



IST-2001-34340

D3.3 Report of the second meeting

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 :	31 May 2002
Issue :	1.0
File Name :	EUPKI-WP3-D3.3-0.1.doc
Work Package :	WP3 Requirements
Deliverable Number :	D 3.3
Deliverable Type :	Public
Deliverable Nature :	Meeting report
Total Number of Pages :	24
Contact Details for EUPKI :	Project Coordinator Yann Fraval GIP-MDS mail : yann.fraval@gip-mds.fr web site : www.eupki.org

0 Table Of Contents

0	TABLE OF CONTENTS	2
1	DOCUMENT CONTROL	4
1.1	ABSTRACT	4
1.2	KEYWORDS	4
2	MANAGEMENT OVERVIEW	5
2.1	EXECUTIVE SUMMARY	5
2.2	SCOPE STATEMENT	5
3	INTRODUCTION AND GLOSSARY.....	6
3.1	GLOSSARY	6
4	OBJECTIVES OF THE SECOND BRAINSTORMING MEETING	7
5	PARTICIPANTS OF THE MEETING.....	8
6	INTRODUCTION	9
6.1	OVERVIEW OF THE AGENDA OF THE MEETING	9
7	CGE&Y INTRODUCTION TO THE SECOND BRAINSTORMING MEETING.....	10
8	LEGAL ISSUES	11
8.1	LICENSE	11
8.2	ELECTRONIC SIGNATURE	11
8.3	PERSONAL DATA PROTECTION	11
9	PKI SECURITY REQUIREMENTS.....	12
10	PKI FUNCTIONS REQUIREMENTS.....	13
10.1	FLOWS OF EVENTS	13
10.2	TIME-STAMPING.....	14
10.3	VALIDATION OF CERTIFICATES IS OUT OF SCOPE	14
10.4	KEY GENERATION	15
10.5	STORAGE OF EVIDENCES	15
10.6	RECOVERY.....	15
11	EXAMPLES OF PKI	16
11.1	NET-ENTREPRISES	16
11.2	VITAL SMART CARD	16
11.3	COMPANY EMPLOYEES	16
11.4	BANKING	17
11.5	INTESA	17
12	ADDITIONAL INFORMATION.....	18
12.1	ROLES.....	18
12.2	USERS COMMUNITIES.....	18
13	CONTENT OF THE DELIVERABLE D3.6.....	19
14	SOME REMAINING QUESTIONS.....	20
15	BENEFITS	21
16	CONCERNS.....	22
17	LIST OF ACTIONS	23

18 NEXT MEETING..... 24

1 Document Control

<i>Issue</i>	<i>Date of Issue</i>	<i>Comments</i>
1.0	31 May 2002	Creation

1.1 Abstract

The purpose of the deliverable D3.3 'Report of the second meeting' is to communicate the results achieved during the second brainstorming meeting (22/05/2002) to all members of the consortium.

1.2 Keywords

EUPKI	EUPKI, the libre software Public Key Infrastructure (project name)
WP3	Work Package 3
WP4	Work Package 4
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'
PKI	Public Key Infrastructure
EC	European Commission
EU	European Union
GIP-MDS	Groupement d'Intérêt Public Modernisation des Déclarations Sociales
CGE&Y	Cap Gemini Ernst & Young

2 Management Overview

2.1 Executive Summary

This document contains the results achieved during the second brainstorming meeting (22/05/2002). These outputs will also be included into the draft D3.5, which will be submitted to all members of the consortium for approval. The final version of the draft will be referred to as the deliverable D3.6 and will contain all requirements of the EUPKI project which will be the inputs of the Work Package 4.

2.2 Scope Statement

The scope of this document is to capture the results achieved during the second brainstorming meeting (22/05/2002).

This documents refers to the following external documents :

Reference	Document
D3.1	Brainstorming requirements analysis
D3.2	Report of the first meeting

3 Introduction and Glossary

3.1 Glossary

CA	Certification Authority
RA	Registration Authority
CC	Common Criteria
PP	Protection Profile
EAL	Evaluation Assurance Level
GPL	GNU Public License
VPN	Virtual Private Network
OCSF	On-line Certificate Status Protocol
API	Application Programming Interface
URSSAF	Union de Recouvrement des cotisations de Sécurité Sociale et d'Allocations Familiales
URL	Uniform Resource Locator
ASAP	As Soon As Possible

4 Objectives of the second brainstorming meeting

The objectives of the second brainstorming meeting are the following ones :

- Validation of the deliverable D3.2 'First brainstorming meeting report',
- Determination of the legal issues
- Determination of the PKI security requirements
- Determination of the PKI functions requirements
- Determination of the content of the final deliverable D3.6 'Definition of the perimeter of the project and requirements'.

5 Participants of the meeting

France Telecom	Sylvie Camus, Béatrice Renard
EDF	Ludovic Piètre-Cambacédès
CGEY	Edouard Jeanson, Minaradjy Pascal, Pierre-Olivier Baudot
GIP-MDS	Jacques Sauret
INTESA	Franco Tafini
FINSIEL	Paolo Arenaccio
INPS	Annarita Sala
CERTINOMIS	Jean-Severin Lair
AXETEL	Eduard Tric
GIESECKE	Olaf Schlueter
ON-X	Peter Sylvester
AQL	Christophe Anier
EADS	Eric Choffat

6 Introduction

6.1 Overview of the agenda of the meeting

The agenda of the second brainstorming meeting held on 22/05/2002 in Paris (CGE&Y, La Défense) was the following one :

09.30	Introduction (PowerPoint presentation – file : Secondmeeting2.ppt)
10.15	Legal issues
10.30	PKI security requirements
<i>10.40</i>	<i>PKI functions requirements</i>
<i>12.00</i>	<i>Break</i>
12.15	PKI functions requirements (continued)
<i>13.00</i>	<i>Lunch</i>
14.15	PKI functions requirements (continued)
<i>16.10</i>	<i>Break</i>
16.20	PKI functions requirements (continued)
17.10	List of actions
17.20	Benefits & Concerns
<i>17.30</i>	<i>End of meeting</i>

7 CGE&Y introduction to the second brainstorming meeting

A PowerPoint presentation (see file Secondmeeting2.ppt) deals with the following items :

- Validation of the deliverable D3.2 'First brainstorming meeting report'
 - Giesecke remarks
 - EDF remarks
- Decision of the audience : the participants approve version 1.0 of the deliverable D3.2 'First brainstorming meeting report', which needs to be amended to include the correct meaning of RA (a version 1.1 of the deliverable D3.2 will then be published).
- List of actions to be performed after the first brainstorming meeting
 - AQL security training
 - Structure for this meeting
 - Legal issues
 - PKI processes
- Feedback on the support material proposed by CGE&Y
 - EDF feedback
- Legal issues
 - Electronic signature (How to deliver 'qualified certificates')
 - Personal data protection
- PKI security requirements
 - Common Criteria (CC) and Protection Profiles (PP)
- PKI functions requirements
- Content of the final deliverable D3.6 'Definition of the perimeter of the project and requirements'
 - Giesecke feedback

8 Legal issues

8.1 License

Existing decision of GIP-MDS/EC for the EUPKI project : Use of Mozilla and lesser GPL instead of GPL (GNU Public License) so that the code which will be produced in the EUPKI project or in any project using the code produced by the EUPKI project will not become some GPL code.

8.2 Electronic signature

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

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

Decision of audience : Our PKI must also be able to deliver qualified certificates, which therefore enables the delivery of non-qualified certificates.

8.3 Personal data protection

Personal data protection :

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

9 **PKI security requirements**

CGE&Y suggests to use the French PPs (written in French) in order to determine the security requirements.

The following PPs are identified :

- PKI PP,
- CA PP,
- RA PP,
- Key Management PP.

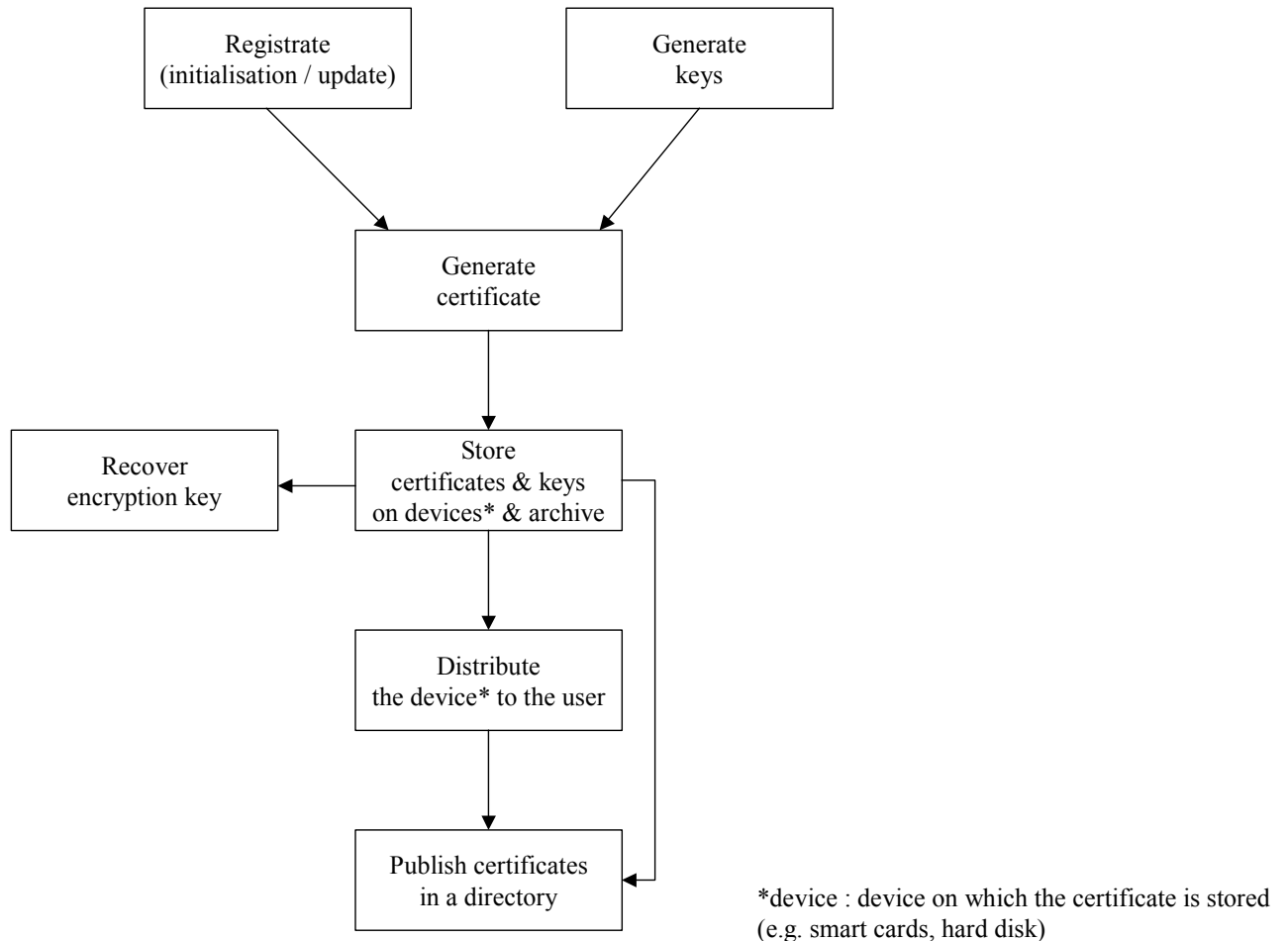
Decision of the audience : First work on the determination of the PKI functions then work on the security requirements.

10 PKI functions requirements

10.1 Flows of events

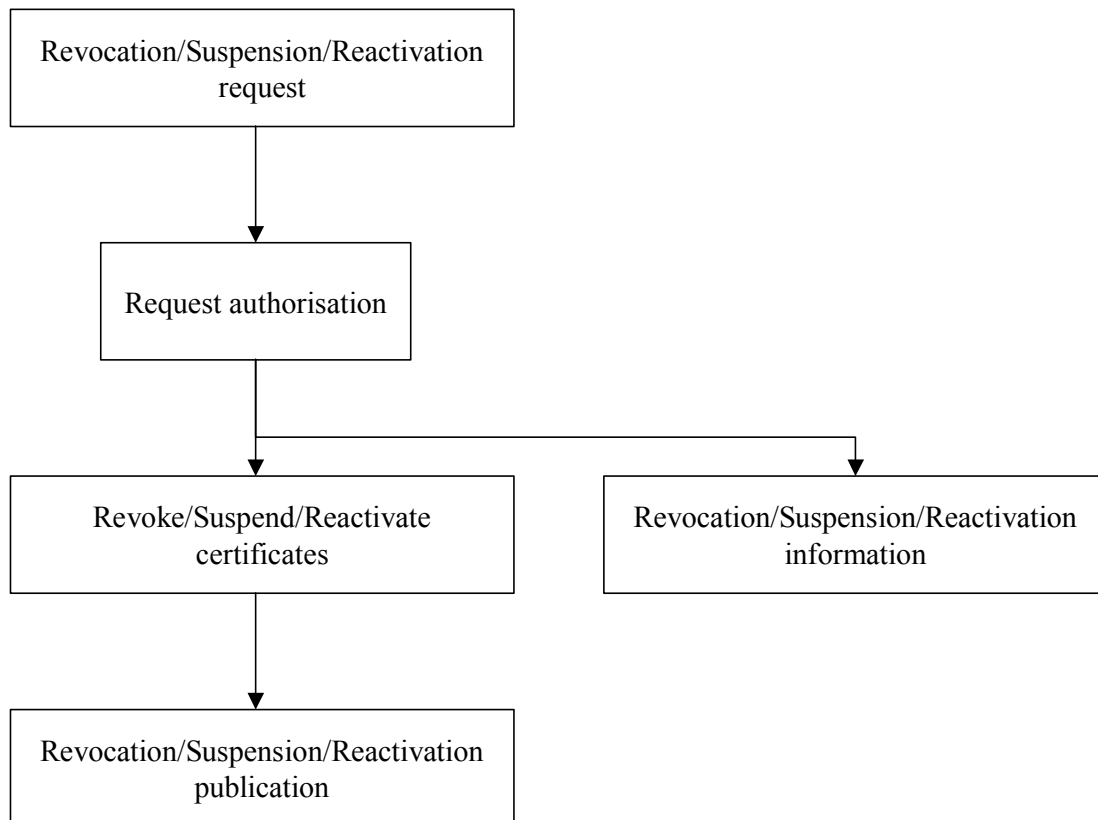
The following processes are identified :

Process 1



The proof of possession can occur either during the upper-left 'Registration (initialisation / update)' block or after the 'Distribute the device to the user' block.

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

Process 2

The service level e.g. reactivity (time response) is rather an organisational matter and is therefore out of the scope of the EUPKI project.

10.2 Time-stamping

There are mainly two approaches to time-stamping :

- simply use the date (in French : 'horodatage'); this approach is acceptable for qualified certificates,
- use date within the digital signature.

Decision of audience : Time-stamping is out of the scope of the EUPKI project (only the use of time-stamping is within the scope of the EUPKI project). This decision is based on the elements :

- no need for a fully reliable time source,
- no need for a date within the digital signature.

10.3 Validation of certificates is out of scope

Decision of audience : Validation of certificates is out of the scope of the EUPKI project since it shall not be performed by the PKI itself but rather by an end-user application.

Decision of audience : OCSP (On-line Certificate Status Protocol) server will not be implemented by the EUPKI project

10.4 Key generation

Decision of audience : Our 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 one of Microsoft Internet Explorer. The reason for this is that, despite the wide use of Internet Explorer, its key generator is not an open source key generator.

10.5 Storage of evidences

Comments on the storage of evidences : 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.

10.6 Recovery

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

The key archive system is important.

11 Examples of PKI

11.1 Net-Enterprises

The use of PKI has been experienced by the GIP-MDS with the Net-Enterprises project.

The registration scenario

The RA is URSSAF and therefore not the GIP-MDS.

The first step is a face-to-face meeting, which is held at the very beginning of the registration process and which is far less expensive when dealing with millions of users than any registration whenever the registration process must be aborted due to some errors such as the lack of a valid official identity card.

During this face-to-face meeting, the identification of the user is fully processed and two passwords are given to the user :

- the first password is used only once in order to activate the user certificate (proof of possession),
- the second password is used by the user during the authentication of the Net-Enterprises application.

The user is also asked to choose a question/answer.

11.2 Vital smart card

The PKI must allow the user to have several certificates of the same type at the same time, as transition periods may exist between two smart cards issued to the same user (the validity period of these two smart cards overlap each other during this transition period).

The PKI must allow certificates to have several attributes (with their corresponding keys) as follows :

- authentication,
- encryption,
- signature.

11.3 Company employees

The use of the PKI is experienced by various participants whenever accessing their own intranet from outside their company (use of certificates). The registration and revocation processes are then automatic; they are performed by a batch routine.

In this case, the RA needs some external data such as the list of employees of the company (e.g. payroll system can be trusted).

The PKI can also be used for internal use within a company.

11.4 Banking

In the banking sector, face-to-face meetings to deliver credit cards to end-users are held at the distribution stage of the PKI, which is at the end of the whole PKI process as opposed to the handling of the face-to-face registration meeting in the Net-Enterprises PKI that occurs at the very beginning of the whole PKI process. Smart cards then locally generate keys (software based or token).

11.5 INTESA

All PKI processes involving INTESA depends on the certification policy statement of INTESA customers.

12 Additional Information

12.1 Roles

The following roles are extracted from the French PKI PPs :

- users,
- operating people, which includes the following roles :
 - operator (of the PKI),
 - system administrator,
 - policy administrator,
 - security officer.

12.2 Users communities

The following users communities are identified :

- citizens,
- employees of a company (the customer is therefore the company itself),
- internal use,
- external use,
- servers, computers (VPN), workstations,
- organisations, employers,
- customers of a service.

Closed groups	Open groups
Examples : employees of a company, internal use, external use	Examples : citizens, external use
The sponsor can expect attributes to be added in the certificates.	

13 Content of the deliverable D3.6

The deliverable D3.6 'Definition of the perimeter of the project and requirements' must contain the following elements :

- Use cases,
- Applications which will use the PKI,
- PKI functions requirements,
- PKI security requirements,
- PKI scaling requirements
 - The maximum number of people using the PKI shall be determined because of its impact on costs and on the technical architecture. OpenLDAP cannot be used to deal with millions of certificates.

14 Some remaining questions

The following questions are still subject for discussion :

NUMBER	QUESTION
1	Which platform(s) shall be supported by the PKI ?
2	Determine interfaces and protocols.

15 Benefits

The following benefits about this brainstorming meeting have been identified by the participants :

- Block & processes are clarified,
- Specifier Giesecke viewpoint on which inputs are needed for WP4 was useful,
- Better idea of the architecture,
- No overlapping between the two brainstorming meetings (only new material),
- AQL training helps to organise our findings,
- Dynamic group (Team Building),
- Open for discussion.

16 Concerns

The following concerns about this brainstorming meeting have been identified by the participants :

- Many contributions are needed between the second and the third brainstorming meetings,
- No tool available to facilitate the communication between participants,
- Not sure yet about the scope of the PKI,
- Need to set-up priority list of functions to be implemented.

17 List of actions

The following actions are to be performed :

ACTION	WHO	WHEN
Determine legal issues	All	ASAP
Map functions with own processes	All	30/05/2002
Provide link with the EU smart card project	Eduard Tric	ASAP
Determine security requirements	All	third meeting (04/06/2002)
Exchange URLs and documents between participants	All	on going
Hold/attend third brainstorming meeting	All	04/06/2002
Answer the questions of §12 'Some remaining questions'	All	ASAP

18 Next meeting

The next meeting is the third brainstorming meeting on 04/06/2002 in Paris (CGE&Y offices).