INFORMATION SOCIETIES TECHNOLOGY (IST) PROGRAMME

D.1.2.1: EuPKI 1st Technical Management Report

Period April 1st – December 31, 2002

Authors: D.BONNEROT
EADS-TELECOM
Version: 1.0
Date: 20/01/03
Status: VALIDATED

0 Table of Contents

1 Technical board Overview

1.1 Abstract

The purpose of the deliverable D1.2.1 "Technical management Report 1" is to make the point upon all the actions and the decisions which were elaborated by the consortium, during the first period of the activity, from April to December 2002.
Moreover it gives a view of the quality management which has to be taken place, during the development phase and the integration phase, for the acceptance of PKI modules.
This document will progress and be updated all along the project, in order to reflect as much as possible the technical progress of the project.

1.2 Technical Board Overview

1.2.1 Technical Board function

This board is lead by the Technical Manager (D.BONNEROT) and includes a representative from each technical partner. The Technical Board is in charge of the technical development of the project. Problems detected by the Technical Board are be reported to the Steering Board, which has the full responsibility of decision making.

All Work Package Managers, who are responsible for co-ordination of tasks and activities towards the WP objectives, report to the Technical Board about deviations from scheduling, suitability or expected results, designation and co-ordination of tasks leaders.

In order to be very efficient during the Technical Board, the Manager has asked all the members to transmit the technical subjects that they want to discuss one week before. Some time (it was the case for the last technical board), a technical meeting is organized in order to discuss, in detail, some technical points and prepare, if it is possible, the recommendations for the technical board.

1.2.2 Technical work

Except for the WP1 and WP2, the works of all others WP has to be accepted by the technical board.

1.2.2.1 WP3: Requirements

The WP3: "Requirements" started during the Kick Off Meeting in April, with the principal objectives to put in relief the requirements and the global scope of the project.

The method chosen by the WP3 leaders, CGE&Y, was to lead brainstorming with all the WP3 members and voluntary members. It allowed producing three brainstorming meetings reports (D.3.2, D.3.3, D.3.4), one brainstorming method deliverable (D.3.1).

Then, the first project perimeter and requirements draft (D.3.5) was validated in August to let the place to the definitive Project Perimeter & Requirements Deliverables (D.3.6) in September.

1.2.2.2 WP4: Design & Specifications

The WP4: "Specifications & Design", led by Giesecke & Devrient, has been kicked off during the first Steering Meeting in July.

It produced the Architectural Specifications (D.4.1) that has been validated during the Second Steering Board.

Then, it is currently working on the design of the components interfaces, which was the object of the two following deliverables, D.4.2 & D.4.3

1.2.2.3 WP5: Implementation

The WP5: "Implementation", led by AXETEL, has been kicked off during the Second Steering Meeting. It is currently drawing action plans and planning the delivery of the modules put in evidence in the D.4.1.

1.2.2.4 WP6: Integration

The WP6: "Integration", led by ON'X, has produced one formal document (D6.1) to explain the way the consortium will or not integrate external PKI modules, the validation process they will have to be submitted to, the sources we could integrate and finally the responsibilities the contributors will have to take.

1.2.2.5 WP7: Demonstration

The WP7: "Demonstration", led by CertiNomis, has participated to the elaboration of the deliverables of WP3 & WP4.

1.2.2.6 WP8: Guidelines for Security & Homologation

The WP8: "Guidelines for Security & Homologation", led by AQL, delivered two deliverables :

- D.8.1 summarizing general aspects for a potential homologation
- D8.2 defining the security functional requirements for all PKI modules

More than that, it participated in every technical meeting of the consortium to give the necessary technical framework for a potential homologation, pointed out at the end of the project. It disclaimed all security level aspects.

1.3 List of Technical Meetings

The list of the technical meetings is :

- Concerning Technical Boards Meetings:
  - Kick Off Meeting in Paris, at GIP-MDS: 13th & 14th of April 2002

- 1st Technical Board Meeting in Munich, at Giesecke & Devrient: 5th of July 2002
- 2nd Technical Board Meeting in Paris, at GIP-MDS: 24th of September 2002
- 3rd Technical Board Meeting in Paris, at GIP-MDS: 28th of November 2002

- Concerning internal WP3 meetings :
  - Kick Off Meeting in Paris, at GIP-MDS: 13th & 14th of April 2002
  - First Brainstorming Meeting: 24th of April 2002 in Paris at CGE&Y
  - Second Brainstorming Meeting: 22nd of May 2002 in Paris at CGE&Y
  - Third Brainstorming Meeting: 4th of June 2002 in Paris at CGE&Y
  - Draft review Meeting: 4th of July 2002 in Munich, at Giesecke & Devrient
  - Final Review Meeting: 24th of September 2002 in Paris, at GIP-MDS.
  - Concerning internal WP4 meetings:
  - Kick Off Meeting in Munich, at Giesecke & Devrient: 12th of July 2002
  - D.4.1 Draft Review Meeting in Munich, at Giesecke & Devrient: 8th of August 2002
- Concerning WP8 meetings :
  - One training day organized by AQL in Paris, at CGE&Y: 21st of May 2002.

1.4 List of Technical decision

The list of the technical decisions which were adopted during technical boards is :

- First Technical Board :
  - About technical documents : Agreement of the first WP3 documents even if some aspects are still not covered
  - About legal aspect : Need to have an acceptance process for the PKI modules
  - About technical subjects : EADS-TELECOM and On-X and Axetel prepare a draft-proposal for next Technical Board meeting
- Second Technical Board :
  - About technical documents :
    - Agreement of the WP3 deliverable D.3.6
    - Agreement of the WP4 deliverable D.4.1
    - Agreement of the WP8 deliverable D.8.1
  - About legal aspect :
    - Agreement of the WP3 deliverable D.3.6
    - Need to sign a chart about the obligations of each member 'GIP-MDS)
    - Need to write on the Web site that no body guarantees nothing (Actimage)
    - Need to have a validation process and it could be good to put it on the Web site
  - About technical subjects :
    - Agreement of technical choice : OpenSSL, Apache and MySQL
- Third Technical Board :
  - About technical documents :
    - Agreement of the WP4 deliverables D.4.2 and D4.3

- Agreement of the WP8 deliverable D.8.2 (Need a final review in order to answer to a few questions)
- Agreement of the WP6 deliverable D.6.1

o About legal aspect : Agreement of the propositions about source code dissemination (responsibility of contributors, host disclaimer)

o About technical subjects :

- Integration process : see §3
- Source code servers organization :
  - CVS 0 : Development Server (internal to Axetel)
  - CVS 1 : Consortium Server (Axetel responsibility)
  - CVS 2 : Public Server
    - Zone A : public access for everyday work with free/open-source developers with invalidated code-contributions
    - Zone B : public access for validated code – access after qualification
    - To be in line with the European commission willing this CVS will be open to public access as soon as possible (on February 2003)
- Agreement of technical choice :
  - Programming language : JAVA (see §4)
  - Cryptography : BouncyCastle
  - For the development and integration platform :
    - Operating System : Linux Mandrake version ?
    - Data base (MySQL) à Version 4
    - Ldap V3 with OpenLdap
    - Apache Mod_SSL version ? / Tomcat-Jboss version ?
    - Secured transfer protocol : No technological preference but standard solution
  - For the validation platform : No requirement of using a HSM

2 Technical Actions and Reports

2.1 GIP-MDS

2.1.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis -Participation to the Requirements Brainstorming Meetings lead by CGE&Y
T3-2	Definition of the project perimeter and requirements -Participation to the redaction of the deliverables D.3.2, D.3.3, D.3.4, D.3.5, D.3.6
WP4	**Specifications & design**
T4-1	Overall Architecture -Attendances to the internal WP4 meetings -Participation to the redaction of the architecture deliverable D.4.1

2.1.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final
WP4/T4-1	M4	D.4.1 Architectural Specifications	Final
WP4/T4-2	M8	D4.2 « Specification of External Interfaces »	Final
WP4/T4-3	M8	D4.3 « Internal functional specification »	Final

2.2 AQL

2.2.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis - Brainstorming - Participation in working meetings(3) in Paris - Reading activities & feedbacks
T3-2	Definition of the project perimeter and requirements - Reading activities & feedbacks - Brainstorming & participation in the Deliverable 3.6
WP4	**Specifications & design**
T4-1	Overall Architecture - Participation in the specific annex concerning security - Reading activities
WP8	**Guidelines for Security & Homologation**
T8-1	Scope of the homologation process - Animation, reflexion and writing of the D8.1 - Animation of a specific workshop on the Common Criteria
T8-2	Stating of the Security requirements - Document in progress, draft document has been proposed

2.2.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP8/T8.1	M3	D8.1 v1.0 : "Security Reference Document List"	Final
WP8/T8.2	M4	D8.2 v0.03 : "Components subject to homologation process"	Final

2.3 AXETEL

2.3.1 Technical work accomplished this period

WP/ Task	Action
WP3	**Requirements**
T3-1	Requirements Analysis: -Participation to the Brainstorming Meetings lead by CGE&Y -Participate to the user requirements and needs. -Express the Romanian specificities for setting a PKI service. -Translate the Romanian law on electronic signature

T3-2	Perimeter of the project: -Participation to the redaction of the deliverables D.3.5 & D.3.6
WP4	**Specifications & Design**
T4-1	Architectural Specifications - Participate to the design process.
WP5	**Implementation**
T5-1	Development of the components -Maintain the software. -Be sure that specifications are realistic

2.3.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final
WP4/T4-1	M4	D.4.1 Architectural Specifications	Final
WP4/T4-2	M8	D4.2 « Specification of External Interfaces »	Final
WP4/T4-3	M8	D4.3 « Internal functional specification »	Final
WP5/T5-1		R5.4 « Use case »	Draft
WP5/T5-1		R5.5 « Architecture, Design & Implementation »	Draft
WP5/T5-1		R5.6 « Delivery Planning Phase 1 »	Draft

2.4 CERTINOMIS

2.4.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis - Participation to the Brainstorming Meetings - Participation to the redaction of the deliverables D.3.1, D.3.2, D.3.3, D.3.4
T3-2	Definition of the project perimeter and requirements - Participation to the redaction of the deliverables D.3.5, D.3.6
WP4	**Specifications & design**
T4-1	Overall Architecture - Participation to the definition of the architectural specifications - Participation to the redaction of the deliverable D.4.1

2.4.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final
WP4/T4-1	M4	D.4.1 Architectural Specifications	Final
WP4/T4-2	M8	D4.2 « Specification of External Interfaces »	Final
WP4/T4-3	M8	D4.3 « Internal functional specification »	Final

2.5 INTESA

2.5.1 Technical work accomplished this period

WP/ Task	Actions

WP3	Requirements
T3-1	Requirements Analysis INTESA has participated to WP3 in order to define the business & organizational model for a PKI implementation starting from our experience as commercial and public CA.
T3-2	Definition of the project perimeter and requirements We have attended all meetings dedicated to this WP and provided organizational and technological contributions.

2.5.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final

2.6 CGE&Y

2.6.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis - Lead, organization and coordination of the Brainstorming Meetings - Production of the deliverables D.3.1, D.3.2, D.3.3, D.3.4
T3-2	Definition of the project perimeter and requirements - Production of the deliverables D.3.5, D.3.6 - Definition of the perimeter of the project
WP4	**Specifications & design**
T4-1	Overall Architecture - Participation to the definition of the architectural specifications - Participation to the redaction of the deliverable D.4.1

2.6.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final
WP4/T4-1	M4	D4.1 « Architectural Specification »	Final
WP4/T4-2	M8	D4.2 « Specification of External Interfaces »	Final
WP4/T4-3	M8	D4.3 « Internal functional specification »	Final

2.7 EDF

2.7.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis : Internal inquiries (requirements definition) and restitution Brainstorming sessions attendance and participation Inputs and feedbacks on all the related deliverables (D.3.1, D.3.2, D.3.3, D.3.4)
T3-2	Definition of the project perimeter and requirements: Feedbacks and inputs for the D.3.5 & D3.6 deliverables Meetings attendance

2.7.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final

WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final

2.8 FT R&D

2.8.1 Technical work accomplished this period

WP/ Task	**Actions**
WP3	**Requirements**
T3-1	Requirements Analysis - Participation to the Brainstorming Meetings - Participation to the redaction of the deliverables D.3.1, D.3.2, D.3.3, D.3.4
T3-2	Definition of the project perimeter and requirements - Participation to the redaction of the deliverables D.3.5, D.3.6

2.8.2 Deliverables due this period

WP/ Task	**Due**	**Deliverable**	**Status (Final, Draft, Pending)**
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final

2.9 FINSIEL

2.9.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis: Finsiel took part to the following Requirement Analysis meetings: - Paris, 24th of April 2002 - Paris, 21st of May 2002 - Paris, 4th of June 2002 Finsiel cooperated to the definition of end user requirements and scenarios and to the preparation of WP Deliverables
T3-2	Definition of the project perimeter and requirements: Finsiel took part to the WP3 review meeting held in Munich on 4th of July 2002 and contributed to the final refinement of WP Deliverables

2.9.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final

2.10 INPS

2.10.1 Technical work accomplished this period

WP/ Task	Action
WP3	**Requirements**
T3-1	Requirements Analysis: -Participation to the Brainstorming Meetings lead by CGE&Y
T3-2	Perimeter of the project: -Participation to the redaction of the deliverables D.3.5 & D.3.6

2.10.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP3/T3-1	M0,5	D.3.1 Brainstorming Requirement Analysis	Final
WP3/T3-1	M1	D.3.2 Report of First Meeting	Final
WP3/T3-1	M1,5	D.3.3 Report of Second Meeting	Final
WP3/T3-1	M2	D.3.4 Report of Third Meeting	Final
WP3/T3-2	M2,5	D.3.5 Review of the draft of the definition of the perimeter of the project	Final
WP3/T3-2	M3	D.3.6 Definition of the perimeter of the project	Final

2.11 Giesecke & Devrient

2.11.1 Technical work accomplished this period

WP/ Task	Actions
WP3	**Requirements**
T3-1	Requirements Analysis - participated in workshops in Paris, - participated in document organization and writing
T3-2	Definition of the project perimeter and requirements - driven discussion on project requirements - participated to meetings and document organization and writing
WP4	**Specifications & design**
T4-1	**Specification of Overall Architecture** - organized kick-off meeting - structured the document - planned the work - received approval from consortium - organized working meetings and TV conferences - organized the work packages of every WP 4.1 participant - collected input form consortium members who are not part of the WP 4 - written over half of the document - reorganized work load distribution - written use cases - defined module structure and list

	- with other WP4 members specified each module - organized review meeting and integration of comments in to D4.1 - coordinated the checks with the WP3 documents - delivered input to the WP3 documents - delivered the full, approved, and final WP 4.1 document called **"Architectural specification"**
T4-2	**Specification of External Interface** - presented the kick-off in Paris - structured the document - got approval from the consortium - organized the weekly work packages of every WP 4.2 participant - written and distributed first draft of document
T4-3	**Specification of relations between core components** - presented the kick-off in Paris - structured the document - got approval from the consortium - organized the weekly work packages of every WP 4.3 participant
WP5	**Implementation**
T5-1	Development of the components - collected input about existing components - summarized the input to the WP5 leader
T5-2	Support on developed components - no activities
WP8	**Guidelines for Security & Homologation**
T8-1	Scope of the homologation process - helped in defining the scope
T8-2	Stating of the Security requirements - gave input for this topic

2.11.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP4/T4-1	M4	D4.1 « Architectural Specification »	Final
WP4/T4-2	M8	D4.2 « Specification of External Interfaces »	Final
WP4/T4-3	M8	D4.3 « Internal functional specification »	Final

2.12 ON-X

2.12.1 Technical work accomplished this period

WP/ Task	Actions
WP3	Requirements
T3-1	Requirements Analysis - Participation to the "brain-storming meeting" &Contribution of comments to the initial report
T3-2	Definition of the project perimeter and requirements - Participation to the Munich meeting &Contribution of comments to the report
WP6	**Integration**
T6-1	Technical Integration Coordination /Architectural Framework Implementation - Coordination of the integration WP activities
T6-2	Preparatory activities : - Initial report (progress report one) - Elaboration of a set of documents (integration guidelines and procedure) - Analysis and initial specifications of the technical tools required

2.12.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP6/T6-1	M6	D6.1 « Initial integration report »	Final
WP6/T6-1		R6.1 « Integration process overview »	Draft
WP6/T6-1		R6.2 « Integration guidelines and acceptance procedures »	Draft

2.13 EADS-TELECOM

2.13.1 Technical work accomplished this period

WP/ Task	Actions
WP6	**Integration**
T6-1	Technical Integration Coordination /Architectural Framework Implementation
T6-2	Launching of the first studies : • Writing of the procedure for the Open Source contributions reception • Inventory of potential software that can be integrated to the project

2.13.2 Deliverables due this period

WP/ Task	Due	Deliverable	Status (Final, Draft, Pending)
WP6/T6-1	M6	D6.1 « Initial integration report »	Final
WP6/T6-1		R6.1 « Integration process overview »	Draft
WP6/T6-1		R6.2 « Integration guidelines and acceptance procedures »	Draft

3 Technical quality management

3.1 Overview

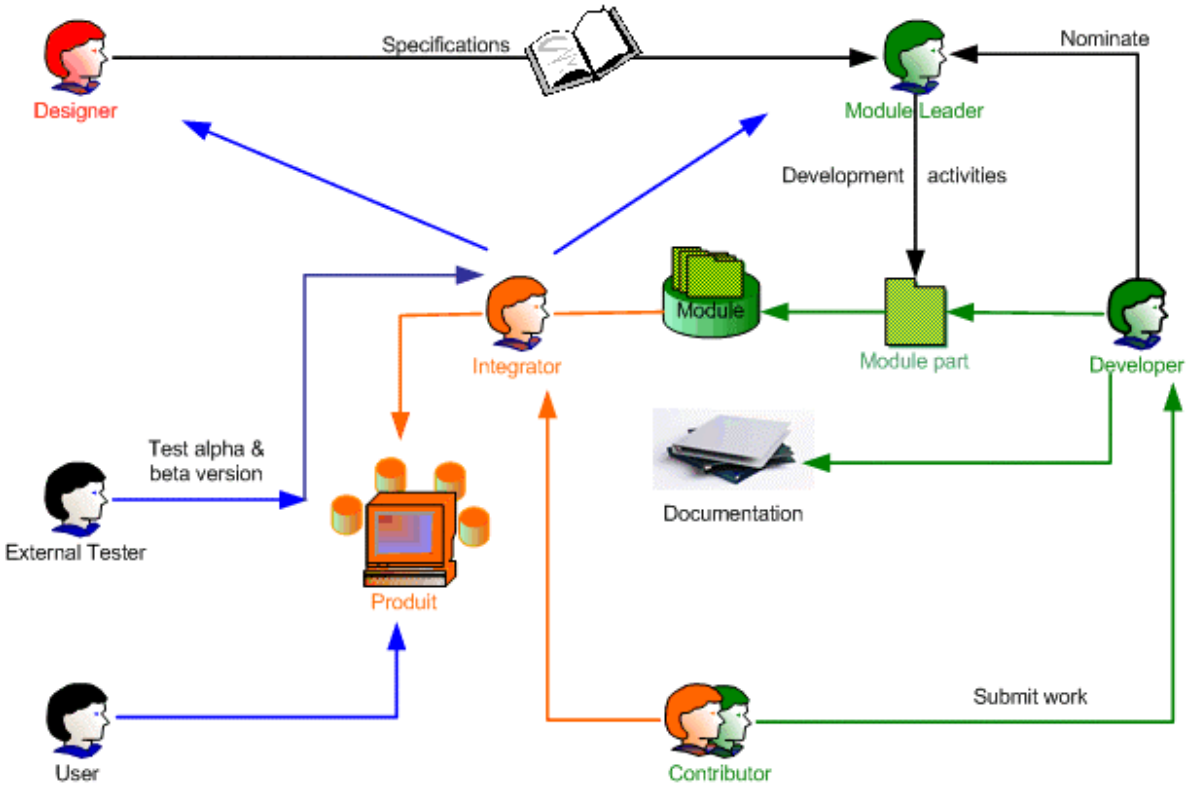
The purpose of this paragraph is to make available an overview of the development and integration process and, also, acceptance control for PKI modules that has been taken in place in order to assure the quality of these modules.
WP5 and WP6 have well defined all these procedures and a summarize is shown in this document.

3.2 Actors Interactions

EUPKI identified seven actor profiles (and major related WP):

- Designer (WP4) : Designers specify at the overall project level the complex work-flows and functions. They have to translate the functions coming from the requirements (a functional specification) into lower level specifications.
- Integrator (WP6) : Integrators consolidate developers and external contributions so as to produce a functional product for publication and testing.
- Module Leader (WP5) : The module leader is a developer who is in charge of development activities around one particular module. Module leader is a member of WP5 and is nominated by developers.
- Developer (WP5) : The developer is in charge of implementing what have been specified. He is a member of the consortium and has write access to the source code repository. In the future, valuable contributors may become developers upon Steering Committee agreement.
- Contributor : Contributors are external persons who may furnish bug fixes (patches) or a complete function implementation; they may also participate to integration work or document redaction. They are trained to EUPKI development process by the Module Leader (development contributor) or WP6 leader (integration contributors). Contributors must follow EUPKI procedures and constraints.
- Tester (WP7) : Testers are the persons who test alpha and beta versions.
- User (WP3) : Users are the persons who use the products of the Project. They are typically system integrators or PKI Service Providers. WP3 members fall into this category but we hope EUPKI will have of a lot of external users.

The following diagram resumes the essential interactions between project actors in an iterative development process.



Designers give the initial specification of the product to developers and provide assistance all along the product development lifetime. They are responsible for:

- Initial specifications of the initial release,
- Enhancement requests analysis and specifications
- Global complex workflows and functions specification
- Global Software architecture

The Technical Board must validate all specifications

Module leaders are the interface (contact point) between development and integration and as such responsible for the compliance with the related rules (once approved at project level). They manage development work:

- Developer planning,
- Call for contributions and contributors management,
- Converting specifications into development activities,
- Writing development procedures and coding rules and make sure they are applied.

All Module leaders should agree on general coding rules and development procedures. They are under the responsibility of the WP5 leader. The Technical board must validate all procedures and conventions.

Developers are responsible for:

- Implementation of parts attributed by the Module Leader,
- User Documentation,

- EAL furniture,
- Install Documentation,
- Verification and commit of work received from contributors

Actually, WP5 implements base API (Log, DB, …), modules, blocks, SQL scripts to put up DB structure after installation, unit tests programs for modules and produces the Initial documentation.

Integrators are responsible for putting together developers' source code, external contributions and documentation to validate through a first set of global tests the consistency of the components and to produce a complete package ready for external publications and external testing.

Integrators are responsible for :

- Verification of compliance with quality requirements,
- Enhancement requests, reception and qualification,
- Problem reports, reception and qualification (They analyze and try to reproduce the problem),
- Sending their analysis to the module leader who is in charge to fix it.

Users may report bugs or make enhancement proposals. They download official releases of the project from the public web site.

External testers have the same responsibilities as users in testing the product but a deeper analysis is expected from them, particularly for security requirements. They must ensure that the deliverables meet the user and security requirements. They download intermediate releases from the private web site.

3.3 Development global process

At the beginning of the development phase, WP5 produces two new technical documents :

- "Uses Case" which describes the technical specifications allowing the implementation in Java of EuPKI, according to the WP4 documents. This document is technology dependent and thus has to be used as a complement of WP4 documents (which are independent of the programming language),
- "Architecture, Design & Implementation" which describes the chosen technologies to implement the EU-PKI project and the concrete implementation of EU-PKI modules using those technologies

The development process is divided in three main successive efforts that highlight the need for an organization pattern starting from scratch, as no code except the standard libraries and APIs are currently available.

3.3.1 Phase 1 – General structure, common ground and a skeleton implementation

Following the technological decisions phase, actual implementation and code writing begins with phase one. This phase is meant to define a clear and intuitive structure for the different modules and parts of the project, by clearly separating and identifying inter-module relations, code reusability and common bases.

Another objective is the development of the common core of the project. The common core is delimited by the critical code mass is the absence of which, no other code can be deemed reliable. Generally speaking, the common core is made up of those elements that are completely independent of the other modules, but stand out to form the base on which further application logic will be developed. Memory management, file access, IPC, abstraction layers are examples of blocks contained by the common core. No project of a non negligible scale should ignore this first development phase, especially a security targeted one.

Careful planning and implementation of future needs into these common blocks is an imperative necessity, and should take all the time needed to guarantee further non-regressive development afterwards.

Finally, this phase will permit WP6 to start its integration work, by delivering a functional skeleton configuration, based on a functional version of the common core, and implementing most of the modules that build up the CA, RA and the User KGS. This means the skeleton's sole purpose will be to grant WP6 the possibility to start building specific integration tools, platform related frameworks, and possible test cases. Performance tests, benchmarks, compliance tests and the like are out of the question.

As part of this phase, it should also be stated that certain blocks of the common core are only partially required by the skeleton, and that the skeleton will be delivered without the final completion of these blocks. Communications, log and access control are components of the common core. Audit and database abstraction layers for instance are only partially integrated into the core and are not going to be bound to the skeleton.

3.3.2 Phase 2 – Module implementation

The main development efforts are due to be dedicated to this phase. The whole module list is separated into several development threads, prioritized, and actual implementation starts in parallel. Module delivery can be scheduled accurately enough so that integration work can proceed in tandem.

The general idea is to "fill in" the skeleton with the real module implementations, based on the common core, and not braking consistency. Not braking consistency means organizing and rearranging development tasks within the development team as to not impede the integration team to do its work. Basically it means having a functional "head" at all times.

As modules are released, they are clearly stated as such, and so QA tests may start providing feedback. Intermediary versions are open to debate; the source code will at least be available to the whole consortium so direct input from the partners is clearly a development boost.

The logical bricks of this phase are, of course, the external entities that make up the product (CA, BO, KGS, etc.). As parallel development threads are to be sustained, care will be taken as to favor critically functional parts over non-critical ones, guaranteeing that integration efforts can have a constant functional workload. Disruptions or deviations from this scheme will clearly and timely be handled between WP5 and WP6 so that preferably no overhead is imposed to either party.

This phase will be officially over when no further issues remain to be solved or implemented with regard to individual modules' specifications. No general architecture or module interaction specifications are directly handled in this phase.

3.3.3 Phase 3 – Wrap up & Final touches

Depending on the attention paid to the "not so obvious" interaction and general architecture aspects of the logical bricks in the second phase, this final part will vary in time, with minimal consequences though on the final delivery. Time spent here can probably be considered negligible compared to the first and second phases, as heavy work will have been 99% completed.

Work done here guarantees that the final product is "a whole". Details like fine tuning of the interaction between modules, revision of the error handling routines, exception handling, UI design analysis, fault tolerance, aesthetics and probably a security overhaul constitute the main tasks of this phase. Work largely depends on leftovers from the previous phases but importance is greatly diminished compared to the whole development effort.

This final part is almost exclusively a developer duty and the impact on integration is minimal. Changes that can influence integration decisions are discarded or carefully discussed with WP6 so that no more decisive measures are acted upon in this phase.

No mistake should be made in judging this phase though. This last investment can have dramatic consequences on the impact of the final result on the market, as it has been proved time and time again by established commercial actors. This very last energy consumer is so often ignored or forgotten in the open source community it's become a de facto. It is this very last thing that can make the first difference in the global arena.

3.3.4 Coding standards

Generally accepted coding standards will follow the Sun specifications for the Java language. A detailed document explaining all the aspects of these standards can be consulted online at

http://java.sun.com/docs/codeconv/html/CodeConvTOC.doc.html.

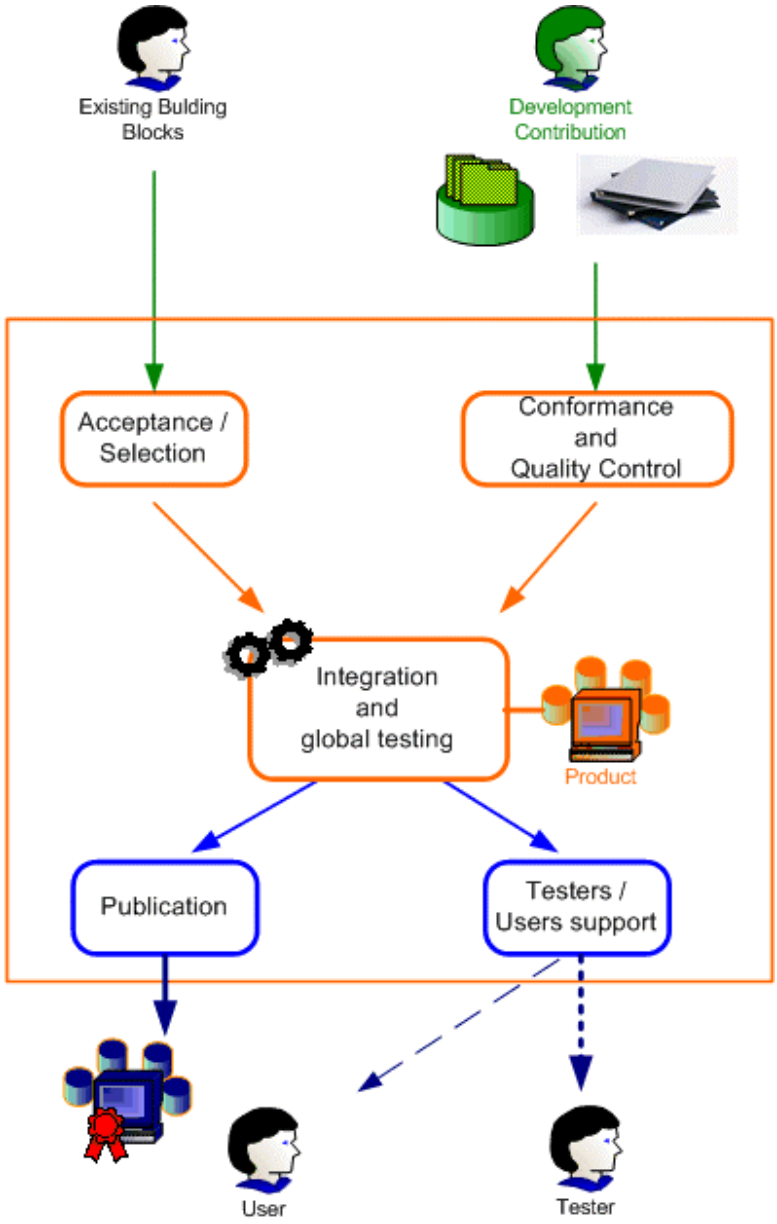
These specifications should be regarded as compulsory for code acceptance and general contributions to the project from the consortium as well as external.

They will be imposed in order to reduce to a minimum the number of maintenance problems that may be encountered as a consequence of the lack of such guidelines, and to provide for an easy integration between developers of our team and external ones as the majority of Java developers are at the very least remotely familiar with these specs.

3.4 Integration global process

The process described in this paragraph applies to the first step in EUPKI product elaboration: Industrial and quality oriented production. These constraints are necessary due to the important effort produced by every partner of the consortium. Once this first step is achieved, the project steps into its genuine Open Source nature (the second step: "evolution: fixes and enhancements" - EFE)

The global approach proposed for EUPKI's production is:
Requirements => design/specifications => development => integration => tests.



WP6 receive contributions from development or exterior. It checks their quality (acceptance procedure and selection of external contribution) and conformance to specifications, particularly based on unitary testing done by WP5. Then WP6 integrates them and performs global testing of the integrated product. When users requirements are estimated completed, WP6 publish a "stable" version of the product. WP6 is also responsible for the support for external users and external testers of the product.
In order to perform integration, WP6 can use "Existing Building Blocks" (e.g. libraries such as BouncyCastle) and tools (e.g. Apache web server).
Development contribution concerns blocks of developed modules (conform to specifications) and related documentation.

The "Industrial" step is split into three phases:

- The Design phase specifies requirements and functionalities for EUPKI.
- The Initial Production phase produces EUPKI beta version
- The Validation and Testing phase ensures EUPKI is ready to step to Open Source phase

3.5 Quality Procedures for Development contributions

Development contributions consist in software realizations made for the EUPKI project. Typically, these contributions are realized by WP5 but may also be developed by external contributors provided that they commit to respect the following procedures.

3.5.1 Acceptance Procedure

Acceptance procedure is divided in two steps:

- Conformance control
- Quality Control

3.5.1.1 Conformance Control

When a development delivery is submitted to WP6, previous to start the integration, a Conformance Control procedure is performed.
These controls lead to the integration phase of the package or the emission of a refusal note explaining the reasons.

This procedure is formal and only consists in examining the delivery.

If the delivery passes this procedure, the Quality Control Procedure is applied. Otherwise an Acceptance report is sent to WP5 stating the reason of rejection or the modifications made.

3.5.1.2 Quality Control

As for skeleton deliveries, the checks concern:

- API conformance to specifications
- Makefiles and dependencies (make on a Block directory compile and link with all modules and external contributions).

Regarding prototype and complete deliveries, checks verify:

- Satisfaction of the user requirements
- Satisfaction of the security requirements (CC)
- Satisfaction of the coding rules
- Completeness of documentation
- Unit test plan

After an Acceptance procedure has been completed, WP6 may decide to publish the source code in the Public CVS repository. This allows external actors to follow the EUPKI project progression before the publication of validated beta distributions.

3.5.2 Integration procedure

The integration procedure is split in two phases:

- Integration (develop necessary components and make a build)
- Functional tests: test the distribution

If the integration phase or testing phase is not successful, an Integration report is sent to WP5 explaining the problems or defaults met for correction.

An integration procedure always ends up by the redaction of an Integration report. If this procedure is successful, the Integration report will help testers in their work.

4 Technical issues

4.1 Issues encountered during this period and solutions

4.1.1 Delay in the D.3.6 final validation

The final review Meeting of D.3.6 and WP3 was held in Munich the 4th of July 2002.
It led to admit that the D.3.6: "Project Perimeter and Requirements" was not enough completed to allow a functional scope for the WP4 work. Many suggestions of modifications and improvements of the document have been made by the members so that the D.3.6 becomes more complete.
Consequently, initially planned for mid-July, the date of official delivery for validation of this document was prorogated to the end of September.
The Commission was formally informed during the meeting organized with the Project's Managers the 1st of August 2002.
However, the work hand-in-hand with WP4 has allowed to avoid any latency in the WP4 deadlines since the D.4.1 document elaboration lied on already stated information in the D.3.6 draft. The collaboration of both Work Packages has fulfilled the project's requirements.
All these documents don't speak enough about the legal aspect of PKI deployment. It is necessary to complete the last version of the delivery D.3.6 with an overview of this issue.

4.1.2 Choice of programming language

The last technical meeting had to do the choice of programming language between JAVA and C/C++. To do it, 4 topics were taken into account :

- Developers preference and risks for the project
- Compatibility with the users applications
- Differentiation with the others solutions on the market
- Specific interest of each partners

4.1.2.1 Developers preference and risks for the project

WP5 would like to develop in Java because its developers are more efficient with this language and more confident in the schedule defined into the project.

4.1.2.2 Compatibility with the users applications

This point is the big issue of this choice. It is evident that the C/C++ solution will be compatible with the applications which would like to integrate PKI modules and, perhaps, it is not the case for a Java solution (or it would be more complex). As it is very easy to integrate C/C++ modules into Java application, it could be difficult to integrate Java modules into C/C++ application.

4.1.2.3 Differentiation with the others solutions on the market

The Open-Source PKI solution available on the market are programming C/C++. If EUPKI solution integrates Java components, it could be a real differentiation on the PKI market.

4.1.2.4 Specific interest of each partners

Each partner has its own strategy about PKI market (for example, some have still a solution with C/C++ modules and want an other one with Java).

4.1.2.5 The choice

The choice was Java :

- Vote for C/C++ : two (EADS, Actimage)
- Vote for Java : six (G&D, GIP MDS, Certinomis, CGE&Y, On-X, Axetel)
- Abstention : one (AQL)

The consequence of this choice was the change of crypto library : moving from OpenSSL to BouncyCastle.

4.1.3 Planning of the PKI modules delivery

During the third Technical Board on November 28, WP5 explains that they need to produce detailed conception (D5.4) before the development of PKI modules and, as there are no source code contributors, except Axetel, from consortium, WP5 is obliged to develop more PKI modules than it expected. The consequence is first a delay of one month for PKI modules deliveries to WP6 but also, and it is the most important, a major change of the assumptions of the project (the European commission agrees about this change). The Technical board is awarded that there is a risk of delay for the project.

In order to begin the integration phase as soon as possible, WP6 would like to have :

- At first, a skeleton integrating all the APIs,
- After, a monthly PKI modules delivery

The principle has been accepted and a new schedule was proposed and approved by WP5 :

- Second Technical Board :
  - About technical documents :
    - Agreement of the WP3 deliverable D.3.6
    - Agreement of the WP4 deliverable D.4.1
    - Agreement of the WP8 deliverable D.8.1
- Short time schedule (till end of February 2003) :
  - Preparation of D5.4 :
    - Draft version V0.1 and detailed delivery planning : 20/12/02
    - Comments by Technical Board : 05/01/03
    - Draft version v0.2 : 10/01/03
    - Comments by Technical Board : 12/01/03
    - Final review meeting : 13/01 in Bucharest

        - (virtual) Technical Board (+ virtual SB if necessary) : 21/01/03
    - First deliveries :
        - Skeleton : 15/02/03
        - First complete modules (minimum two modules defined by WP5 on 20/12) : 15/02/03
- Mid-time schedule (February till summer 2003) :
    - Monthly milestones : to be defined by WP5 for 20/12/02
    - Deliveries from WP5 for a « workable » version for two scenarios : by end of July 2003
    - Deliveries from WP5 enough for « demonstrations » for two scenarios (Banking scenario, On-line scenario) : by end of August 2003

4.2 Eupki review meeting

A first review meeting occurred in December , 2002.After the meeting, the experts made a series of recommendations. The minutes will be distributed to the consortium.

4.3 Action plans for the continuation of the project

Next Technical Board will occur on the 21st of January. The goal is to :

- do an agreement about the document Wp5 R5.x documents (use case, architecture, planning)
- analyze the planning of the delivery from WP5
- finalize the WP5 action plan and deadlines for the delivery of the modules in accordance with WP6.

The technical board is careful of the WP5 activity (planning, quality of deliveries, ..) because there is a risk of delay for the project.

5 Conclusions

This first period of the EuPKI project has led to walk through several steps. Our technical achievements do not fail our objectives and our goal has not stopped to be more and more precise.

The EUPKI Technical Board does not put in evidence any important issue but is careful of the next steps; in particular source code development. The quality process is now well defined and we can enter into the production phase (development and integration) with a very good quality of documentation (requirement (WP3 has to complete its document by a study of the legal aspect for PKI deployment), specification, security functions definition).

The main issue is the lack of open source PKI modules which are available. WP5 is obliged to develop more than it was planned to do at the beginning of the project. The consequence is a risk of delay for the project.

The actors of that project are particularly involved and motivated. Their different profiles and skills are but a considerable asset to take advantage of their complementarily. One very important tool for the project continuation will be for sure the efficiency of the collaborative work, so that, hand-in-hand, each member can bring his expertise to finally deliver one major security solution in Europe.