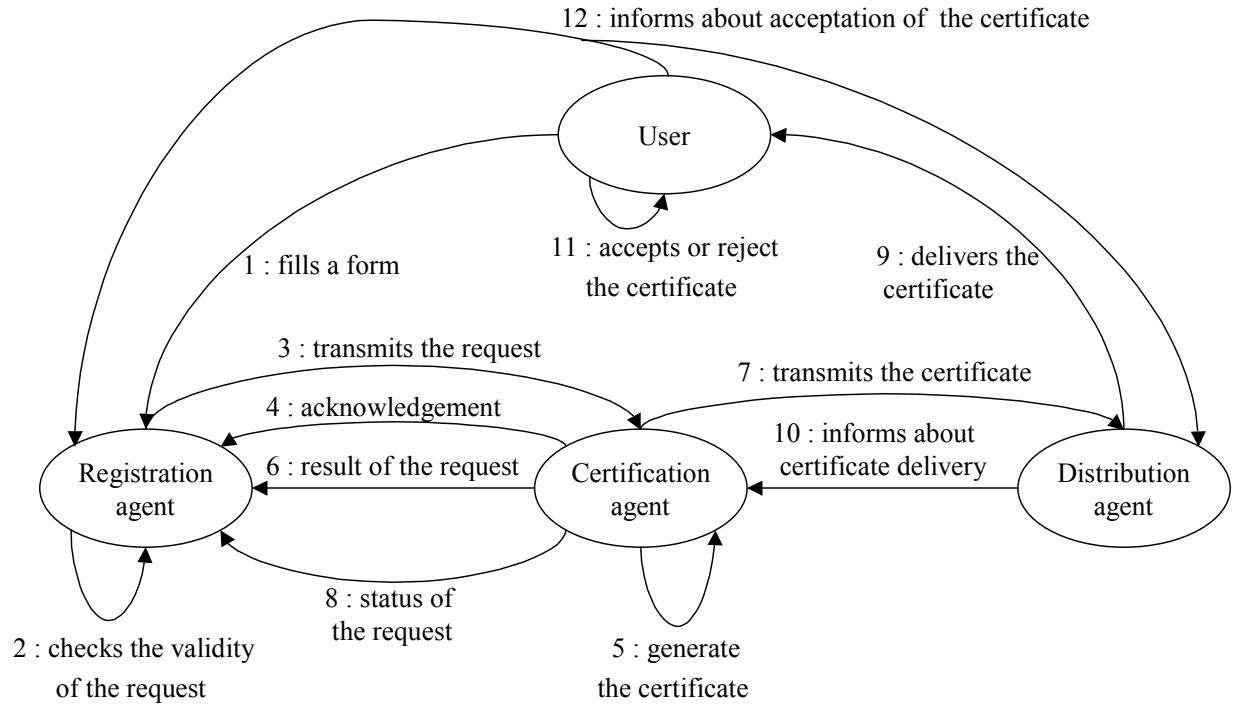
The private key of the user must be protected so that it can be used only by the user it belongs to.

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 has not to force any user public key to be unique but the key generator should be a good quality random generator specially in the case of a centralized key generator.

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 an electronic form to generate a certificate or proceeds a face to face registration.
- Context 1 : The user has already generated his/her keys (public and private)
  the user provides his public key to the registration agent,

or
- Context 2 : 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 generated in different ways described in §6.3.3 except the lower-right scheme. The private key and the certificate can be :
  - stored on separate devices and distributed separately to the user

  or
  - stored and distributed on the same device.

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 (bulk 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 in a bulk mode in large PKIs with millions or thousands of users.

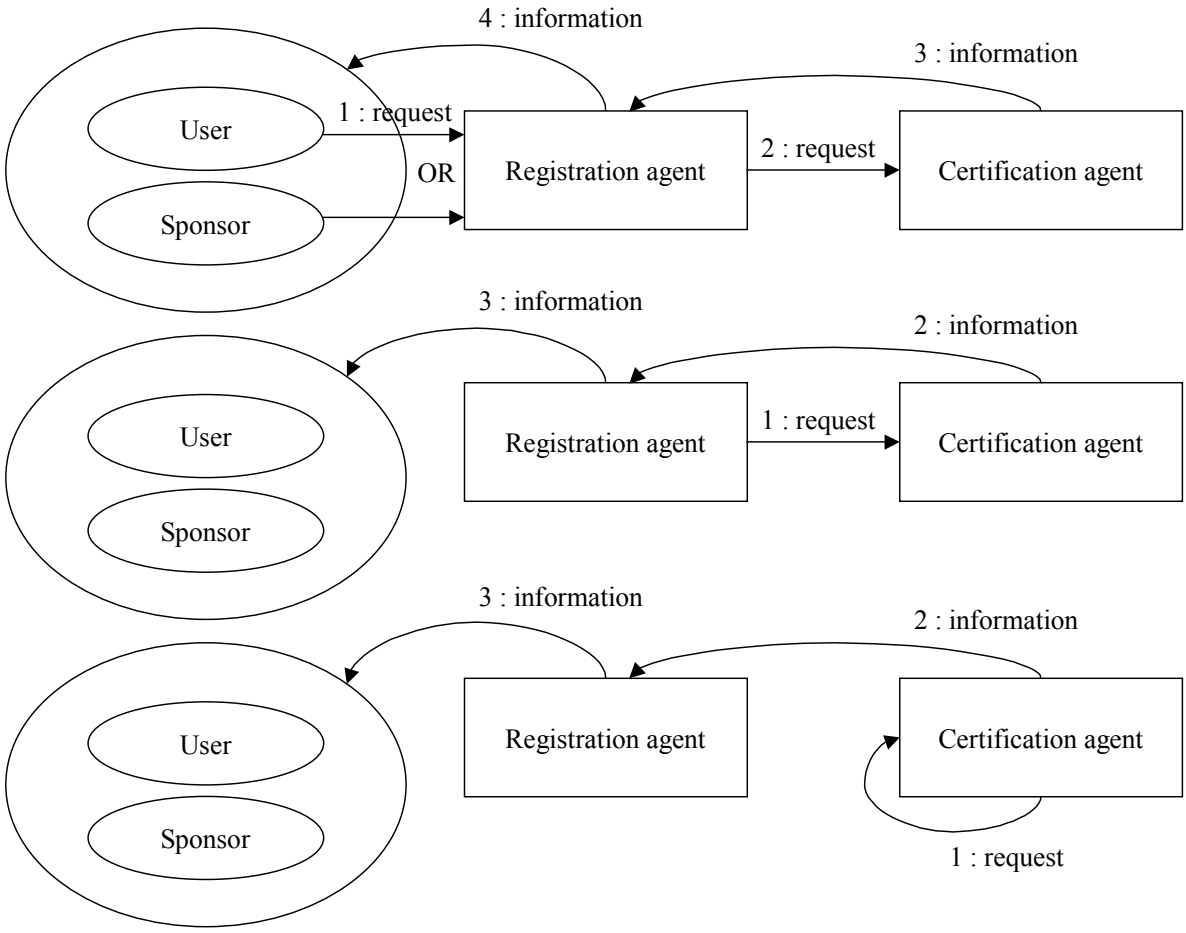
6.3.5 Requirements of function F2 – Recover private encryption key

The recovery of one or an historic of private encryption keys is a PKI function that is needed for most applications which make use of encryption, including medical applications, secure e-mail, etc.

The PKI has to be able to interface with a key archive system.

6.3.6 Requirements of function F3 – Revoke certificate

Certificates can be revoked in various ways as shown below :



The actors can ask for the revocation of certificates depending on their rights.

The certificate revocation can be automatically processed in a bulk mode.

6.3.7 Requirements of function F4 – Repudiate keys

The repudiation of keys also triggers the revocation of the corresponding certificate.

6.3.8 Requirements of function F5 – Publish certificate in a directory

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 directory, as opposed to obligation of publishing the CRL. Anyway the PKI must allow the publishing of the directory 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 directory of its employees certificates (e.g. whether the directory can be viewed only by its employees or also by the public).

6.3.9 Requirements of function F6 – Publish certificate in a Certificate Revocation List

Certificates which have been revoked are listed in the CRL.
The publication of the CRL is mandatory according to the law.

6.3.10 Requirements of function F7 – Suspend certificate

As for revocation, the same actors can ask for the suspension of certificates depending on their rights.
Certificates which have been suspended are listed in the CRL.

6.3.11 Requirements of function F8 – Reactivate suspended certificate

Certificates which have been reactivated must be removed from the CRL.

6.3.12 Requirements of function F9 – Update information in a 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 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.

6.3.13 Requirements of function F9.1 – Renew certificate

This function generates a new certificate with informations updated through function F9.

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 and stored for appropriate and configurable duration.

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.

Only authorised actors like auditors can view this event log.

6.3.15 Requirements of function F11 – Recover certificate

Any certificate can be recovered when lost by the owner who can show the proof of possession of the private key.

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

6.4 Examples of existing use of PKI

The list below maps existing PKIs with EUPKI functions.

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	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	No	No	Yes	Yes
Italian Pension Fund	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	No	No	No	Yes	No

7 PKI functions requirements for internal users

7.1 PKI administration

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

- Initialisation,
- Key ceremony,
- Key recovery,
- Split responsibilities,
- Logging,
- Archives,
- Administration of profiles.

7.2 List of PKI administration functions

Functions	Description
	Manage the PKI configuration
F12	Create a Certificate profile where the rules to construct the certificate are described
F13	Create a Certification Authority associated with one or more Certificate profiles This Certification Authority will generate certificates compliant to the associated Certificate profiles
F14	Create a Registration Policy associated with one Certification Authority and where the identifying information set is described
F15	Create a Registration Authority associated with one or more Registration policies This Registration Authority will registrate and transmit the request to the Certification Authority described in the Registration policy
	Manage the PKI administrators and operators
F16	Configure in a centralized mode the profiles where the privileges are described
F17	Create an administrator or an operator associated with a profile
F18	Update information or associated profile of an administrator or operator
F19	Delete an administrator or an operator
	Manage the statistics and the logs
F20	Consult the list and the historic of requests (generation, revocation) and their status (pending, accepted, rejected)
F21	Consult the status of the platforms, processes and cryptographic devices
F22	Consult the different logs in a detailed view
F23	Consult alarms when a major event or a problem happens (attack, crash …)
F24	Consult statistics about platforms (activity, access, security)
F25	Consult the different logs in a consolidated view through a centralized interface

8 Security requirements for a potential evaluation

Our references on security requirements :

- EC SSCD Profile of Protection n°CWA 14167-2
- French PKI Profile of Protection PPnc0004
- French RA Profile of Protection PPnc0005
- French CA Profile of Protection PPnc0006.

8.1 Assets

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 : • Generate keys (public and private) • Recover encryption key • Repudiate keys
Certificate	Protect the personal data (identity, evidences) Store personal data for a limited time Distribute the certificate to the right actor.	X		The authorised actor can : • Generate certificate • Update certificate • Suspend certificate • Reactivate certificate • Revoke certificate
Directory	Protect information contained in the directory	X		The authorised actor can : • Publish his/her/its certificate(s) • View the directory
CRL		X	X	The revocation process has to be highly available.
Event Log	Protect information contained in the event log	X		The authorised actor can : • View the event log

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

The right or habilitation of an actor to perform an action have to be defined in a directory for example.

8.2 Assumptions

8.2.1 Mandatory Assumptions

Assumption 1	Procedural measures are available to verify the identity of an end-user.
Assumption 2	Physical access to the CA is restricted to operators and system/database administration staff.
Assumption 3	Physical access to the RA is restricted to operators, RA administrator and system/database administration staff.
Assumption 4	Operators will keep their password or passphrases secret and change them at regular intervals.

8.2.2 Optional Assumptions

Optional assumption 1	Network links between TOE Components and Database(s) are protected from eavesdropping in accordance with a defined security policy that defines suitable countermeasures to mitigate any risk factors to an acceptable level.
Optional assumption 2	Procedural measures are in place to ensure that CRLs and ARLs are made available in a timely manner, to end users and applications that are using certificates issued by CAs in the PKI hierarchy. Users are responsible for the correct use of such CRLs and ARLs, in accordance with policies and procedures issued by the operators of the TOE e.g. Certificate Practice Statement.

8.3 Threats

T 1	Creation of untrusted certificate	An attacker may attempt to create an untrusted certificate and masquerade as a holder of a trusted certificate.
T 2	Unauthorised request for certificate	An attacker may attempt to masquerade as a valid requestor of a certificate by impersonating an authorised operator.
T 3	Unauthorised modification of CRP	An attacker may attempt to amend the Customer Registration Policy which is enforced by an operator for registering end users.
T 4	Unauthorised access to private keys	An attacker may attempt to obtain access to the private key of a component or an end user.
T 5	Unauthorised modification of certificate	An attacker may attempt to modify a trusted certificate.
T 6	Unauthorised revocation	An attacker may attempt to revoke a valid certificate without authorisation.
T 7	Undetected modification/deletion of CRL or ARL	An attacker may attempt to modify or delete a CRL or ARL to prevent revocation of invalidated certificates.
T 8	Undetected modification of audit log entry	An attacker may attempt to modify entries within the audit log.
T 9	Carry out undetected attack on the system	An attacker may attempt to mount a direct attack on the system without detection.
T 10	Generate bad keys	The keys generated by the product may be invalid or may be more repetitions of previous keys.
T 11	Corrupt the TOE data	The information managed by the TOE is corrupted, accidentally or intentionally, during their storage or of their transport between components of the IGC or towards the outside of the latter.
T 12		The TOE is unable to provide availability policy for registration or revocation requests.
T 13		A user or an owner denies to be the author of an action.

9 Legal issues

9.1 License

According to the Annex1 of the contract, the EUPKI project will be available in a GPL-compatible license form.

9.2 Electronic signature

The European Union has issued an European Electronic Signature Directive (1999/93/EC of 13 December 1999) and most of the individual Member Countries have already implemented this framework into national law.

9.2.1 Main Points of the EU Directive

The EU Directive defines the requirements for electronic signature certificates and certification services to ensure "minimum levels of security".
The following paragraphs show a synthesis (cf. details in appendix) of the main points of this directive.

9.2.1.1 Legal recognition of electronic signature

- Electronic signatures cannot be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that they are in electronic form (cf. art 5 § 2).
- If a certificate, the service provider, and the signature product used meet a set of clearly defined specific requirements (an "**advanced electronic signature based on a qualified certificate created by a secure-signature-creation device**"), there will be an automatic assumption that any resulting electronic **signatures are just as legally valid as a hand-written signature** (cf. art 5 § 1).

9.2.1.2 Free circulation within EU

All products and services **related to electronic signatures can circulate freely** within the UE and are only subject to the legislation and control by the country of origin (cf. art 4 § 2 and art 3).

9.2.1.3 Liability for services providers

The legislation of each member states should establish **liability** rules for **service providers** (cf. art 6) who would, in particular, be liable for the validity of a certificate's content.

9.2.1.4 Public scope

The directive covers certificates that are supplied to the public for identifying the sender of an electronic message : **it** does **permit the operation of systems governed by private law agreements** such as corporate Intranets or banking systems, where a relation of trust already exists (cf. art 1).

9.2.1.5 Privacy protection

Electronic signatures shall not make data mining easier (cf. art 8) and the freedom of using pseudonyms is a granted individual right.

9.2.1.6 Consumer protection

The directive establishes minimum liability for users (cf. art 6) and **assures** the **transparency of technological issues** for them since the requirements for qualified certificate (Annex I), secure signature creation device (Annex III) and trustworthy systems (Annex II) are defined in a functional way.

9.2.1.7 International dimension

The directive includes **mechanisms** for co-operation with third countries **based on mutual recognition of certificates** and on bilateral and multilateral agreements (cf. art 7).

9.2.2 Practical Meanings of the EU Directive

As shown before, the main objectives of the Directive was :

- To make sure that all of the European Member States accept the legal validity of an electronic signature;
- To make sure that all services relating to electronic signatures can be provided in a European Union (EU) market without national obstacles.

The following paragraphs show the practical meanings of this directive.

9.2.2.1 Legal Issues

Electronic documents to which an electronic signature has been appended **cannot be denied legal validity by a judge only because they are made by electronic means** but:

- A judge can still decline giving legal value to an electronic signature because he or she assumes that the security was not high enough to make it trustworthy;
- A judge can deny giving the legal value of a hand-written signature to someone's electronic signature if that person used an electronic signature which is not qualified.

9.2.2.2 Certification Service Providers Issues

Certification Services can be provided on an EU market without being confronted with national legal barriers (for instance a national licensing system): a CSP does not need a positive agreement of any kind from national authorities if it wants to have access to a national market.

Member States are, however, allowed to have voluntary accreditation schemes for the purposes of an enhanced level of certificate services but :

- This scheme should exist apart from the EU scheme;
- This scheme is on a voluntary basis : **no certification service should be obliged to participate in this scheme.**

9.2.2.3 Member States Issues

Member States are obliged to install a supervisory system to control the CSPs that are established on its territory:

- CSPs willing to issue qualified certificates will only have to meet the conditions of Annex II;
- The establishment of private-sector-based supervision systems are not excluded by the Directive.

With respect to the use of electronic signatures **in the public sector, Member States are permitted to make them subject to additional requirements**:

- These requirements should be objective, transparent, proportionate and non-discriminatory, and only relate to the specific characteristics of the application concerned;
- Typical examples are the implementation of enhanced secure electronic signature schemes for social security or taxation declaration purposes (eg France)

9.2.3 UE States Legislation Overview

Most of European Member States have implemented the Directive completely. Nevertheless the national laws may differ on many details even if the harmonisation of the basic principles as set out in the Directive has been accomplished.
The following matrix shows an overview of the national laws in the Member States (including Romania) and scans:

- Their compliance with the UE directive;
- The existence of procedures for secure signature verification;
- The eventual specificity of the public sector;
- The relevant supervision body;
- Other relevant specific provisions.

	Laws governing electronic signature[ii]	Compliance with EU directive	Procedures for secure signature verification	Specific Public sector rules	Relevant supervision body	Specific provisions[iii]
Austria	➢ Act of 1999 (190/1999) ➢ Electronic Signature Order of 2000	Literal transposition	Yes : annex 4 of the directive transposed	No	'Telekom-Control-Kommission'	
Belgium	➢ Law of October 2000 ➢ Law of July 2001 ➢ Order of December 2002	Literal transposition	Only recommendations	Yes	'Administration de la qualité et de la sécurité'	
Denmark	➢ Act of May 2000 ➢ Order of October 2000	Literal transposition	No	No	'National Telecom Agency'	
Finland	➢ Law of July 2002 ➢ Act of Feb 2003	Literal transposition	No	Yes	'FICORA'	
France	➢ Act of March 2000 ➢ Decree of March 2001 ➢ Order of May 2002	Literal transposition	No	Yes (e.g. taxes)	'SCSSI'	➢ For notaries acts such as matrimonial acts, handwriting is still required
Germany	➢ Act of May 2001 ➢ Ordinance of Nov 2001	More or less compliant	Yes : annex 4 of the directive transposed	Yes (e.g. invoice)	'Regulierungsbehörde'	➢ Advanced electronic signature is recognised if and only if it is issued from an accredited CSP ➢ Liability is extended to all services of the certification service provider that may have a harmful impact on third parties ➢ Provisions are far more restrictive than the EU directive
Greece	➢ Presidential decree of June 2001	Literal transposition	Yes : annex 4 of the directive transposed	Yes	'National Telecommunications and Post Commission'	
Ireland	➢ Electronic Commerce Act of 2000 ➢ Decrees for compliance with EU directive on Draft	Compliant except for the accreditation and supervision of CSP	No	Yes	To be designed by the Minister of public enterprise	
Italy	➢ Law of 1997 ➢ Law (technical rules) of 1999 ➢ Decree of 2002	More or less compliant	Yes: more or less annex 4	Yes	'AIPA'	➢ Becoming accredited as a CSP requires a government license; ➢ Legal effect is limited to certificates from accredited CSPs ➢ Technical provisions are numerous
Luxembourg	➢ Law of August 2000 on electronic commerce ➢ Regulation in June 2001	Literal transposition	Yes: more or less annex 4	Public initiatives	The 'National Registry of Accreditation'	
Netherlands	➢ Law of May 2001	Literal transposition	No	Public initiatives	The Ministry of Transport and Communications	
Portugal	➢ Portuguese Digital Signature Law of 1999 ➢ Decree of September 2000	Compliant	Yes : more or less annex 4	No	To be designed	➢ Only a digital signature based on a certificate issued by an accredited certification authority has the same evidential value as a hand-written signature
Spain	➢ Law of Sept1999 ➢ Order of 2000	Literal transposition	Yes : annex 4 of the directive transposed	Public initiatives	'ENAC & Ministry of Science and Technology'	➢ Accredited CSP must comply with additional security measures ➢ Additional legal effects are provided to electronic signatures issued by accredited CSP
Sweden	➢ Act of Nov 2000 ➢ Act of Jan 2001	Literal transposition on the most important points	No	Public initiatives	'National Post and Telecom Agency'	
Romania	➢ Law on the electronic signature of 2001 (no. 455) ➢ Decree of Dec 2002	Completely compliant	Yes : more or less annex 4	Public initiatives (prototypes)	'Romanian authority for reglementation and supervision'	➢ Technologically oriented (PKI) with many technical specifications (private keys, algorithms,…)
The UK	➢ Electronic Communications Act of 2000 ➢ E-sign regulations of March 2002	More or less compliant	No	No	'Secretary of State'	➢ The law does not authorise the use of electronic means if the law currently requires a traditional medium

[ii] It does not include the laws related to electronic commerce
[iii] Thos is not an exhaustive list of the specific provisions

10 Other requirements

10.1 Scalability

The following deployment requirements in terms of scalability 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;
- Bulk processes in operating the PKI.

10.2 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.

10.2.1 Modularity

The PKI shall make full use of modularity.
For small to medium size PKIs, a light and "turn-key" solution should be provided.
For large size PKIs, the modularity should allow integrators to use either software or hardware devices to build large solutions.

10.2.2 Platforms

The PKI must be available for the client-side key generator and the RA interface on the following platforms : Linux, Unix and Windows.

10.2.3 Protocols and standards

The PKI should use open high level protocols and standards : X509v3, RFC 2459, PKCS#12 ...
To ensure a full interoperability and in particular between the core components in order to propose interfaces for other PKI solution, EUPKI will use the CMP protocol to ensure standardized exchanges.

10.2.4 External devices

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

10.2.5 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,
- Ease of renewal process.

11 Examples of PKI

11.1 France Telecom

Description of scenarios and specificities for EUPKI's pki fulfilling France Télécom needs
Context: PKI within an enterprise.

11.1.1 Certificates

Here follows the list of the different kinds of certificates we feel to be useful for our pki scenario and why they are used for. We distinguish :

- Certificates for users. They have to be delivered for the support of different services :
    - Authentication (secure access to applications)
    - Encryption (e-mail)
    - Electronic signature

- Certificates for servers/gateway

They are used during authentication in a client/server mode: access to a web server, authentication of a client connecting to a VPN.

11.1.2 Actors

Before a description of the processes to be supported by the PKI, we list here after the different actors involved in such processes and their responsibilities:

11.1.2.1 User

He/she uses the key pair to operate some secure services. He/she is responsible for the usage of his/her private key (he/she has not to divulgate it by, e.g. providing his/her PIN code)

11.1.2.2 Registry Authority

He/she verifies that data related to a certificate request are correct (i.e., data related to users or servers). It is his/her responsibility to validate the request (by verifying each element constituting the request) before sending it to the Certification Operator.
In the case of a big community, it can be interesting (and even necessary, to be applicable) to delegate RA rights/responsibilities to several people (e.g., if an enterprise is geographically divided into different sites, such a people can be needed on each place). Thus are called Local Registry Authorities.

11.1.2.3 Local Registry Authority

They are habilitated people to act as Registry Authority. Thus, they verify information on certificate requests, whether by a face-to-face with users (or administrators of servers) or by phone calls.

11.1.2.4 Certification Operator

He/she delivers certificates when it is asked to him. Thus, he/she creates the certificates and manages also CRL.
It is his/her responsibility to keep the CA private key (secure place) and to use it only for CA.

We do not include in the list of actors the smart card provider (even if it is often referred to smart cards as a support for certificates) since it seems to us to be out of the scope of EUPKI.

11.1.3 Support

We describe the type of support used in this PKI.

- Certificates for server and gateway are software certificates.
- Each user must have a smart card. There are two types of Smart Card:
    - Smart Card with a key pair:

  A key pair is generated by the Certification operator. This key pair is stored in the database.
  Then, this key pair is written in a smart card. This key pair will be used as an encryption key pair. There is not yet a certificate associated to this key pair.
  When a user wants a certificate dedicated to encryption, a smart card containing a key pair must be used.

    - Smart Card empty: no keys, no certificates has already exist in this smart card.

11.1.4 Processes

Practically, the LRA makes the different requests from a dedicated application (with an adapted interface). Since he/she is an habilitated person, access to this application is authenticated.

11.1.4.1 Certificate request

We distinguish different kinds of requests (processes are slightly different, as described below) according to the kind of certificate to be generated.
NB: requests are synchronous.

User certificate dedicated to signature:

1. The key pair is generated on the smart card (private key is only present on the smart card and never leaves it)
2. User registration (face-to-face registration): LRA verifies data provided by the user to fill in certificate request. He/she is sure a certificate can be delivered to the user. Once LRA has validated information, the request is automatically validated (as seen from a RA point of view) and sent to the Certification Operator. The request contains the public key.
3. LRA (and user) are waiting the certificate to be delivered
4. Once data has been received (certificate), it is written on the smart card

User certificate dedicated to encryption:
The smart card already contains a key pair (not associated, for the time being to any certificate).

1. User registration (face-to-face registration): LRA verifies data provided by the user to fill in certificate request. He/she is sure a certificate can be delivered to the user. Once LRA has validated information, the request is automatically validated (as seen from a RA point of view) and sent to the Certification Operator. The request contains the public key.
2. LRA (and user) are waiting the certificate to be delivered
3. Once data has been received (certificate), it is written on the smart card.

Certificate for server or gateway:

1. A Certificate Server Request (CSR) is generated on the server/gateway by the administrator of the machine
2. CSR is sent by e-mail to the LRA
3. LRA verifies information of the CSR (i.e., the identity of the administrator), e.g., by phone
4. LRA sends the CSR and the e-mail address of the administrator to the Certification Operator
5. Certification Operator sends an e-mail to the administrator containing an URL where he/she can retrieve and install the asked certificate.

11.1.4.2 Recovery request

Only encryption key pairs can be recovered. So, theses requests concern only users.

We distinguish different kinds of recovery requests according to the kind of the support.
If a user destroys his smart card, then his encryption key pair and the certificate associated can be written in the new smart card. But, if a user looses his smart card, then his encryption key pair and the certificate associated must be recovered in the file. This recovery can be useful to decrypt his mails.
Only a LRA makes theses requests.

NB: requests are synchronous.

Recovery Request on the smart card

1. The user meets his LRA who makes the request.
2. The validation is automatic
3. The LRA (and the user) are waiting for the key pair and the certificate associated. This information is encrypted with the LRA's public key.
4. After having decrypted this information (a specific application installed on the post of the LRA), the key pair and the certificate associated are written in the empty smart card

Recovery Request on a file (PKCS#12 format)

1. The user meets his LRA who makes the request.
2. The validation is automatic

3. The LRA (and the user) are waiting for the key pair and the certificate associated. This information is encrypted with the LRA's public key.
4. After having decrypted this information, the key pair and the certificate associated are written in a PKCS#12 format file protected by a password chosen by the user.

11.1.4.3 Revocation

Only a LRA makes this request. User, server and gateway certificates are concerned by the revocation

1. The user or the administrator of the server/gateway meets his LRA who makes the request.
2. The validation is automatic
3. Certification operator signs a new CRL.

11.2 FINSIEL

User Scenario for PKI

11.2.1 Context

PKI within a Pension Fund, to provide certificates to a closed group of users (representatives of enterprises associated to the Fund). Certificates allow stronger user's authentication to access applications (Internet interactive services).

The Fund plays the role of Certification and Registration Authority. Key pairs are generated locally on users workstations. Private keys are stored at client level on diskette (a secure hardware device is not implemented).
According to Italian legislation, certificates issued by the Fund are not considered as "Qualified Certificates".
PKI platform is Baltimore Unicert. Potential users are 22000 (associated enterprises). Certificates issued so far are nearly 1000.

Details about process follow.

11.2.2 Registration

The Fund itself acts as a Registration Authority. Users are identified face to face at the offices of the Fund. Personal identification documents are verified. Users must also demonstrate to be an authorised representative acting on behalf of an associated enterprise.
Identified users are then registered by an operator. Registered users are assigned Userid and Password to access on line services and to request a Certificate.

11.2.3 Certificates Request and Issuing

Certificates are requested and issued on line (Internet). The request may be submitted only by registered users (identified by Userid and Password).
The same on line session allows to:

- *Submit Request*
  User fills in a request form (name, surname, fiscal code). Data must match to those recorded in the Registration phase
- *Generate Keys*
  Key are generated on the client browser. Generation rely on Java libraries (Baltimore) which must be installed in advance. An installation CD is distributed to registered users
- *Issue Certificate*
  Certificate is generated at server level and installed on the client
- *Store private key*
  Private key may be stored on a diskette. Access to the private key is protected by a pass phrase
- *Publish Certificates*
  Generated certificates are published in a LDAP directory accessible to users of PKI domain

11.2.4 Certificate Revocation

Users may revoke a certificate by submitting a paper form. Revocation is performed by an authorised operator at CA level. The CA may autonomously revoke the certificate, informing the user about the operation

11.2.5 Key Recovery

Not implemented

11.3 Cap Gemini

11.3.1 Objectives of Capkey

Capkey is the CGE&Y internal PKI, which objectives are to provide to all CGE&Y employees :

- Electronic signature
- Strong central authentication to all intranet servers without using any login/password system
- Secure mail system with the use of cryptography

Capkey has also the following objectives :

- Cost reduction
  Pricing not related to the number of users/certificates
- Almost no intervention by the Capkey administrator is needed
  Fully automatic processes (administrator of the PKI has minimal work)

11.3.2 Functions of Capkey

11.3.2.1 Use of a Capkey certificate

- Central web authentication to all intranet servers
  Single Sign On
- Electronic signature and/or cryptography
  - Mail
  - Electronic documents : Word, Excel, PowerPoint, PDF…
- Certificate stored on client or on smart card

11.3.2.2 Capkey website

- User interface
  - Client installation of the CGE&Y CA certificate
  - Generation of certificate
  - List of certificates
  - CRL
  - Renewal of certificates
  - Revocation of certificates
- Administrator interface (additional features)
  - Creation of a user certificate
  - Revocation of any certificate
  - Creation of assistant administrators
  - Creation of a server certificate (on user request)

11.3.3 Capkey Processes

11.3.3.1 Registration

- Only initialisation (no update feature)
- Installation of the certificate
  - CGE&Y directory

as trustable identification source
  - Key generation transparent to end-user
- Users performs manual backup
  - His/her own certificate
  - His/her private key
- Automatic publishing of certificates
- No recovery of private key
  (unless previously saved by the end-user)

11.3.3.2 Revocation

- No suspension process
- No reactivation process
- A certificate can be revoked
  - by its owner (the end-user)
  - by the PKI administrator
    (user identification ID)

12 UE Directive on Electronic Signature

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 47(2), 55 and 95 thereof,

Having regard to the proposal from the Commission[iv],

Having regard to the opinion of the Economic and Social Committee[v],

Having regard to the opinion of the Committee of the Regions[vi],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[vii],

Whereas:

(1) On 16 April 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce;

(2) On 8 October 1997 the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on ensuring security and trust in electronic communication - towards a European framework for digital signatures and encryption;

(3) On 1 December 1997 the Council invited the Commission to submit as soon as possible a proposal for a Directive of the European Parliament and of the Council on digital signatures;

(4) Electronic communication and commerce necessitate " electronic signatures" and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;

(5) The interoperability of electronic-signature products should be promoted; in accordance with Article 14 of the Treaty, the internal market comprises an area without internal frontiers in which the free movement of goods is ensured; essential requirements specific to electronic-signature products must be met in order to ensure free movement within the internal market and to build trust in electronic signatures, without prejudice to Council Regulation (EC) No 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods[viii] and Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council concerning the control of exports of dual-use goods[ix];

(6) This Directive does not harmonise the provision of services with respect to the confidentiality of information where they are covered by national provisions concerned with public policy or public security;

(7) The internal market ensures the free movement of persons, as a result of which citizens and residents of the European Union increasingly need to deal with authorities in Member States other than the one in which they reside; the availability of electronic communication could be of great service in this respect;

(8) Rapid technological development and the global character of the Internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically;

[iv] OJ C 325, 23.10.1998, p. 5.
[v] OJ C 40, 15.2.1999, p. 29
[vi] OJ C 93, 6.4.1999, p. 33
[vii] Opinion of the European Parliament of 13 January 1999 (OJ C 104, 14.4.1999, p. 49), Council Common Position of 28 June 1999 (OJ C 243, 27.8.1999, p. 33) and Decision of the European Parliament of 27 October 1999 (not yet published in the Official Journal). Council Decision of 30 November 1999.
[viii] OJ L 367, 31.12.1994, p. 1. Regulation as amended by Regulation (EC) No 837/95 (OJ L 90, 21.4.1995, p. 1)
[ix] OJ L 367, 31.12.1994, p. 8. Decision as last amended by Decision 99/193/CFSP (OJ L 73, 19.3.1999, p. 1).

(9) Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures;

(10) The internal market enables certification-service-providers to develop their cross-border activities with a view to increasing their competitiveness, and thus to offer consumers and businesses new opportunities to exchange information and trade electronically in a secure way, regardless of frontiers; in order to stimulate the Community-wide provision of certification services over open networks, certification-service-providers should be free to provide their services without prior authorisation; prior authorisation means not only any permission whereby the certification-service-provider concerned has to obtain a decision by national authorities before being allowed to provide its certification services, but also any other measures having the same effect;

(11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service-providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;

(12) Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services;

(13) Member States may decide how they ensure the supervision of compliance with the provisions laid down in this Directive; this Directive does not preclude the establishment of private-sector-based supervision systems; this Directive does not oblige certification-service-providers to apply to be supervised under any applicable accreditation scheme;

(14) It is important to strike a balance between consumer and business needs;

(15) Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market needs conformity assessment must be timely and efficient;

(16) This Directive contributes to the use and legal recognition of electronic signatures within the Community; a regulatory framework is not needed for electronic signatures exclusively used within systems, which are based on voluntary agreements under private law between a specified number of participants; the freedom of parties to agree among themselves the terms and conditions under which they accept electronically signed data should be respected to the extent allowed by national law; the legal effectiveness of electronic signatures used in such systems and their admissibility as evidence in legal proceedings should be recognised;

(17) This Directive does not seek to harmonise national rules concerning contract law, particularly the formation and performance of contracts, or other formalities of a non-contractual nature concerning signatures; for this reason the provisions concerning the legal effect of electronic signatures should be without prejudice to requirements regarding form laid down in national law with regard to the conclusion of contracts or the rules determining where a contract is concluded;

(18) The storage and copying of signature-creation data could cause a threat to the legal validity of electronic signatures;

(19) Electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in the public procurement, taxation, social security, health and justice systems;

(20) Harmonised criteria relating to the legal effects of electronic signatures will preserve a coherent legal framework across the Community; national law lays down different requirements for the legal validity of hand-written signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures only if the requirements for hand-written signatures are fulfilled;

(21) In order to contribute to the general acceptance of electronic authentication methods it has to be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States; the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved; national law governs the legal spheres in which electronic documents and electronic signatures may be used; this Directive is without prejudice to the power of a national court to make a ruling regarding conformity with the requirements of this Directive and does not affect national rules regarding the unfettered judicial consideration of evidence;

(22) Certification-service-providers providing certification-services to the public are subject to national rules regarding liability;

(23) The development of international electronic commerce requires cross-border arrangements involving third countries; in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial;

(24) In order to increase user confidence in electronic communication and electronic commerce, certification-service-providers must observe data protection legislation and individual privacy;

(25) Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Community or national law;

(26) The measures necessary for the implementation of this Directive are to be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[x];

(27) Two years after its implementation the Commission will carry out a review of this Directive so as, inter alia, to ensure that the advance of technology or changes in the legal environment have not created barriers to achieving the aims stated in this Directive; it should examine the implications of associated technical areas and submit a report to the European Parliament and the Council on this subject;

(28) In accordance with the principles of subsidiarity and proportionality as set out in Article 5 of the Treaty, the objective of creating a harmonised legal framework for the provision of electronic signatures and related services cannot be sufficiently achieved by the Member States and can therefore be better achieved by the Community; this Directive does not go beyond what is necessary to achieve that objective,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Scope

The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market. It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

Article 2

Definitions

[x] OJ L 184, 17.7.1999, p. 23

For the purpose of this Directive:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. "advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

3. "signatory" means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;

4. "signature-creation data" means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

5. "signature-creation device" means configured software or hardware used to implement the signature-creation data;

6. "secure-signature-creation device" means a signature-creation device which meets the requirements laid down in Annex III;

7. "signature-verification-data" means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

8. "signature-verification device" means configured software or hardware used to implement the signature-verification-data;

9. "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;

10. "qualified certificate" means a certificate which meets the requirements laid down in Annex I and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II;

11. "certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;

12. "electronic-signature product" means hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;

13. "voluntary accreditation" means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.

Article 3

Market access

1. Member States shall not make the provision of certification services subject to prior authorisation.

2. Without prejudice to the provisions of paragraph 1, Member States may introduce or maintain voluntary accreditation schemes aiming at enhanced levels of certification-service provision. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Member States may not limit the number of accredited certification-service-providers for reasons which fall within the scope of this Directive.

3. Each Member State shall ensure the establishment of an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public.

4. The conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States. The Commission shall, pursuant to the procedure laid down in Article 9, establish criteria for Member States to determine whether a body should be designated. A determination of conformity with the requirements laid down in Annex III made by the bodies referred to in the first subparagraph shall be recognised by all Member States.

5. The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

6. Member States and the Commission shall work together to promote the development and use of signature-verification devices in the light of the recommendations for secure signature-verification laid down in Annex IV and in the interests of the consumer.

7. Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens.

Article 4

Internal market principles

1. Each Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.

2. Member States shall ensure that electronic-signature products which comply with this Directive are permitted to circulate freely in the internal market.

Article 5

Legal effects of electronic signatures

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

- in electronic form, or
- not based upon a qualified certificate, or
- not based upon a qualified certificate issued by an accredited certification-service-provider, or
- not created by a secure signature-creation device.

Article 6

Liability

1. As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;

(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;

(c) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both; unless the certification-service-provider proves that he has not acted negligently.

2. As a minimum Member States shall ensure that a certification-service-provider who has issued a certificate as a qualified certificate to the public is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the certification-service-provider proves that he has not acted negligently.

3. Member States shall ensure that a certification-service-provider may indicate in a qualified certificate limitations on the use of that certificate. provided that the limitations are recognisable to third parties. The certification-service-provider shall not be liable for damage arising from use of a qualified certificate which exceeds the limitations placed on it.

4. Member States shall ensure that a certification-service-provider may indicate in the qualified certificate a limit on the value of transactions for which the certificate can be used, provided that the limit is recognisable to third parties. The certification-service-provider shall not be liable for damage resulting from this maximum limit being exceeded.

5. The provisions of paragraphs 1 to 4 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts[xi].

Article 7

International aspects

1. Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:

(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or

(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or

(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

2. In order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries, the Commission shall make proposals, where appropriate, to achieve the effective implementation of standards and international agreements applicable to certification services. In particular, and where necessary, it shall submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council shall decide by qualified majority.

3. Whenever the Commission is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Council for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries. The Council shall decide by qualified majority. Measures taken pursuant to this paragraph shall be without prejudice to the obligations of the Community and of the Member States under relevant international agreements.

Article 8

Data protection

1. Member States shall ensure that certification-service-providers and national bodies responsible for accreditation or supervision comply with the requirements laid down in Directive 95/46/EC of the

[xi] OJ L 95, 21.4.1993, p. 29.

European Parliament and of the Council of 24 October 1995 on tile protection of individuals with regard to the processing of personal data and on the free movement of such data[xii].

2. Member States shall ensure that a certification-service-provider which issues certificates to the public may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the certificate. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

3. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name.

Article 9

Committee

1. The Commission shall be assisted by an "Electronic-Signature Committee", hereinafter referred to as "the committee".

2. Where reference is made to this paragraph, Articles 4 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof. The period laid down in Article 4(3) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its own rules of procedure.

Article 10

Tasks of the committee

The committee shall clarify the requirements laid down in the Annexes of this Directive, the criteria referred to in Article 3(4) and the generally recognised standards for electronic signature products established and published pursuant to Article 3(5), in accordance with the procedure laid down in Article 9(2).

Article 11

Notification

1. Member States shall notify to the Commission and the other Member States the following:
(a) information on national voluntary accreditation schemes, including any additional requirements pursuant to Article 3(7);

(b) the names and addresses of the national bodies responsible for accreditation and supervision as well as of the bodies referred to in Article 3(4);

(c) the names and addresses of all accredited national certification service providers.

2. Any information supplied under paragraph 1 and changes in respect of that information shall be notified by the Member States as soon as possible.

Article 12

Review

1. The Commission shall review the operation of this Directive and report thereon to the European Parliament and to the Council by 19 July 2003 at the latest.

2. The review shall inter alia assess whether the scope of this Directive should be modified, taking account of technological, market and legal developments. The report shall in particular include an assessment, on the basis of experience gained, of aspects of harmonisation. The report shall be accompanied, where appropriate, by legislative proposals.

Article 13

Implementation

[xii] OJ L 281, 23.11.1995, p. 31.

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001. They shall forthwith inform the Commission thereof. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall communicate to the Commission the text of the main provisions of domestic law which they adopt in the field governed by this Directive.

Article 14

Entry into force

This Directive shall enter into force on the day of its publication in the Official Journal of the European Communities

Article 15

Addressees

This Directive is addressed to the Member States.

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:
(a) an indication that the certificate is issued as a qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;
(c) the name of the signatory or a pseudonym, which shall be identified as such;
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
(e) signature-verification data which correspond to signature-creation data under the control of the signatory;
(f) an indication of the beginning and end of the period of validity of the certificate;
(g) the identity code of the certificate;
(h) the advanced electronic signature of the certification-service-provider issuing it;
(i) limitations on the scope of use of the certificate, if applicable; and
(j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:
(a) demonstrate the reliability necessary for providing certification services;
(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;
(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;
(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;
(l) use trustworthy systems to store certificates in a verifiable form so that:
- only authorised persons can make entries and changes,
- information can be checked for authenticity,
- certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and
- any technical changes compromising these security requirements are apparent to the operator.

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
(a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
(b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
(c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

ANNEX IV

Recommendations for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:
(a) the data used for verifying the signature correspond to the data displayed to the verifier;
(b) the signature is reliably verified and the result of that verification is correctly displayed;
(c) the verifier can, as necessary, reliably establish the contents of the signed data;
(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;
(e) the result of verification and the signatory's identity are correctly displayed;
(f) the use of a pseudonym is clearly indicated; and
(g) any security-relevant changes can be detected.

13 Answers to the EUPKI questionnaire

13.1 Questionnaire produced by G&D

Use case:

- Which of the existing PKIs named in D3.5 Draft 1.0 are you describing with this questionnaire?
- Please give a short description of your applications (in about 5 sentences). Why do you need a PKI?
- Which PKI enabled software will be used on client side? Which PKI functionality is enabled there? How is it enabled (interfaces used towards the PKI)?
- Please describe the users of your PKI.
  How many users do you expect? ("user" as defined in chapter 5 of D3.5 Draft 1.0)
  How many key pairs will a user have?

Architecture and functions:

- Which of the functions listed in chapter 6 of D3.5 Draft do you need to build up your PKI?
  Please add your requirements to the table below (taken from section 6.4 of D3.5 Draft 1.0) .
  Is this set of functions complete or do you need extra functions?

Functions → ↓ Examples	**F1**	**F1.1**	**F1.2**	**F2**	**F3**	**F4**	**F5**	**F6**	**F7**	**F8**	**F9**	**F9.1**	**F10**	**F11**
your PKI														

- Do you perform authentication, signature, encryption?

- Will a smart card or another kind of hardware be used on client-side for secure storage of private keys?
  If any: what kind of token? Is it optional or mandatory for the user?
  Which are the procedures for token production and distribution?

- Will key generation be done by the user or centralised or at registration points?
  If a device like a smart card is used, will key generation be done by this device?
  If centralised, how will the keys be assigned and distributed?

- Registration of users: will the data entry be done in a manual or automatic way (e.g. from an existing database)? What data will be stored?

- What are the procedures for certificate generation, update and cancellation?
  Which information will be stored in a certificate?

- CA-Interaction:
  Is there just one CA or a CA hierarchy? (Cross-certifications, Bridge-CA?)
  How will the public keys of the (root) CA be distributed?
  How will a CA key update and in consequence the update of certificates take place ?

- Directory services:
  What data will be stored in the black list? Who is allowed to retrieve which information from it?
  How is the black list accessed? How is it updated?
  Do you plan to provide a white list?
  What data will be stored in the white list? Who is allowed to retrieve which information from it?
  How is the white list accessed? How is it updated?

- Will there be an encryption key archive?

Algorithms and formats:

- What cryptographic algorithms are used for asymmetric encryption/signing, symmetric encryption, hashing? Key lengths?

- Which formats do you prefer for signatures, certificates, encrypted data? Which authentication protocol?
- Do you have necessities for proprietary formats instead of standards like X.509, S/MIME?

Optional:

- If available, please add flowcharts of your registration / key generation / certification processes.
- Is there anything else you consider important to be mentioned?

13.2 Answers from PKI end-users

	FINSIEL	FT	CGEY
Use Case			
Described PKI	Italian Pension Fund	Internal PKI	Cap Key Internal PKI
Applications	- Closed group of users - User authentication to Web services - Face to face registration - On-line issued certificates - Locally generatede key-pairs - Baltimore Unicert platform - 22 000 potential users - 1 000 so far	- Secure access (authentication) - Email encryption - Signature (integrity) - Authentication on Web server or VPN - About 50 users and 10 servers	- Electronic signature - Strong central authentication to all intranet servers without using any login/password system - Secure mail system with the use of cryptography
PKI enabled software on client side	No client side software but for Key Generating libraries	- Dedicated interface to access PKI - For LRA and administrators who perform requests for end-users	Clients use their browser capacities.
PKI enabled functionality	On-line requests for certificate issuing and revoking	- Key generator connected to LRA computer LRA can put key pairs on empty smartcards or use pre-personalized ones (certificate is then put onto the smartcard - for encryption purpose) - Smartcard reader needed	Key generation & Certificate integration
Interfaces used towards PKI	Web browser		Collaborators can also install a smart card or a USB Token to generate their keys and to store their certificate.
PKI users	1 000 users, 22 000 potential ones	Objectives : from 4 000 to 15 000 users	Potentially, the 55000 collaborators of CGEY.
Number of key pairs	One per user	- Two key pairs for users (signature, encryption) - One key pair for servers/gateway (soft certificate)	One per user

Architecture			
Functions			
F1		Y	Y
F1.1	Y	Y	Y
F1.2	Y	Y	Y
F2	N	Y	N
F3	Y	Y	Y
F4	N	N	N
F5	Y	Y	Y
F6	Y	Y	Y
F7	N	N	N
F8	N	N	N
F9	N	N	N
F9.1	N	N	N
F10	Y	Y	Y
F11	N	Y	Y
Purpose			
Authentication	Y	Y	Y
Encryption	N	Y	Y
Signature	N	Y	Y
Hardware for key storage (client side)	No (diskette)	Smartcard mandatory (token USB forecasted)	Optional Users manage their smart card and choose their solution.
Procedures for token production and distribution		- Smartcards are provided by smartcard provider - Pre personalised or empty - Distribution (with key pairs and certificate) done by the LRA (face to face)	No procedure for the moment
Centralized Key generation	No (user level)	- Pre personalised cards : centralised way - Empty cards : done on-board by the smartcard	Key generation is done by the user. If the user wishes, the key generation can be done by a device like a smart card.

User registration	Manual data entry	Data extracted from a directory	Registration of users is done in a automatic way from a CGE&Y directory.
Stored data	Name	Name	
	Surname	First name	
	Fiscal ID Code	Unique identifier	
	Entreprise represented		
	Role in the entreprise		
	Email	Email	
		Certificate	
Procedures			
Certificate generation	Requested and issued on line. Only made by previously registered users (Userid/pwd) - Fills in on line request form - data must match with those previously registered - Keys generated on client browser - Java librairies (Baltimore) must be installed (installation CD distributed) - Certificate generated at server level and installed on the client - Private key may be stored on diskette, and protected by passphrase - Certificates are published in a LDAP	- User name manually specified - software search for user name in the directory and returns matching ones : LRA chooses the right one, then all relevant data are automatically extracted from the directory - Request is sent to CA	The certificate generation and cancellation can be done by the user or the PKI administrator.
Certificate revocation	- Requested by user through paper form - Performed by CA operator - CA may autonomously revoke certificate	- User unique id is specified manually - If several certificates are valid, they are proposed - LRA chooses the one to revoke	
Certificate renewal			

Information stored in certificate	Standard x509 - no detail available	Name	
		First name	
		Unique identifier	
		Email	
CA Interaction			
CA hierarchy	One CA	One CA Root	One CA
		One sub-CA ("operational CA" or "daughter")	
Distribution of root CA public keys	#NA	- Public key available on a public URL - Private key stored in a strongbox	In the first step of certificate generation.
CA Key update	No key update implemented	- New key ceremony => new CA certificate - Only when users certificates are no longer valid (CA certificate validity period much longer than user's one) - If CA key is compromised, all certificates are revoked	
Directory services			
Data black list	- Revoked certificates stored on CRL - Public read access to CRL	- CRLs with revoked certificates serial number - Available on public URL	No black list
Data white list	- Certificates published onto directory - Read access to Certificates Directory public to LDAP clients		- LDAP or HTTP - Data : Entreprise Directory - Access : all the collaborators of CGEY - Update : all the days
Encryption key archive	No key archive implemented	Yes	No
Algorithms and formats			
Cryptographic algorithms			
Asymetric encryption	RSA (512-2048)	RSA	RSA

	DSA (512-2048)		
	ECDSA		
	Blum Blum Shub		
Symetric encryption		DES	
	3-DES	3-DES	
		AES	
		RC2	
		RC4	
Hashing	MD5	MD5	MD5
	SHA-1	SHA-1	SHA-1
Key length	512 to 2048	1024 bits for user and 2048 for CA keys	1024 for users and servers 2048 for CA
Preferred format	X509 v3	X509 v3	X509 v3
	RFC 2459		
	CRL v2		
	PKCS #1	PKCS #1	
	PKCS #7	PKCS #7	PKCS #7
	PKCS #10	PKCS #10	
	PKCS #11	PKCS #11	PKCS #11
	PKCS #12	PKCS #12	PKCS #12
Authentication protocols		SSL / TSL	
Necessity for proprietary format	No	No	No

13.3 Answers from PKI operators

	CERTINOMIS	INTESA
Use Case		
Described PKI	Certinomis PKI	Intesa PKI
Applications	- Deliver certificates in software format or on tokens (smartcards, USB tokens, HSM…), and crl to end users, customers of our company. The generated certificates are mainly used to Authenticate or Sign, but also to Encipher and for that usage the PKI has to be able to recover keys. - Able to delegate RA-functions to a client (Local RA), in order to have internal like PKI. - Can be used to build an operator dedicated PKI (i.e. : GIP-CPS).	- Complete system for issuance and management of X509 v3 certificates - Supports X.500 directory systems - Issuance of Certificate Revocation Lists (CRLs) - Supports separate, multiple Registration Authority (RA) systems connecting to central Certification Authority (CA) system - Support for multiple certificate issuance policies - Supports Tamper-Resistant Hardware Security Modules for CA key generation storage and signing. - Uses PKIX for all inter-process communications.
PKI enabled software on client side	- Clients can use their browser capacities. Key generation via script in browser. Certificate integration by the same way - Certificate and key pair are used via standard tools like IE, Outlook, or Netscape, with all the crypto librairies (CSP, PKCS#11) they accept. - Can provide a Sagem Crypto Tool (Confidence), for security enhancement using one certificate for signing and an other for encryption. - An ActiveX is used to communicate between browser and Sagem Confidence and to implement the PKCS#10, PKCS#7 exchange with the PKI. - Encryption key is sequestrated; trans-encryption or key recovery is possible. - Certificate and key pair is only accessible by the Sagem tool.	
PKI enabled functionality		- Mail Secure, - Form on line Signature - Signing SW for all kinds of documents (plug in version, standalone version or applet)

Interfaces used towards PKI			All solutions are integrated with a smart card (or token USB) component (but if requested it is possible to generate also software keys), depending on policies there are two key pair (one for sign, and another for encryption , or just one).
PKI users	The users are very different from one type of certificate to the other. - Free certificate (any kind of user) : about 2500 by year - Personal certificate (for the moment early adopters) : about 100 by year (market is not yet ready) - Professional and Qualified certificate (company managers used or not to computers) : about 10000 by year - Professional but Internal-use certificate (company managers and workers used or not to computers): about 100000 by year.		Citizens, corporate suppliers, corporate employees.
Number of key pairs	1 to 3 (signature, encryption, authentication). But a user can have many of these (if he pays for it…)		Usually two, signing and encryption.
Architecture			
Functions	Confidence	Browser	
F1	Y	Y	Y
F1.1	Y	Y	Y
F1.2	Y	Y	Y
F2	Y	N	Y
F3	Y	Y	Y
F4	N	N	Y
F5	Y	Y	N
F6	Y	Y	Y
F7	N	N	Y
F8	N	N	Y
F9	Y	N	N
F9.1	Y	N	N

F10	Y Y	Y
F11	Y Y	Y
Purpose		
Authentication	Y	Y
Encryption	Y	Y
Signature	Y	Y
Hardware for key storage (client side)	Optional User can use a Confidence Kit, or and Product compatible with Microsoft CSP or Netscape PKCS11 to store keys. So keys can be stored into a Smartcard or a USB Token.	Optional Smart card and/or token USB
Procedures for token production and distribution	There are different ways: 1. Software token The user receives a delivery code (via email, postal mail, or face-to-face distribution) With this code he can access to the web page dedicated for the generation of its certificate. 2. User personalization We have blank card where we can print the logo we need and names. The card is sent by postal mail, and a delivery code is sent via email, postal mail, or face-to-face distribution. With the smartcard and the code he can access to the web page dedicated for the generation of its certificate. 3. Token personalization The keys and certificate are generated in the PKI after registration. We have blank card where we can print the logo we need and names, and then insert automatically the keys and certificates. The smartcard is distributed via postal mail or face-to-face distribution. The pincode is managed separately and delivered	A complete card management system integrated in the PKI services.

	via email, postal mail, or face-to-face distribution.	
Centralized Key generation	- Key generation is only done by the user, but we are working on centralized production (PKCS#12 sent to a card manufacturer) - For the smartcard case: By the user the key is generated by the card. In centralized, the key is generated by the CA (PKCS#12).	Both, normally centralised for Corporate, at the registration points for Public Administration Key generation can be done by a device like a smart card. Using PKCS#12 packet if sw keys, or send a kit containing smart card (with RSA key and certificate) , reader e digital signature sw.
User registration	- Data entry is done manually by CertiNomis after checking. - Data entry can be done automatically with a database, but need specific development (like GIP-CPS) to adapt to the database information and format.	Depending on policies, the data entry can be done in a manual or automatic way. Data will be stored in the PKI database.
Stored data		Depending on the policy
Procedures		
Certificate generation	For the certificate generation the general process is: First the requester has to give some information to the RA. For qualified certificate it can be quite complex, but for internal-use certificate it can be only a name. Then the RA enters the request in the system, and then generates a delivery code that is printed. This code is sent via postal mail or face-to-face distribution to the requester. In the same time, an email is sent to the requester with a connection URL. Connected on this URL using the delivery code, the requester can proceed to the key generation using the browser or the smartcard key generator. Then the session is closed.	For Public Administration PKI implementations, a direct registration system is the only secure means to correctly authenticate users and distribute/generate keys and certificates accepted by our National Agency . An organisation may implement a policy whereby users must visit a security officer personally to receive a disk or smartcard based secret-key and certificate. This registration may involve the candidate showing a employee ID card, driver's license, passport or other means of identification. In an Internet environment, corporate organisations may require that the same info can be sent to Registration Authority via form on line.

	The requester receives a second mail with a new URL. Connected on this URL using the delivery code, the requester can proceed to the certificate download.	
Certificate revocation	For the certificate revocation, we use some information exchanged during the registration process. The requester, and if applicable the company person in charge of the request, give a list of personal questions/answers during the registration process. If they are asking for revocation by phone, they are asked the questions, and are authenticated with the answers. For electronic revocation, the delivery code can be used.	In both cases a special password is provided for the certificate revocation request, the certificate can be revoked calling our green number or via internet.
Certificate renewal	We are not supporting certificate update, we only provide renewal and the process is the same as the initial registration except that using already known information it can be done in a simpler way.	
Information stored in certificate	Information stored in certificate depends strongly on the certificate class for the DN. The DN can only contain an email address, or can contain precise identification of the user and his company. Our certificates contains always the following fields: Version, SerialNumber, Algorithm, Issuer, NotBefore/UTCTime, NotAfter/UTCTime, Subject, Algorithm, SubjectPublicKey, AuthorityKeyIdentifier (NC), SubjectKeyIdentifier (NC), SubjectAltName (NC), KeyUsage (NC),	Common Name

	NetscapeCertType (NC), BasicConstraints (C), CRLDistributionPoints (NC), CertificatePolicies (NC), Algorithm, SignatureValue For internal-use we can add any extension.	
		Organisation Unit
		Sub-Organisation
		Email
CA Interaction		
CA hierarchy	A root CA with 5 childs (Class 1, 2, 3, Corporis, Test, Horodatage)	Both one CA and CA hierarchy
		In our premises there are INTESA PKI and hosted customer PKI (some hierarchy)
Distribution of root CA public keys	On CertiNomis web site, and as soon as possible in the Microsoft root store.	The public keys of the (root) CA are distributed depending of the project, in any case the root keys are available in the CA Web site.
CA Key update	All the certificates have a validity period included in the validity period of there CA. So CA key update is always done with an overlap between the old and new validity periods. For the distribution of new CA certificates we inform our customers that new ones are needed.	- New key ceremony => new CA certificate - Only when users certificates are no longer valid (CA certificate validity period much longer than user's one) - If CA key is compromised, all certificates are revoked.
Directory services		
Data black list	- HTTP or LDAP - Certificate Serial numbers, and only that. No revocation reason. - Everybody is allowed to retrieve information from it – Updated at least every 4 hours.	- HTTP or LDAP - Certificate Serial numbers - The directory is public - Configurable, customer requirement depending
Data white list	- Have an LDAP directory but only used for CRL. The certificates publication is only optional, and the fact that a certificate is in the LDAP directory has no contractual meaning on the certificate validity. - Data stored in the white list : names, email, certificate - Everybody is allowed to retrieve information from it. That is the reason why we do not publish for moment.	No white list

	- LDAP - Update : insert at creation, remove at revocation, no update for the moment this is another reason why we do not use it.	
Encryption key archive	Only for Confidence Clients.	Yes Provide encryption keys if requested Is available also an archive system for the key recovery.
Algorithms and formats		
Cryptographic algorithms		
Asymetric encryption	RSA	RSA
	DSA	DSA
	DH	
		ECDSA
Symetric encryption	DES	
	3-DES	3-DES
	RC2	
	RC4	
Hashing	MD5	MD5
	SHA-1	SHA-1
	MD2	
	HMAC	
	HMACSHA	
	HMACMD5	
Key length	512 to 4096 (512 and 1024 is the most common)	The secret keys of the CA and RA system and their operators are 2048 bits long, the secret keys of the end user are usually 1024 bits long
Preferred format		X.509 v1, v3 certificates as specified in ITU RFC 1422
		PKIX messages
		PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
		PKCS#5 Password Based Encryption Standard
		PKCS#7 Cryptographic Message Syntax Standard
		PKCS#8 Private Key Information Syntax Standard
		PKCS#9 Selected Attribute Types
		PKCS#10 RSA Certification Request

		PKCS#11 Communication with an external cryptographic modules
		PKCS#12 Vault to store private keys and certificates
Signature formats	CMS, PDF, XML	PDF, XML
Encryption formats	CMS	PDF, XML
Authentication protocols	SSL / GSS	SSL
Necessity for proprietary format	Manage Sagem proprietary formats (PKCS10, 7, 12 like) for enrollment. But the outputs are standards: X509 SMIME and so on.	No