IST-2001-34340
D3.2 Report of the first meeting

Distribution List :	Project Partners
Author :	Minaradjy Pascal & Pierre-Olivier Baudot, **CGE&Y**
Distribution List :	Project Partners
Authorised by :	Eduard Tric, **GIP-MDS**
Date of Issue :	27 May 2002
Issue :	1.1
File Name :	EUPKI-WP3-D3.2-1.1.doc
Work Package :	WP3 Requirements
Deliverable Number :	D 3.2
Deliverable Type :	Public
Deliverable Nature :	Meeting report
Total Number of Pages :	23
Contact Details for EUPKI :	Project Coordinator Yann Fraval GIP-MDS mail : yann.fraval@gip-mds.fr web site : www.eupki.org

0 Table Of Contents

0 TABLE OF CONTENTS 2

1 DOCUMENT CONTROL 3

1.1 ABSTRACT 3
1.2 KEYWORDS 3

2 MANAGEMENT OVERVIEW 4

2.1 EXECUTIVE SUMMARY 4
2.2 SCOPE STATEMENT 4

3 INTRODUCTION AND GLOSSARY 5

3.1 GLOSSARY 5

4 OBJECTIVES OF THE FIRST BRAINSTORMING MEETING 6

5 PARTICIPANTS OF THE MEETING 7

6 INTRODUCTION 8

6.1 OVERVIEW OF THE AGENDA OF THE MEETING 8
6.2 OBJECTIVES/EXPECTATIONS OF THE PARTICIPANTS 8
6.3 RULES OF THE MEETING 8
6.4 THE BROWN PAPER TECHNIQUE 9

7 BUSINESS SCOPE 10

8 SERVICES 12

9 LEGAL ISSUES 14

10 SECURITY REQUIREMENTS 15

11 LIST OF OTHER NEEDS 17

12 VOLUMETRY 18

13 BUDGETS 19

14 BENEFITS 20

15 CONCERNS 21

16 LIST OF ACTIONS 22

17 NEXT MEETING 23

1 Document Control

Issue	*Date of Issue*	*Comments*
1.0	13 May 2002	Creation
1.1	27 May 2002	Amendments of the validated version 1.0 : RA stands for Registration Authority, Contact details of the new EUPKI project coordinator.

1.1 Abstract

The purpose of the deliverable D3.2 'Report of the first meeting' is to communicate the results achieved during the first brainstorming meeting (24/04/2002) 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'
CGE&Y Cap Gemini Ernst & Young

2 Management Overview

2.1 Executive Summary

This document contains the results achieved during the first brainstorming meeting (24/04/2002). 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 first brainstorming meeting (24/04/2002).

This documents refers to the following external documents :

Reference	Document
D3.1	Brainstorming requirements analysis

3 Introduction and Glossary

A short introduction about the document, defining the content of each section within the document.

3.1 Glossary

CA	Certification Authority
RA	Registration Authority
IS	Information System
CRM	Customer Relationship Management
B2B	Business to Business
ASAP	As Soon As Possible

4 Objectives of the first brainstorming meeting

The aim of the first brainstorming meeting is to determine the business perimeter of the EUPKI project (see §5 'Framework of the brainstorming meetings', D3.1).

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	Eduard Tric
INTESA	Franco Tafini
FINSIEL	Paolo Arenaccio
CERTINOMIS	Jean-Severin Lair, Franck Leroy
AXETEL	Elena Zvarici

6 Introduction

6.1 Overview of the agenda of the meeting

The agenda of the first brainstorming meeting held on 24/04/2002 in Paris (CGE&Y, La Défense) was the following one :

09.30	Introduction
10.00	Business Scope
10.40	Services
11.40	*Break*
12.30	Services (continued)
12.30	*Lunch*
14.00	Legal Issues
14.30	Security Requirements
15.30	*Break*
15.45	List of other needs
16.00	Volumetry
16.30	Budgets
17.00	Benefits & Concerns
17.30	*End of meeting*

6.2 Objectives/Expectations of the participants

The objectives and expectations of the participants were listed at the beginning of the meeting :

- Basic requirements of PKI,
- Determination of all services to be deployed with this PKI,
- Importance of legal issues and of their links with security requirements,
- Business scope and budget,
- Determination of the inside and the outside of the EUPKI project,
- Common vision of the matrix,
- Security functions.

6.3 Rules of the meeting

In order to be able to produce as many ideas as possible before selecting any of them, the following rules were agreed at the beginning of the meeting :

- All ideas are good ideas; no ideas are bad,
- No missiles,
- One meeting – no side conversations,
- Everyone participates,
- Keep to the time contract.

6.4 The Brown Paper technique

A brief explanation of the Brown Paper technique allows participants to master this technique, as described in D3.1 'Brainstorming requirements analysis', §8.1 'Annexe A – Brown Paper'.

7 Business scope

A Brown Paper is dedicated to the determination of the business scope.

Once participants have sticked their post-its on the Brown Paper, the facilitator helps the audience to identify the duplicated contents of post-its and to group the remaining post-its by business.

The outputs of this Brown Paper is therefore the determination of all businesses. Some services have also been identified but need to be completed by the use of another Brown Paper, which will be dedicated to the determination of all services (see §8 Services).

The outputs of the Brown Paper dealing with the business scope are listed below.

	BUSINESSES								
	e-Government scenarios	**Financial Services**	**Home Networking**	**Telco**	**Utilities**	**Health**	**Internal PKI**	**Archive**	**Transverse**
IDEAS	✓ Secure identity ✓ Secure payments ✓ Social Security declarations ✓ Secure e-Declarations ✓ Large Scale PKI for TTP services ✓ E-Government scenarios ✓ E-Government (e-Voting) ✓ Electronic identity card ✓ Bring trust for social declaration ✓ Same security level for small and big companies ✓ Identification of subject	✓ Internet banking ✓ Internet insurance ✓ Secure banking ✓ Authentication in payments ✓ Operations of compensation	✓ Domotics ✓ Domotics, Home Networking	✓ Telco ✓ Telecom-munication ✓ PKI for mobiles	✓ Utilities	✓ Health	✓ Company dedicated PKI ✓ Internal PKI ✓ Corporate/company scenario ✓ Work from home ✓ 'Scientific' use Grid computing	✓ Intellectual property	✓ Electronic forms ✓ Electronic declarations ✓ Certification authority (Romania) ✓ Multiple signatures (validation) ✓ Offer tools for free ✓ Swiss Knife for applications ✓ Tele-declaration ✓ Single identity ubiquity/mobility ✓ Strong security image

8 Services

A Brown Paper is dedicated to the determination of the services of each of the businesses identified in §7 'Business scope'.

Once participants have sticked their post-its on the Brown Paper, the facilitator helps the audience to identify the duplicated contents of post-its and to group the remaining post-its by business.

The output of this Brown Paper is therefore the determination of all services, which are listed below.

	BUSINESSES								
	e-Government scenarios	**Financial Services**	**Home Networking**	**Telco**	**Utilities**	**Health**	**Internal PKI**	**Archive**	**Transverse**
SERVICES	✓ Administrative e-procedure ✓ Tax declaration ✓ e-Voting ✓ Social declarations ✓ e-Procurement ✓ Time stamping ✓ Return receipt	✓ Home banking ✓ Professional banking ✓ On-line insurance ✓ Time stamping ✓ Return receipt	✓ Customer Home Networking (access to domestic control portal, to home computers …) ✓ Service Provider Home Networking (remote administration, remote maintenance …)	✓ Secure access to Back-Office (network admin) ✓ VPN ✓ Mobile services	✓ Monitoring	✓ Medical "paper" treatment ✓ Clinical essays ✓ Secure document exchange (secure mailing) ✓ Key recovery	✓ EDI, ebXML ✓ e-Procedures ✓ Secure access to Information System (IS) ✓ Key recovery ✓ Home working ✓ Secure e-mail ✓ Telecom infrastructure (VPN) ✓ Grid computing	✓ Time stamping ✓ Notarization ✓ Authentication/ signature	✓ Code signing ✓ Secure mailing ✓ Revocation ✓ Time stamping ✓ Confidentiality ✓ Signature (multiple) ✓ Multiple identities ✓ e-Declaration (B2B) ✓ Mail tracking ✓ CA (trust image) ✓ Secure access to IS ✓ Federation with other services ✓ Customer Relationship Management (CRM) ✓ Form signing ✓ e-Order ✓ e-Billing ✓ e-Payment ✓ Contract Management

The transverse column is just a working area where we put together services common to some businesses.
A service in that column is not always common to each business (e.g. contract management, e-billing)
But you can find, some services repeated in many columns (e.g. time stamping) because participants think they are different between businesses.

9 Legal issues

Since the audience does not have any knowledge of law, most participants need to perform some further investigations on the legal issues of the PKI. Therefore these later legal issues remain to be determined as soon as possible (before the second brainstorming meeting if possible) :

- Each participant will gather some information about the legal issues from the Legal Department of the company he/she belongs to,
- GIP-MDS will contact the European Commission

No output dealing with legal issues has been yet produced.

10 Security requirements

A Brown Paper is dedicated to the determination of the security requirements.

Businesses and services have been determined by the matrix in §7 and §8. The audience proposed to determine the security requirements with a PKI modular approach rather than with the use of the matrix (Businesses, Services).

The participants first determine the topics of the security requirements. These topics (or PKI modules) are listed below :

- RA (Registration Authority),
- CA (Certification Authority),
- Protocols,
- Directory,
- Key Archive,
- Time Stamping & Notarization,
- Validation Authority.

Once participants have sticked their post-its on the Brown Paper, the facilitator helps the audience to identify the duplicated contents of post-its and to group the remaining post-its by topic.

The outputs of this Brown Paper is therefore the determination of the security requirements, which are listed below.

	RA	Common to RA and CA	CA	Protocols	Directory	Key Archive	Time Stamping & Notarization	Validation Authority
SECURITY REQUIREMENTS	✓ Graphical Policy Editor ✓ Privacy ✓ Reliable Information ✓ Multilevel Requirements ✓ Profiles ✓ Automatic registration ✓ Consultation of external info/basis	✓ Operating system ✓ Role separation ✓ All entities/modules authentication ✓ System integration ✓ System recovery ✓ Integrity of log files ✓ Operator strong authentication	✓ High availability ✓ High availability of revocation ✓ HSM, Smart Card/HSM Interface, Physical protection of CA key	✓ Encrypted Protocol ✓ Secure exchange between modules ✓ Authentication protocol for technical entities modules ✓ Authentication protocol for human operation, Authentication ✓ Habilitation of modules to perform actions		✓ m-2-n, Protection of key archives by several keys ✓ Key fragmentation	✓ Secure time source	✓ On-line

Priorities have been defined :

- High Priority : RA, Common to RA and CA, CA, Protocols
- Low Priority : Directory, Key Archive, Time Stamping & Notarization, Validation Authority

11 List of other needs

A list of some additional needs is made on a flip chart.
The following needs are identified :

- Volumetry (see §12 'Volumetry'),
- Budgets (see §13 'Budgets'),
- Localisation (language specificities such as accents, etc.),
- Connexion to external sources (external databases, etc.),
- Documentation,
- Ease of installation,
- Portability (plateforms),
- Maintenability & maintenance,
- Ease of administration,
- Administration of logs,
- Key ceremony (generating process),
- Ease of renewal process.

12 Volumetry

To complete requirements with deployment and operations, participants determined volumetry constraints.
The following volumetry items are identified :

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

13 Budgets

To complete requirements with economic model, participants determined budget constraints.
The following budget items are identified :

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

14 Benefits

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

- Brainstorming method (first experience for some participants),
- Identification of several businesses and services (the list can still be amended anyway),
- Identification of priorities (RA, CA and Protocols, etc.),
- Team building,
- Discovery of new approaches to PKI,
- Other identified needs to work on,
- Timing

15 Concerns

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

- Legal aspects require expertise of lawyers,
- PKI processes still to be determined,
- Structure of the matrix is subject for discussion for the next two brainstorming meetings.

16 List of actions

The following actions are to be performed :

ACTION	WHO	WHEN
Determine legal issues	All	ASAP
Contact European Commission about legal issues	GIP-MDS	ASAP
Determine PKI processes	All	22/05/2002
Propose structure of the next two brainstorming meetings (process approach, security functions of PKI, etc.)	CGE&Y	ASAP
Deliver training on security	AQL	21/05/2002
Hold/attend second brainstorming meeting	All	22/05/2002

17 Next meeting

The next meeting is the AQL security training on 21/05/2002 in Paris, which will be followed by the second brainstorming meeting on 22/05/2002 in Paris (CGE&Y offices).