



# IST-2001-34340

## D3.4 Report of the third meeting

|                             |   |
|-----------------------------|---|
| Distribution List :         | Project Partners  |
| Author :                    | Minaradjy Pascal & Pierre-Olivier Baudot, <b>CGE&amp;Y</b>  |
| Distribution List :         | Project Partners  |
| Authorised by :             | Yann Fraval, <b>GIP-MDS</b>   |
| Date of Issue :             | 14 June 2002  |
| Issue :                     | 1.0   |
| File Name :                 | EUPKI-WP3-D3.4-1.0.doc  |
| Work Package :              | WP3 Requirements  |
| Deliverable Number :        | D 3.4   |
| Deliverable Type :          | Public  |
| Deliverable Nature :        | Meeting report  |
| Total Number of Pages :     | 21  |
| Contact Details for EUPKI : | Project Coordinator Yann Fraval GIP-MDS<br>mail : <a href="mailto:yann.fraval@gip-mds.fr">yann.fraval@gip-mds.fr</a><br>web site : <a href="http://www.eupki.org">www.eupki.org</a> |

## 0 Table Of Contents

|           |  |           |
|-----------|--|-----------|
| <b>0</b>  | <b>TABLE OF CONTENTS .....</b>   | <b>2</b>  |
| <b>1</b>  | <b>DOCUMENT CONTROL .....</b>  | <b>3</b>  |
| 1.1       | ABSTRACT .....   | 3         |
| 1.2       | KEYWORDS .....   | 3         |
| <b>2</b>  | <b>MANAGEMENT OVERVIEW .....</b>                                       | <b>4</b>  |
| 2.1       | EXECUTIVE SUMMARY .....  | 4         |
| 2.2       | SCOPE STATEMENT .....  | 4         |
| <b>3</b>  | <b>INTRODUCTION AND GLOSSARY.....</b>                                  | <b>5</b>  |
| 3.1       | GLOSSARY .....   | 5         |
| <b>4</b>  | <b>OBJECTIVES OF THE THIRD BRAINSTORMING MEETING.....</b>              | <b>6</b>  |
| <b>5</b>  | <b>PARTICIPANTS OF THE MEETING.....</b>                                | <b>7</b>  |
| <b>6</b>  | <b>INTRODUCTION .....</b>  | <b>8</b>  |
| 6.1       | OVERVIEW OF THE AGENDA OF THE MEETING .....                            | 8         |
| <b>7</b>  | <b>CGE&amp;Y INTRODUCTION TO THE THIRD BRAINSTORMING MEETING .....</b> | <b>9</b>  |
| <b>8</b>  | <b>PKI FUNCTIONS REQUIREMENTS.....</b>                                 | <b>10</b> |
| 8.1       | MAIN PROCESS.....  | 10        |
| 8.2       | ACTORS AND OPERATORS.....  | 11        |
| 8.3       | PKI SCENARIOS .....  | 11        |
| 8.3.1     | <i>Main scenario.....</i>  | <i>11</i> |
| 8.3.2     | <i>Company scenario.....</i>   | <i>12</i> |
| 8.3.3     | <i>Sub-scenarios.....</i>  | <i>12</i> |
| <b>9</b>  | <b>PKI SECURITY REQUIREMENTS.....</b>                                  | <b>14</b> |
| 9.1       | ASSETS .....   | 14        |
| <b>10</b> | <b>PKI ADMINISTRATION.....</b>   | <b>15</b> |
| 10.1      | LIST OF NEEDS .....  | 15        |
| 10.2      | EVENT LOG .....  | 15        |
| <b>11</b> | <b>FUNCTIONAL ARCHITECTURE.....</b>                                    | <b>16</b> |
| 11.1      | FEEDBACK ON GIESECKE'S QUESTIONNAIRE.....                              | 16        |
| 11.2      | PLATFORMS .....  | 16        |
| 11.3      | PROTOCOLS AND STANDARDS .....  | 16        |
| 11.4      | MODULARITY .....   | 16        |
| <b>12</b> | <b>CONTENT OF THE DELIVERABLE D3.6.....</b>                            | <b>17</b> |
| <b>13</b> | <b>BENEFITS .....</b>  | <b>18</b> |
| <b>14</b> | <b>CONCERNS.....</b>   | <b>19</b> |
| <b>15</b> | <b>LIST OF ACTIONS .....</b>   | <b>20</b> |
| <b>16</b> | <b>NEXT MEETING.....</b>   | <b>21</b> |

## 1 Document Control

| <i>Issue</i> | <i>Date of Issue</i> | <i>Comments</i> |
|--------------|----------------------|-----------------|
| 1.0          | 14 June 2002         | Creation        |

### 1.1 Abstract

The purpose of the deliverable D3.4 'Report of the third meeting' is to communicate the results achieved during the third brainstorming meeting (04/06/2002) 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'        |
| D3.4    | Reference to the deliverable 'D3.4 Report of the third meeting'         |
| PKI     | Public Key Infrastructure   |
| GIP-MDS | Groupement d'Intérêt Public Modernisation des Déclarations Sociales     |
| CGE&Y   | Cap Gemini Ernst & Young  |

## 2 Management Overview

### 2.1 Executive Summary

This document contains the results achieved during the third brainstorming meeting (04/06/2002). 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 third brainstorming meeting (04/06/2002).

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        |

## **3 Introduction and Glossary**

### **3.1 Glossary**

CP Certification Policy

## **4 Objectives of the third brainstorming meeting**

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

- Validation of the deliverable D3.3 'Report of the second meeting',
- 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           | Minaradjy Pascal, Pierre-Olivier Baudot |
| GIP-MDS        | Yann Fraval                             |
| INTESA         | Franco Tafini                           |
| AXETEL         | Eduard Tric                             |
| ON-X           | Peter Sylvester                         |
| AQL            | Christophe Anier                        |

## **6 Introduction**

### **6.1 Overview of the agenda of the meeting**

The agenda of the third brainstorming meeting held on 04/06/2002 in Paris (CGE&Y, La Défense) was the following one :

|              |  |
|--------------|--|
| 09.30        | Introduction (PowerPoint presentation – file : Thirdmeeting2.ppt)<br>PKI functions |
| <i>13.00</i> | <i>Lunch</i>   |
| 14.00        | PKI functions<br>Security requirements<br>PKI Administration                       |
| 17.20        | List of actions  |
| 17.30        | Benefits & Concerns  |
| <i>17.40</i> | <i>End of meeting</i>  |

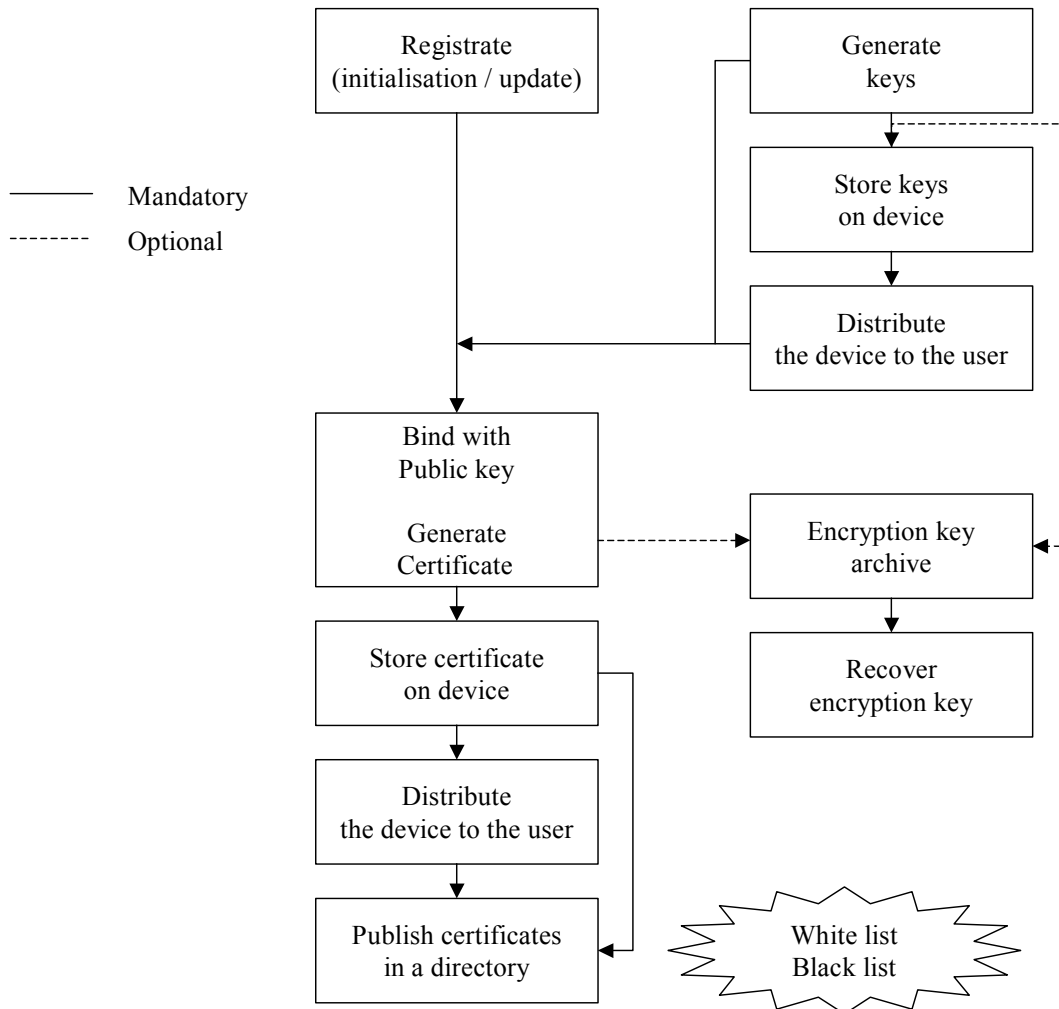
## 7 CGE&Y introduction to the third brainstorming meeting

A PowerPoint presentation (file Thirdmeeting2.ppt) deals with the following items :

- Validation of the deliverable D3.3 'Report of the third meeting'  
Decision of the audience : the participants approve version 1.0 of the deliverable D3.3 'Report of the second meeting'.
- Feedback on questionnaire (since second meeting)
  - On-X and EADS feedback
  - FT
  - EDF examples of CP
- PKI functions requirements
  - CGE&Y example of internal PKI
    - Capkey
  - FT example of internal PKI
  - On-X example
    - Openevidence
  - FINSIEL example of Pension Fund PKI
  - GIP-MDS needs of authentication mean in the context of Net-Enterprises
- PKI security requirements
  - Giesecke proposal to use EESSI deliverables
  - AQL proposal for a support to determine assets, threats and security objectives
- Architecture
  - Open Source
  - Platforms
  - Protocols and standards
  - Scaling requirements
- Content of the deliverable D3.5
  - Use case
  - Functions requirements
  - Security requirements
  - Functional architecture
- Legal issues
  - GIP-MDS
  - Participants
    - Extract from Romanian law regarding the electronic signature
- Next steps
  - Every participant is a contributor to this deliverable  
CGE&Y is also the facilitator of the WP3
  - Payment of the co-contractors
  - D3.5 draft review meeting
  - WP4 first meeting
  - Customer Satisfaction Evaluation

## 8 PKI functions requirements

### 8.1 Main process



White list : valid certificates list  
 Black list : certificates revocation list

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

The black list is mandatory to be published, while the white list is not. Anyway the PKI must allow the publishing of the white list since owners or group of owners of certificates (e.g. company) can decide whether his/her certificate can be published. For example, it is up to a company to decide who can view the white list of its employees certificates (e.g. whether the white list can be viewed only by its employees or also by the public).

## 8.2 Actors and Operators

Actors and Operators are considered as different PKI set of communities.

| <b>Actors</b>   | <b>Operators</b>         |
|---|--------------------------|
| Agents and users  | PKI administration       |
| End-users <ul style="list-style-type: none"> <li>• People</li> </ul>                            | Infrastructure operators |
| Sponsors <ul style="list-style-type: none"> <li>• Company</li> <li>• Human resources</li> </ul> |                          |
| Registration agent  |                          |
| Certification agent<br>(each block in §8.1 has its own agent)                                   |                          |
| Auditors  |                          |

## 8.3 PKI scenarios

There are two types of PKI scenarios which involve registration agents :

- Main scenario
- Company scenario

### 8.3.1 Main scenario

- The user fills a form to generate a certificate.
  - Context : The user already generated his/her keys (public and private) the user provides his public key to the registration agent (PKCS#10),  
or
  - Context : The user has NOT generated his/her keys (public and private) the user requests to have his/her keys generated (PKCS#12) - the private key can be optionally protected by a password chosen by the user.  
*Nota. - This sub-scenario has not been discussed by the audience due to the lack of time needed by such a complex scenario.*
- The registration agent checks the validity of the request, which status can be :
  - pending,
  - accepted,
  - rejected.
- The registration agent transmits the request (with the user information needed by the PKI and the user public key) to the certification agent after having signed it :
  - manually (electronic forms),  
or
  - automatically (batch or real-time).
- The registration agent receives the acknowledgement from the certification agent.
- The registration agent receives the result of the request.
- The registration agent can view the current status of any request.
- The certification agent transmits the certificate to the distribution agent.
- The distribution agent delivers the certificate to the user.

- The distribution agent informs the certification agent that the certificate was delivered to the right user (PKCS#12).
- 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.

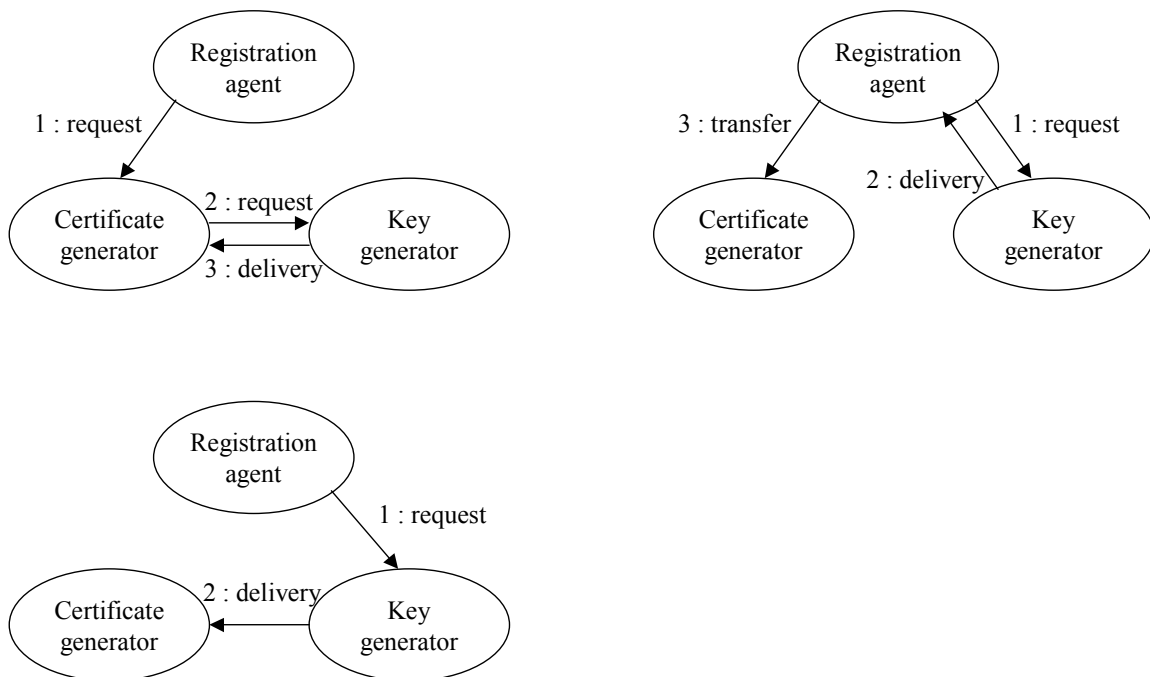
### 8.3.2 Company scenario

The company scenario is similar to the standard scenario described in §8.3.1 'Main scenario' but is processed in a far more automatic way. For example, the registration request can be performed automatically by accessing the company staff database.

### 8.3.3 Sub-scenarios

#### 8.3.3.1 Key generation scenario

The audience determined the following 3 scenarios of the key generation :



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

There are two means of protecting the private key :

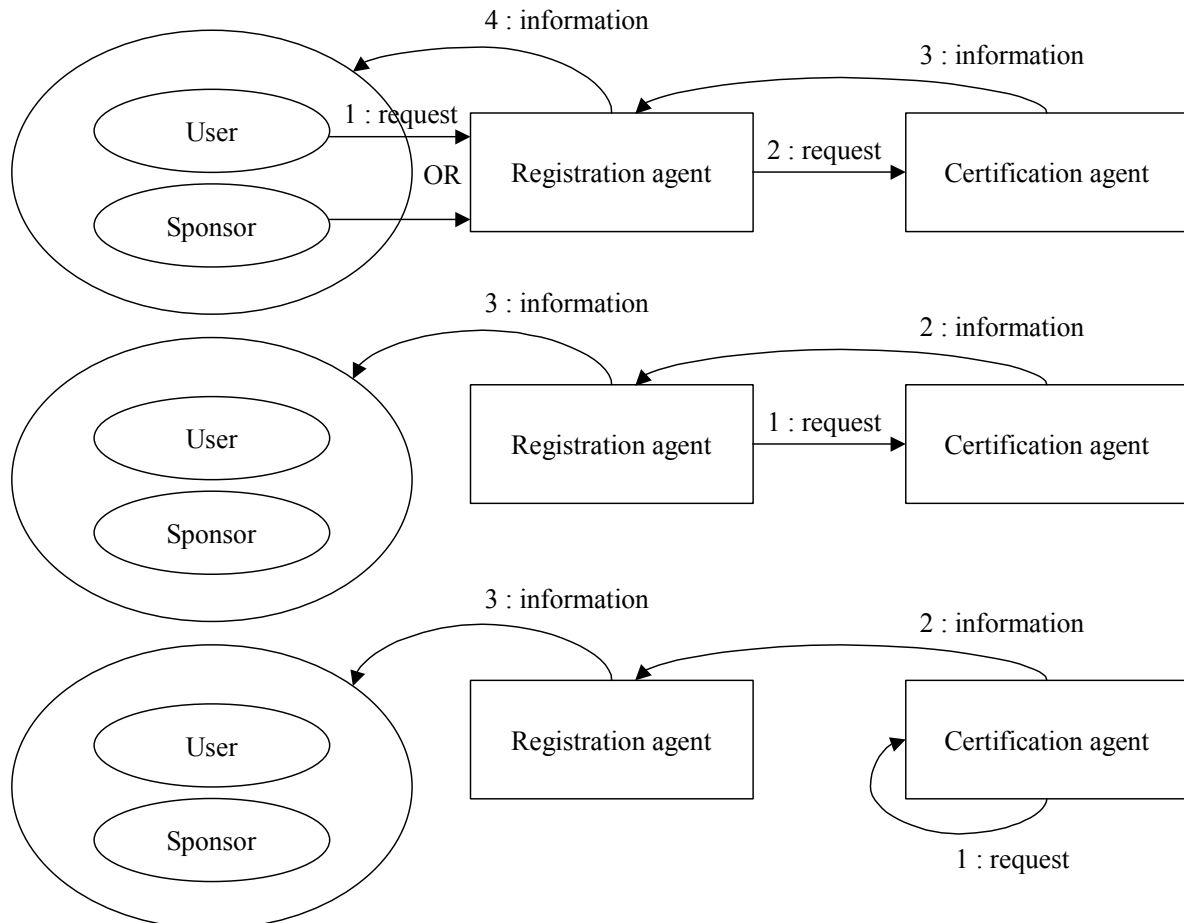
- password chosen by the user,
- pin code provided by the key generator.

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

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

*8.3.3.2 Revocation scenario*

The audience determined the following 3 scenarios of the revocation :



The actors can revoke certificates depending on their rights.

## **9 PKI security requirements**

### **9.1 Assets**

The different kinds of security requirements are :

- Confidentiality,
- Integrity,
- Availability.

AQL is expected to propose security requirements on PKI assets on 07/06/2002 to all participants. Feedback is expected from participants before 14/06/2002.

## **10 PKI Administration**

### **10.1 List of needs**

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

- Initialisation,
- Key ceremony,
- Key recovery,
- Split responsibilities,
- Event log
- Administration of roles.

Participants who have some experience of PKI administration are expected to send their contributions about PKI administration before 21/06/2002.

### **10.2 Event log**

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

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

The list of events to be logged from a functional point of view has not been defined by the audience.

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.

## **11 Functional architecture**

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

### **11.1 Feedback on Giesecke's questionnaire**

Participants are expected to inform Giesecke about :

- the open source code that their company can provide for free to the EUPKI project,
- some existing open source code outside their company which would be helpful to the EUPKI project.

### **11.2 Platforms**

The PKI must be platform independent.

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

### **11.3 Protocols and standards**

The PKI must use open standards in order to :

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

The PKI must use open high level protocols and standards.

### **11.4 Modularity**

The PKI shall make full use of modularity.

## **12 Content of the deliverable D3.6**

The deliverable D3.6 'Definition of the perimeter of the project and requirements' must contain the following elements (the deliverable D3.6 is the final version of the draft D3.5) :

- 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.

## **13 Benefits**

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

- Dynamic group (Team Building),
- No useless overlapping between the second and third brainstorming meetings,
- Contributions before the third meeting
- Concrete examples of scenarios.

## **14 Concerns**

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

- Agenda with time management would have been helpful,
- Fewer participants.

## 15 List of actions

The following actions are to be performed :

| <b>ACTION</b>  | <b>WHO</b> | <b>WHEN</b>          |
|--|------------|----------------------|
| Send proposal on security requirements to all participants   | AQL        | 07/06/2002           |
| Send feedback on security requirements proposed by AQL   | All        | Before<br>14/06/2002 |
| Send feedback on Giesecke's questionnaire  | All        | Before<br>14/06/2002 |
| Produce some stable chapters of a working version 0.1 of the draft D3.5 to be sent to all participants                       | CGE&Y      | 14/06/2002           |
| Send feedback on draft D3.5  | All        | Before<br>21/06/2002 |
| Send contributions about PKI administration from participants who have some experience of it (e.g. §10 'PKI Administration') | All        | Before<br>21/06/2002 |
| Produce the working version 0.2 of the draft D3.5  | CGE&Y      | 21/06/2002           |
| Send feedback on draft D3.5  | All        | Before<br>28/06/2002 |
| Produce the version 1.0 of the draft D3.5  | CGE&Y      | 28/06/2002           |
| Hold/attend the two-day meeting mentioned in §16   | All        | 04-05/07/2002        |

## **16 Next meeting**

The next meeting is a two-day meeting held in München :

- the draft review meeting on 04/07/2002
- the WP4 kick-off meeting on 05/07/2002.