Open Smart Card Infrastructure for Europe

v2

Volume 4: **Public Electronic Identity, Electronic Signature and PKI**

Part 4: **A pre-inventory of smart card based PKI projects within the EU**

Authors: **eESC TB2 Identification and Authentication**

*e*Europe
Smart Card Charter
Trailblazer 2 on Identification and Authentication

A pre-inventory of smart card based PKI projects within the EU

Version 1.3
February 2002

Andreas Mitrakas
Laurent Blivet
Moise Moyal

Contact information

Dr. Andreas Mitrakas
Chair eE SCC TB2
GlobalSign
Haachtsesteenweg 1426

1130 Brussels
Belgium
andreas.mitrakas@globalsign.net
www.globalsign.net

Laurent Blivet

DICTAO
42, avenue de la Grande Armée
75017 Paris
France
lblivet@dictao.com
www.dictao.com

Moise Moyal

Oberthur Advise
12bis, rue des Pavillons

92804 Puteaux Cedex,
France
m.moyal@oberthurcs.com
www.oberthur-advise.com

Abstract

This pre-inventory addresses certain aspects of smart card based Public Key Infrastructure (PKI) deployments in Europe. Focusing on real-life projects from EU member states, this Pre-inventory highlights organisational, technical and business aspects that are important in PKI deployments in large populations. While scale helps the success of PKI and smart cards, there are still certain grey areas and shortcomings in the planning and implementation phases that may threaten the success of such projects. Recommendations are proposed for additional improvements required to ensure that such deployments meet end-user expectations for cost efficient, interoperable applications in line with legal requirements and standards.

Table of Contents

Background

While the European Commission has proposed the *e*Europe initiative with a view to accelerating the transition of the economy to the digital age, an important part of this initiative, *e*Europe Smart Card Charter (*e*E SCC) aims at stimulating the acceptance and deployment of smart cards across Europe. Within the *e*Europe initiative the Smart Card Charter seeks to underpin the issues to resolve before smart cards can be exploited fully to support the expectations of citizens with respect to ICT. The action plan addresses both the needs of citizens and the business community alike in terms of business cases, multi-functionality and interoperability of systems and infrastructure, and the provision of trust in all aspects of service delivery.

This report is a pre-inventory of present day smart card based PKI projects in the European Union. A pre-inventory has the meaning of a concise coordinated action that provides a snapshot rather than a deep analysis on the matter at hand. This pre-inventory provides the basis for further action, input and in-depth analysis for parties that are interested in further exploiting this possibility. This Pre-inventory has been drafted in the framework of *e*Europe, Smart Card Charter, Trailblazer 2 on Identification and Authentication. The objective of Trailblazer 2 (TB2) within the eE SCC is to contribute, by the end of 2002, to a common, workable and affordable security platform for all electronic transactions in need of identification, authentication and electronic signature in Europe. The work of *e*E SCC TB2 is based on PKI and smart cards.

This Pre-inventory has been carried out with the support of the European Electronic Signatures Standardisation Initiative (EESSI) Steering Group under the ICT Standards Board. In promulgating standards for electronic signatures in Europe the EESSI SG has demonstrated considerable interest in the field that crosses PKI and smart cards. This pre-inventory is intended to provide further insight to the EESSI objectives. The work plan of EESSI focuses on electronic signatures pursuant to the Directive to Council and Parliament 99/93/EC *on a Community framework for electronic signatures*. The EESSI deliverables are widely acknowledged for being generic, flexible and applicable in a multitude of transactions. EESSI deliverables, however, can be further extended to reflect the specific needs of industry and governments.

This Pre-inventory has also received the support of Member States represented at the Telematics for Administrations Committee (TAC) of the IDA program. IDA TAC has provided valuable references for cases examined in this pre-inventory. As the aim of IDA is to issue "Interoperability Guidelines for Smart Cards in Public Administrations" this pre-inventory can also be seen as a step towards that objective.

Public Key Infrastructure (PKI) has widely been seen as an appropriate technology to address the requirements of the Directive 99/93 on electronic signatures as well as the needs of the users of open networks. Standardisation work on electronic signatures currently under way underscores the precedence of PKI with regard to alternative technologies.

Smart cards have also been used as a fail-safe medium to provide access to a wide number of services through diverse technology platforms. Electronic commerce as well as mobile commerce applications make or foresee the usage of smart cards while emerging national identification schemes support the usage of smart cards.

To deliver this Pre-inventory the expert team has been in contact with all parties identified in this Pre-inventory, including, *e*E SCC Co Chairs and SC, EESSI SG, IDA-TAC, CEN/ISSS, the TB2 constituency and the parties interviewed as appropriate.

Abbreviations

CA: Certification Authority
CEN/ISSS: European Standards committee/ Information Society Standardization System
CP: Certificate Policy
CPS: Certification Practice Statement
CSP: Certification Service Provider
CRL: Certificate Revocation List
*e*E: eEurope
EESSI: European Electronic Signature Standardisation Initiative
ETSI: European Telecommunications Standards Institute
ICT: Information and Communication Technologies
IDA: Interchange of Data between Administrations
IDA-TAC: IDA-Telematics for Administrations Committee
OCSP: Online Checking Status Protocol
PIN: Pin Identification Number
PKCS: Public Key Cryptographic Systems
PKI: Public Key Infrastructure
RA: Registration Authority
SCC: Smart Card Charter
SSCD: Secure Signature Creation Device

1.0 Introduction

The emergence of widely deployed electronic services, Public key Infrastructure (PKI) and smart cards technologies have increased in importance across Europe in recent years. This Pre-inventory suggests that while the combination of PKI and smart cards is an appealing combination and an appropriate means to address the requirements for identification and authentication in multiple application areas the ongoing process regarding the employed business model and selected standards may undermine the implementation and limit the results of such projects. Initiatives in the public and private sectors have also been driven by a legal framework that has gradually been put together in the last few years. Industry and standardization bodies have been playing an important role through a number of standardisation initiatives including the European Electronic Signature Standardisation Initiative (EESSI). However as this inventory underscores to date only a limited number of real-life operational projects in Europe can flawlessly combine PKI and smart cards. This survey reveals some of the shortcomings and difficulties that are associated with the deployment of smart card based PKI projects that include technical issues, organizational complexities and often the lack of demand for such services.

To date the more evolved projects combining PKI and smart cards are typically run through public sector initiatives associated with public identity and social security. In the private domain, banking has been an early starter in implementing smart card based PKIs and applications. This large-scale approach relates to the cost and time length of such projects, that can mostly be sustained by such large organizations. Smart card based citizen identity cards emerge as a major targeted area in this field. Smart cards have become a major vehicle for electronic identity cards as a secure network key for all on-line services, which require the identification of a natural person, in public and private sector services. In the countries that have launched an electronic identity card, like Sweden and Finland, for example the deployment of projects based on smart cards and PKI has been easier than in other European member states. Sometimes as a complement to the identity card other services are also supplied by means of the same smart card (e.g. health, vote, social security etc.). Local services are also applied in several ways depending on city or regional needs and requirements (e.g. transport, education etc.).

The remainder of this report addresses certain organisational, technical and legal aspects associated with the deployment of large scale PKIs.

2.0 Methodology and selection criteria

This survey was carried in July and August 2001. In support of this survey a questionnaire was used to collect information from the project managers. Additional publicly available sources were also used together with the interview material such as existing documentation, studies and material previously gathered in another context e.g. [TB1 02], [CEN/ISSS 02]. As there are currently several examples of smart card based PKI deployments in Europe, this Pre-inventory does not express any opinion or preference on the quality or any other aspect of these sample projects included in the survey.

The goal of this survey has been to provide an in-depth understanding of the level of activity associated with such technologies in Europe. As this survey has been styled Pre-inventory, it anticipates that more empirical research will emerge in this area in an effort to evaluate current projects and receive feedback from experience gathered. In this context this Pre-inventory has the meaning of a concise coordinated action that provides a snapshot rather than a deep analysis on the subject matter.

The objective of the selection has been to identify a limited number of projects that can be analysed in detail. To establish this list the following criteria were used in order to maximize the quality of the information gathered:

- Level of maturity of the project (plans to deploy, on-going pilot, deployment phase) with a clear interest for project at an advanced deployment phase, where smart cards carrying digital certificate are already in use.
- Size of the project (e.g. number of cards, certificates deployed etc.), since large projects are more likely to have conducted an in-depth technical analysis and generally encounter increased organizational complexity.
- Geographic and sector scope to support a balanced approach of examined projects in term of scope and application.
- Availability of the project manager, confidentiality issues and willingness to share information with the project team.

One essential aspect of this survey has been to highlight the influence of the deliverables of EESSI in real life applications. The work plan of EESSI focuses on electronic signatures pursuant to the Directive 99/93 *on a Community framework for electronic signatures*. The EESSI deliverables have been worked out by two of the recognisedn standardization organizations: European Committee for Standardization/Information Society Standardization System (CEN/ISSS) and the European Telecommunications Standards Institute (ETSI). Since 1999 EESSI has implemented a work programme that has yielded considerable results in specifying requirements for the large-scale deployment of electronic signatures pursuant to the European Directive 99/93 on electronic signatures including legal recognition for digital signatures under [EESSI 01]:

- The general principle of article 5.2 of 99/93 to give legal effect for all electronic signatures with planned deliverables that include the draft Certificate Policy for 5.1 type signatures;
- Under the second principle of article 5.1 of 99/93 on certain electronic signatures that receive the same legal effect as hand-written signatures that include the deliverable regarding the Qualified Certificate Policy [ETSI 01].

While most of the project address aspects of the generic category under article 5.2 of the Directive some them have already plans to issue qualified certificates in the meaning of article 5.1 of 99/93.

3.0 Projects Selected

The list of the projects analysed and their category features includes the ones below:

Project Name	Project description	Category	Status	Country
ABN Amro - Identrus	B2B authentication, digital signing, payment and trade facilitation	Private sector initiative	Fully deployed	Global
AdeP	Multi-usage citizen card	Identity card	Project stage	France
Finnish Citizen Identity card	Electronic citizen identity card	Identity card	Deployed	Finland
French Notaries	Authentication and digital signing for documentation exchange between notaries	Professional association initiative	Deployed	France
GIP-CPS	Authentication and digital signing in healthcare	Healthcare and social security	Deployed	France
Italian Citizen Identity card	Electronic citizen identity card	Identity card	Pilot project	Italy
PKI Overheid	Multipurpose identity solution	Multipurpose	Project stage	Netherlands
Posten AB	Multipurpose citizen identity card	Identity card	Deployed	Sweden
Satakunta	Social Security application based on the Finnish identity card	Healthcare and social security	Pilot project	Finland
Social security and Communidad Valenciana public services	Public identity	Healthcare and social security	Project stage	Spain
TEKES	Social Security application based on the Finnish identity card	Healthcare and social security	Deployed	Finland

The projects under study mostly focus on governmental applications or have been led by large-scale private initiatives. They all target, however, large populations that are projected to run into millions of users.

Solving the economic equation in a way that ensures appropriate funding is an aspect that has been underlined for its criticality. The cost of these projects has often been quoted as a significant barrier. The business cases appear to be varying among the different projects and encompass a wide range of approaches:

- Fully publicly funded projects mostly in case of general purpose, compulsory and national identity cards.
- Cards and certificate sold to end-user, usually bundled with an application.

4.0 Project Analysis

The analysis of this inventory follows the lines of organizational, technical and legal aspects, as these are the major considerations in electronic commerce projects [Lei et al. 96].

4.1 Business and Organizational Aspects

To provide an overall picture of the considerations in a project the business and organizational features were addressed along the following major guidelines:

- Business model: cost per user, return of investment etc.
- Project deployment: current status, roadmap, size of the project.
- Significant problems encountered: technical, political, legal.
- Processes: registration, certification, personalization.

4.1.1 Project deployment and business model highlights

The projects under consideration all have diverse evolution stages to demonstrate. The main stages of evolution include project analysis, prototype, and ongoing pilot to fully operational. The projects have been classified according to parameters such as current status roadmap, deployment status and size. A wide range of business models has been employed for smart card based PKI implementations. These projects all feature diverse maturity levels with regard to the business model adopted that range from per transaction charging to the end user covering the full costs. This divergence is possibly due to the phase of deployment of smart card based PKI projects in general as well as the varying business objectives that have to be addressed in each individual project.

The surveyed **ABN AMRO - Identrus** project started in 1999. To date more than fifty financial institutions have joined this banking accreditation scheme as accredited Certificate Authorities. These financial institutions now represent more than 133 countries and millions of business relationships. The basic business model of this project involves Payment by transaction slots, fixed on the basis of corporate customers. This model makes available electronic signatures on smart cards and signature verification for applications. For this scheme the challenge has been to deploy a global business and legal framework that also features a technologically neutral solution with interoperable electronic signature capability.

With 500 smart cards issued, the multi functional **AdeP** identity card is currently at its prototyping test phase. Large-scale deployment has been planned for end 2001-2002, targeting French citizens, corporate users, the public administration and local communities. Projections are based on the number of the local communities. It is foreseen that by the year 2005 there will be 3000 smart cards in the market. In its conceptual phase this project has become the reference project in France related to Electronic Signature law issues for certified electronic procedures.

The business model for this multi-functional identity card is based on payment for each act of an electronic procedure that is certified and secured through the smart card. At this initial stage this project is funded through government sources.

The **Citizen identity card project in Finland** is in production with approximately 9500 electronic identity cards issued already. The target number is the entire Finnish population. The project has not reached its deployment goal and the number of cards issued remains low.

This Citizen identity card project bases its business model on the delivery of an electronic identity card to every citizen that requests it on a voluntary basis. Each electronic identity card is personalised and includes two certificates. Accessing the directory and the certificate revocation services remains free of charge. While a list of recommended card readers is published the Population Register Centre develops products using the electronic identity card together with software vendors. While the bare smart card with the certificate costs some €27 the whole package complete with software and a card reader costs about €100.

On the downside, the protracted standardization process is seen as an inhibiting factor. National legislation that was still under consideration in mid summer 2001 and the absence of appropriate electronic services for citizens also hampers the deployment of the system.

The project of the **French Notaries** went into production in 1999. The target audience is the notaries and their employees. To date some 3500 cards and electronic signature packages have been deployed. The target has been set to 22000 cards. The technical goal has been reached, but the number of transactions still remains weak. The project has gathered publicity in France with regard to Electronic Signature and smart cards. Future deployments are currently under examination, addressing the needs of corporate users in need of of notary services. The cost sale is about €150 for the electronic signature package including a smart card reader and a card reader software. The smart card and the certificates are free of charge.

The French notaries' system experiences low usage rates (between 5-10%) for the on line transactions it offers. The remainder is still based on snail mail. There is no interoperability with other PKI systems. The deployment of the smart card reader is also an inhibiting factor, as it has to be delivered separately from the personal computer. The deployment of this system is also limited by the lack of related education and training available for the end-users, the majority of whom are notaries.

With 350 thousand cards issued in October 2001 the GIP-CPS project in France is already in the production phase. The target, however, is 1 million cards deployed in 3 to 5 years. The cost per user of the card and the associated services are under €30. The card is free of charge. In the short term, the return on investment cannot be evaluated. In the long run though, the challenge is to develop a coherent and secure IT system in the healthcare sector. The return on investment will have to include all the contribution in the spreading of the health applications (on line refund forms, secure health care networks etc.).

The **GIP-CPS** project has encountered organisational problems associated with its large stakeholder basis, currently more than 20, from public services. Additional problems relate to the education, information and training of the health professionals involved.

The surveyed project for a **Citizen identity card in Italy** started in 2001 and in the pilot phase has reached a volume of 100 thousand cards. Projections foresee that by the year 2005, 8 million cards will be made available. This project, however, has encountered delays due to non-specified technical problems. At the time of the survey the business model for this project had been under government investigation.

The project of **PKI Overheid** is a multi functional solution in the Netherlands that has already reached the stage of public consultation of requirements with several pilots currently underway. The deployment roadmap foresees large-scale rollouts in the years 2003 through to 2005 when it has been projected to deploy some 20 million active smart cards. The business model, however, has still to be developed and the cost per user to be taken into consideration.

The limited availability of interoperability standards and interoperable application products inhibits the wide deployment of this solution. Such a shortcoming is also related to the European Directive for electronic signatures. Electronic identities only form a small part of electronic services. The real challenge for organizations is the large-scale process redesign before electronic identities can be used.

While the **Posten AB identity card project** in Sweden has already rolled out 50 thousand cards the full deployment stage targets the entire population in Sweden. This project began in 1996 and has shifted its goals to include on line services as this project also involves the promotion of software and smart card based solutions. The smart card solutions are sold with a card reader and the card is personalised with the user certificates. Typical cost per card is about €53 to €63 including a personalised smart card and a card reader for a certificate validity period of 5 years. Software certificates come at about €33 to €42 and the certificates are valid for 2 years. The directory and revocation services are free of charge. Profits are projected in 2 years. A down side is that some applications have not integrated the required PKI system interface and software as yet.

The **Satakunta project in Finland** targets 10 thousand professionals and 1000 citizens for its smart card based services. The Finnish Government through the Population Register Centre of Finland issues the cards. The project goal has been to produce the card, develop the distribution project and distribute the cards to the users. The fixed fee for the card has been set to €50 and it is the same rate for professionals and citizens. A local distributor has been selected for the project. On the downside, the application to update personal information on the card and the application for authentication and authorization have encountered technical problems.

In the project of **Social security and Communidad Valenciana** public services the analysis stage has already been accomplished. The pilot project has been foreseen for June 2002. Full deployment foresees 5 million cards deployed by 2003. The cost per card is €12, half of which is paid by the citizens who are the end users.

The Finnish social security project, TEKES, made available its first operational software version in the beginning of summer 2001. The smart cards are issued through the Population Register Centre, a government agency. The Finnish social security project provides the software and charges an annual maintenance fee. The

smart card distribution is not included in the business model as the requirement is for an electronic identity card to have been issued by the Finnish Population Register.

4.1.2 Significant issues

All business models in the selected projects have encountered some sort of problem. As projected revenue may be unable to sustain the viability of the projects, potential alternative revenue sources such as using the smart cards as platforms for additional applications have to be considered. For most projects, however, the return on investment is projected for the long term with no immediate returns in sight. Areas of potential improvement appear to be:

- The increased number of transactions made by smart card user.
- The increasing number of applications that use PKI as an underlying security layer.

Additional information on the projects analysed can be found in the table below:

Project name	Deployment status
ABN Amro – Identrus	▪ 1999: Identrus LCC founded in 1999 by ABN AMRO, Bank of America,Bankers Trust (since acquired by Deutsche Bank), Barclays, Chase Manhattan, Citigroup, Deutsche Bank and Hypo Vereinsbank ▪ 2000: ABN AMRO fourth bank to become Certificate Authority ▪ 2001: Fifty plus financial institutions have joined the Identrus system as Identrus Certificate Authorities. These financial institutions now represent more than 133 countries and millions of business relationships. ▪ 2001: Microsoft support for Identrus Trust system. Microsoft will directly support Identrus trust services in its Windows XP operating system, .NET Enterprise Server, and its Outlook 2002 email client ▪ 2001: European commission provides regulatory approval for Identrus LCC ▪ 2002: Project Eleanor E-Payments which will offer B2B payment and trade facilitation
AdeP	▪ 2001: Prototype test phase: 500 cards issued ▪ End of 2001 – 2002: Large scale deployment The targets are the French citizens, the enterprise, the administrations and the local communities (36500). The roadmap is build on the number of the local communities: ▪ 2001: 30 ▪ 2002: 300 ▪ 2003: 600 ▪ 2004: 1000 ▪ 2005: 3000 In its conceptual phase AdeP has become the reference project in France related to Electronic Signature law issues for certified electronic procedures.
Finnish Citizen Identity card	▪ Project in production. Approximately 9500 electronic identity cards have been issued already while the target number is the entire Finnish population. ▪ The project has not reached its deployment goal and the number of cards issued remains low.
French Notaries	Project in production since 1999. The target audience is the notaries and their employees. While some 3500 cards and electronic signature packages have been deployed already the target has been set to 22000 cards. The technical goal has been reached, but the number of transactions remains weak. The project has gathered publicity in France with regard to Electronic Signature and smart cards. Future deployments are currently under examination, addressing the needs of corporate that make use of notary services.
GIP-CPS	This project is in production phase. 350k cards have been issued in October 2001. The objective is 1 million cards deployed in 3 to 5 years.
Italian Citizen Identity card	2001: Pilot phase with a volume of 100k cards. 2002: First deployment phase targets 1M cards. 2003: General deployment phase targets 8M cards. This project has encountered delays due to non-specified technical problems.
PKI Overheid	Actual status of the project: ▪ Public consultation of requirements. ▪ Several pilots. ▪ Start of the implementation of central components of the infrastructure. Deployment roadmap: 2001-2002: pilots, requirements 2002-2003: (pre) implementations 2003-2005: large scale roll-out Between 2003-2005 the target is to rollout 20M active smart cards.
Posten AB	This project is in production with 50k cards already issued.. Full deployment to the entire adult Swedish population, will extend this number to 6M cards. . This project, which began in 1996, has reached its staged implementation goals. The focus of this project has shifted from identity card deployment to on-line services.

Satakunta Macropilot	Ongoing Pilot phase Full distribution of cards: September-October Final target is 1000 cards issued for professionals and 10k cards issued for citizens. The Finnish Government/Population Register Centre of Finland issues the cards. The project goal has been to produce the card, develop the distribution project and distribute the cards to the users.
Social security and Communidad Valenciana public services	The project analysis stage has been accomplished. Pilot project: June 2002 Full deployment: January 2003 with 5Mcards.
Tekes project	First operational software version in the beginning of summer 2001. The cards are issued by the Finnish government/Population Register Centre of Finland.

4.1.3 Registration, certification and smart card personalisation procedures

This section addresses aspects associated with the registration procedures the issuance of certificates and the smart card personalisation and delivery. Introducing smart cards in the PKI architecture is also a source of additional complexity with respect to the smart card personalization, security policy (e.g. aspects of key generation), distribution of personalised smart cards and the relationship between registration authorities, certification authorities, certification operators and smart card personalisation agent. Although no unifying scheme has emerged as yet, we can still notice that centralisation of certificate generation and personalisation is essential for the success of a project. Almost all projects have referenced the strong importance of the registration process to support trust in the certificates delivered. The organization of the registration process, however, strongly depends on the scope of the project.

In public identity projects, i.e. for citizen identity cards, the registration procedure is based on face-to-face meetings between the registration authority agent and the user of the system. At the face-to-face meeting the applicant is asked to produce a physical identification document and fill out and sign a Pre-inventory form. The downside of this approach is that it may limit the subscribers to a procedure that cannot be detached from the time of the issuance of a certificate should it require the physical presence at the time of the issuance of the certificate [ETSI 01]. With regard to community projects (e.g. health, notaries public etc.) a central agency mails directly to the user a smart card request form using a reliable database that holds the personal information of the users.

Some projects have separated the certificates issuance (e.g. in-sourced or outsourced) from the smart cards issuance while others have chosen to outsource both certificates and smart card issuance to a smart card personalization centre. In large scale and operational projects, the smart card personalisation is typically outsourced to a smart card manufacturer.

In some projects still under study or at the test stage, an agent in charge of delivering the smart card is responsible for the card personalization (e.g. PIN generation, dual keys generation, on-line public key certification etc.) in a face-to-face meeting with the end-user. The anticipated time for this operation is usually short (about 10 minutes). This personalization process is accomplished through a new generation of smart cards that integrate an on-board key generator. This approach ensures that the private keys are never released to the domain outside the

smart card. The on-board key generation process appeals to projects associated with signature keys. The table below gives further information and details on the projects:

Project Name	Registration procedure	Certificate issuance procedure	Smart card personalisation and delivery
ABN Amro - Identrus	According to Identrus requirements	Outsourced	Outsourced
AdeP	Face-to-face registration with physical presence or on-line.	Outsourced	In sourced. Face-to-face smart card delivery and personalisation (on-board key generation) at a local community office.
Finnish Citizen Identity card	Face-to-face	In-sourced	Outsourced
French Notaries	Postal form from a central agency	In-sourced	In sourced. Face-to-face smart card delivery in Regional Notary Chambers. PIN code is mailed.
GIP-CPS	Postal form from a central point	Outsourced	Outsourced. Smart card postal delivery PIN code is mailed.
Italian Citizen Identity card	No information available	In-sourced	In sourced
PKI Overheid	Under study	Under study	Under study
Posten AB	Face-to-face meeting at a post office	In-sourced	Outsourced. Face-to-face delivery at a post office.
Satakunta	Face-to-face meeting at the distributor's office.	Outsourced	Outsourced
Social security and Communidad Valenciana public services	Face-to-face meeting for the registration and the personalisation.	In-sourced	In sourced. Face-to-face meeting for the registration and the personalisation (on-board key generation).
TEKES	No information available	Outsourced	Outsourced

4.2 Technical Aspects

The projects under examination combine smart cards and PKI due to specific features these technologies have to serve the purposes of the projects. The following reasons have most often been quoted to explain the usage of PKI in these projects:

- Requirement for compliance with emerging standards to ensure interoperability of the project with applications to be developed in the future.
- Need for open solutions as most of the projects involve multiple parties, some of them are expected to join in the future.
- Anticipated move to legally binding digital signatures.
- Maturity of technologies used.

On the other end, inhibiting factors include deployment complexity instigated by the combination of smart cards and PKI and a perceived protracted standardization process that prolongs uncertainty. Some projects have chosen to outsource the PKI management to private entities while others have set up their own processing centre. There has been no clear explanation identified with regard to certain choices such as number of certificates to be deployed, existing internal IT infrastructure etc. This apparently *ad hoc* behaviour can be illustrated by the comment of most interviewees who suggested they would probably have to reconsider their initial project premises following feedback they receive on their projects.

While the PKI architecture varies significantly between the projects examined there is a general consistency in the usage of clear and definite standards. It is typical that projects with one single level of authority coexist with multi-layered projects. The need for specific client side software depends on the project environment; hence it is not a constant requirement for all projects as it is related to the general objectives the project serves. The general tendency has been to avoid client-side software as it is considered an additional complexity factor as deployment and maintenance of the client side software is a significant issue for the final deployment.

The usage of smart card in the examined projects has also been a condition for inclusion in this inventory. The interviews revealed the following main reasons behind the main choices of the projects:

- Need for strong security for the protection of the private key.
- Need for convenience and portability for the end user.
- Perceived impact of national regulation and willingness to ensure results with regard to the solution in hand.
- Continuity of existing card based infrastructures (e.g. Pre-inventory based identity cards).

Deployment complexity and the high cost of smart cards has some times become an obstacle for the final adoption of the technologies. As highlighted in the table below, analysed projects share common views on the smart card profile:

Project Name	Card Memory	Embedded crypto	Security Certification	Onboard key generation
ABN Amro - Identrus	32 Kb	RSA coprocessor		No
AdeP	8 Kb	RSA coprocessor		Yes
Finnish Citizen Identity card	16 Kb	RSA coprocessor	FIPS 140-1 level3	Yes
French Notaries	8 Kb	RSA coprocessor		No
GIP-CPS	4-8 Kb	RSA coprocessor – A3S proprietary symmetric algorithm	ITSEC E3	No
Italian Citizen Identity card	16 Kb	RSA coprocessor	ITSEC E4 for chipset	Yes
PKI Overheid	tbd	RSA coprocessor	tbd	tbd
Posten AB	16 v	RSA coprocessor	ITSEC E4	No
Satakunta	16 Kb	RSA coprocessor	FIPS 140-1 level3	Yes
Social security and Communidad Valenciana public services	tbd	tbd	tbd	Planned
TEKES	16 kB	RSA coprocessor	FIPS 140-1 level3	Yes

There has been limited information on planned moves towards open operating systems for smart cards (e.g. JavaCard, Windows for Smart Card, Multos etc.).

Compliance with security standards on the other hand (e.g. FIPS, Common Criteria etc.) is identified as a key issue to ensure compliance with legal requirements regarding digital signatures. Further information, however, has been limited. Reasons mentioned include the following:

- Limited availability of tested and accredited smart cards.

- Limited, or no awareness of the legal requirements related to digital signatures.

In most cases in the analysed projects, the validity period of the certificates is the same as the validity period of the smart card. This choice means that the certificates and the cards are renewed at the same time. This section aims at describing the PKI technical options taken into consideration in the various projects:

Project Name	Key length (in bits)	Number of certificates per user	Key recovery mechanism	Certificate validation
ABN Amro - Identrus	1024	2	Not allowed for identity Key	OCSP
AdeP	512 will become 1024	TBD	TBD	TBD
Finnish Citizen Identity card	1024	2	No	CRL
French Notaries	1024	4	No	CRL
GIP-CPS	1024, 2048 for root	2	No	CRLv2
Italian Citizen Identity card	1024	No information	No	CRL - OCSP planned
PKI Overheid	TBD	TBD	TBD	TBD
Posten AB	1024	2	No	CRL -OCSP considered
Satakunta	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card
Social security and Communidad Valenciana public services	1024	2	TBD	CRL - OCSP considered
TEKES	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card

The following table addresses the content and profile aspects of the issued digital certificates.

Project Name	Certificate protection	Certificate profile	Applicable standards	Validity period
ABN Amro – Identrus	Stored PIN	Identrus	X509v3	3 years
AdeP	Stored PIN	TBD	X509v3	1 year
Finnish Citizen Identity card	Stored PIN	No information	X509v3	3 years
French Notaries	Stored PIN	No information	X509v3	2 years
GIP-CPS	Stored PIN	No information	X509v3	3 years
Italian Citizen Identity card	Stored PIN	No information	X509v3	5 years
PKI Overheid	No information	No information	X509v3	No information
Posten AB	PIN Code for each certificate	Compliant with SS 61 43 31 and SS 61 43 32 (Swedish standard)	X509v3	5 years
Satakunta	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card
Social security	Local PIN, stored &	No information	X509v3	No information

and Communidad Valenciana public services	online biometrics			
TEKES	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card	See, Finnish identity card

Technical standards and interoperability have been in the focus of all these projects. Nevertheless, the impact of interoperability in the deployment phase is limited. The initial focus of the projects has mostly evolved with respect to their own constraints rather than focusing on establishing the connection with other European projects. It is important to mention the usage of emerging technical standards by either regional initiatives (e.g. SEIS, the Swedish standards organisation) or industry-led organisations (e.g. Identrus). This Inventory demonstrate a clear preference for the following widely recognised standards as the table below shows:

PKI and digital certificates	**Smart cards and interfaces**	**Smart card reader**	**Secure signature creation device**
X509 v3	PKCS# 11 and Crypto API CSP PKCS#15	PC/SC	No standards used as yet
CRLv2			
OCSP			

While only few projects use proprietary readers (e.g. with PINPad) most have already turned to usual PC/SC smart card readers. As interoperability issues have been detected, some projects maintain publicly available lists of tested readers.

Although there is a general awareness of the standardization effort currently carried out by EESSI with regard to digital signatures, only few of them have a clear understanding of the exact scope of the standardisation output and the position of EESSI as opposed to other standardization initiatives or the output of European and non-European standardisation organisations. Few parties involved in the projects analysed have yet quoted EESSI standards as a decisive factor in their projects. This is almost certainly because the EESSI standards are new and have yet to be discussed by the Commission's Article 9 committee. Other standards, such as PKIX, also have rarely been mentioned by the interviewees of this Inventory. Interoperability addresses a wide range of topics from verification of certificates issued by different CAs to application use of certificates by various CAs. The latter has largely been addressed by application interface standards, like PKCS#11 and Microsoft Crypto API, which provide vendor-independent methods of accessing and using certificates and the underlying keys in applications. Almost all the projects studied have chosen these standards or plan to migrate to them.

4.3 Legal Aspects

The projects analysed demonstrate a clear interest in the legal requirements regarding digital signature and certification authorities as they seek compliance with national and European law on electronic signatures alike.

At a legal and procedural level, the CAs involved issue certificate policies (CP) or certification practice statements (CPS) to describe their services.

Compliance with Directive 99/93 on electronic signatures is a claim made by all projects although the criteria on which they are making this claims are usually unclear. Rolling out qualified certificates according to the European Directive remains an objective of most of the projects under review.

Publishing applicable certificate policies is typically done by means of a CP or CPS. Accrediting the CAs is also an objective for the projects under examination. Within the general policy framework a specific reference to liability may support the clear definition of the limits of reliance on digital certificates. Addressing aspects of liability of the various implicated entities (e.g. CA, RA etc.) is currently only dealt with at the very late stage of the projects under consideration.

Project Name	Plans for Qualified Certificates	Qualified certificates target date	Accredited CA	Liability policy	CP/ CPS
ABN Amro - Identrus	Yes	In progress	Identrus	Yes	Yes
AdeP	Yes	TBD	No information	No information	TBD
Finnish Citizen Identity card	Yes	TBD	Population Register Centre	Yes	Yes
French Notaries				No	Yes
GIP-CPS	Yes	End of 2001	Ministry of Finance	No	Yes
Italian Citizen Identity card	TBD	No information	Ministry of Interior	No information	Yes
PKI Overheid	Yes	2003	TTP.NL	Planned	Yes
Posten AB	No	TBD	No information	Yes	Yes
Satakunta	No information				
Social security and Communidad Valenciana public services	Yes	TBD	No information	No information	Yes
TEKES	No information				

All projects have expressed strong concern and interest in data protection issues. However, beyond national laws, there has been no clear reference to any other source (e.g. such as the European Directive 95/46 on Data Protection).

Regarding consumer protection, French projects have been under the supervision of CNIL (Commission Nationale Informatique et Liberté), an independent administrative body that addresses consumer protection matters.

5.0 Conclusions

The combined use of the smart cards with PKI technology adds to the complexity of the CA operations and has a significant impact on the goals and the organization of the PKI projects. For example, a card management process must be taken into account in coherence with the certificate management process.

There is a constant need for end user awareness and training to facilitate the smart card adoption and the acceptance of PKI-enabled applications. The combination of a smart card, a reader and software influences the dynamics of the deployment (e.g. more technical problems, additional support skills). User friendliness should reach a level where the PKI activities are not visible to the end users who do not need to

know what underlying technology is being used. Making the end-user application work together with the smart card through software and a card reader demands a "pre-packaged" and user-friendly solution.
Business models to date have been mostly complex and the return on investment difficult to estimate for the projects reviewed. It is generally considered that the role and responsibility of the stakeholders involved in the supplying and management of smart card based PKIs should better be defined and examined. The proper development and application of of business plans in this area may further help widespread use of these technologies in a cost efficient manner.

A large number of projects have encountered technical problems with regard to the smart card implementation. These issues have sometimes significantly impacted the implementation phase of the projects. There are constant problems to install readers, drivers and application software while the storage of the root key on the smart card is still an issue.

Key recovery policy, while a necessary business requirement is not addressed in this inventory due to the current lack of applicable standards and the resultant process deployment complexity

It is generally felt that PKIs cannot at this particular time be generally interoperable as there is no focus on the interaction, interoperability and mutual recognition of systems, platforms, specifications and requirements between cards, card readers, middleware and applications.

Laws and standards defined at national, European or international level, have been widely welcomed in almost all projects. Some strong operational projects that started early with proprietary systems when standards and laws did not exist, must now migrate to a new system in order to be compliant with such formal legal and regulatory requirements. The need to ensure compliance with prevailing formal statutory requirements is now well recognised and perceived as on of the next challenges.

It is recommended to clearly define well in advance, the subset of the standards and laws that suppliers must comply with and further validate such compliance. A clear vacuum can be identified with regard to privacy issues associated with the PKI infrastructures. There is also a general lack of present day standards or best policies to put formal legal privacy requirements into practice. A limited offer of insurance policies associated with the usage of the certificates adds to the complexity of the operation.

This survey demonstrates that the standardisation work required in the field of electronic signatures has not reached a sufficiently conclusive stage and furthermore that in most cases the current EESSI and other developments have yet to be adequately implemented. Additionally process improvements in project planning will further improve realization of project goals and allow smart card based PKIs to reach a fuller stage of maturity.

6.0 Recommendations

6.1 Business and Organizational Aspects

This Pre-inventory suggests that the combined use of the smart cards with PKI technology has a significant impact on the goals and the organization of the PKI projects. The main reasons for this impact include the following:

A smart card management process must be planned together with the certificate management process.

- Production: graphical chip (e.g. printing techniques).
- Card issuance: key generation, personalization and delivery.
- Information update (e.g. certificates, user information).
- Usage phase
- Card renewal

End user awareness and training are required elements to support the usage and acceptance of smart card based PKIs and associated applications.

The end user application must work together with the smart card through appropriate software and a smart card reader. The end-user needs a "pre-packaged" and user-friendly solution.

The combination of hardware such as a smart card, a reader and a software solution has an impact on the deployment phase of the project (e.g. more technical problems to resolve, support skills required etc.).

The business model is complex and the expected return on investment has not been reached yet in any project under review. Further input is necessary to address this important aspect.

Projects, which also issue their own smart cards, have worked out a cooperation platform with software providers and integrators to deliver user-friendly smart card based solutions.

It is generally considered that the role and visibility of the organizations supplying and requesting smart card based PKIs should be better defined and examined. The proper development of business plans in this area may further help lead to widespread use of these technologies. User friendliness should reach a level where the workings of PKI do not have to be visible by the end users who do not necessarily have to know the underlying technology in use.

Recommendations
Based on the information available, the Pre-inventory team makes the following recommendations with reference to the organisational aspects of a smart card based PKI project:

1. Strongly promote organizational best practices, possibly through extensive case analysis across Europe and beyond (e.g. USA, Asia).

2. Define a global methodology to set up PKI and smart cards projects including organisational, technical and legal aspects.
3. Define registration, personalization and delivery process guidelines for large-scale smart card based PKI deployments.
4. Consider workable business models that include the following:
   - Reference costs since this survey reveals that costs are often underestimated.
   - Possible revenue sources need to be further identified.
   - Understand how the smart card based PKI fits into the overall business requirements.
5. The outsourced PKI model needs to be better taken into account and firmly put into the picture of setting up a smart card-based PKI.
6. Analyse best practices for revocation management.
7. Propose implementation guidelines for further services (e.g. secure archival, validation, time stamping) where such services appear compelling to project managers but are lacking reference implementations and deployment know-how.

6.2 Technical Aspects

This Pre-inventory suggests that a large number of projects have encountered technical problems with regard to the smart card implementation. Such issues have significantly delayed the implementation of the projects.

The following issues have been underlined:
Smart card implementation
- Installation of a smart card reader is time consuming and therefore costly.
- Drivers and application software do not feature the required user friendliness at all times.
- Storage of a root key on a smart card remains a challenge.

Key recovery policy
- There are no clear standards as yet that combine key recovery and back-up mechanisms with secure operations management. Deployment complexity is said to prevent the establishment of key recovery mechanisms.

Signature software
- This survey has not revealed any clear trend or market leading solution.
- Some projects have their own approval policy for the signature software to be used in their application.

On these issues, the choices made in each project vary considerably. This might allow for very limited interoperability only between smart card based PKIs and applications, which in it own turn is likely to hamper the growth of such applications.

To reduce currently outstanding technical issues as much as possible, the following aspects should be examined further:
1. Develop a reference platform to test the system integration and interoperability.
2. Underline interoperability as an essential success factor and take steps to promote it.

3. Focus on specific aspects of interoperability including smart cards, digital certificates, the interaction and mutual recognition of systems, platforms, specifications and requirements between cards, card readers, middleware and applications.

Recommendations

Based on the information available, the Pre-inventory team makes the following recommendations to the organisations involved in this survey with reference to the technical aspects of a smart card based PKI project:

1. Promote the deliverables of EESSI in smart card based PKI. It is necessary to present and disseminate the scope, role and deliverables of EESSI. Analyse in detail the background of technical norms also with respect to the involvement of European standardisation organisations such as CEN/ISSS and ETSI.
2. Define and disseminate high-level norms for electronic signature software. Provide a list of compliant vendors and products that should be maintained, in cooperation with local authorities.
3. Take into account that the lack of available and reliable products has often delayed the deployment of the projects considerably. Therefore, when working on CWA14168-CWA14169, strike a balance between security and effective deployment.
4. Examine and identify "jump start" product packages compliant with EESSI related standards, as there is currently concern about the low level of market availability of such products. Ensure harmonisation and legal interoperability among the various accreditation schemes in the member states that are currently being put in place (See, also the recommendation under the next section "Legal").
5. Explain the impact of PKI architectures (e.g. number of CA / sub CA, cross-certification, bridge CA etc.), possibly through an in-depth case analysis.
6. Analyse the conflicting issues between the emerging regional or national standards and the European norms and standards defined and work towards converging visions.
7. Define the interoperability requirements through functional and business analysis of the projects. This survey highlights that national identity projects for citizen identification cards (if any) practically set the rule and other projects adapt to their specifications.
8. Work in such a way that encourages coherent result of the output of the various accreditation schemes (from a technical point of view). As a minimum level requirement support documentation that highlights convergence points and conflicting issues.
9. Provide technical guidelines with regard to activities in standardisation and definition of specifications in areas like time stamping, secure archival, key recovery as the currently limited activity discourages investment.

6.3 Legal Aspects

Laws and standards that have been defined at a national, European or international level have been widely welcomed in almost all projects. Some strong operational projects that have started early enough with proprietary systems as some standards and laws did not exist at the time, shift to a renewed approach to ensure compliance

with such formal legal and regulatory requirements. Ensuring compliance with prevailing formal statutory requirements often remains a challenge.

It is recommended to clearly define well in advance, the subset of standards and laws that suppliers must comply with and further validate such compliance.

A clear vacuum can be identified with regard to privacy issues associated with the PKI infrastructures. While a general concern on this subject is widely shared the lack of standards or best policies to put formal legal privacy requirements into practice underlines the requirements in this field.

There is currently a clear absence in terms of insurance policies regarding the activities linked with digital certification.

Recommendations
Based on the information available, the Pre-inventory team makes the following recommendations with reference to the legal aspects of a smart card based PKI project:

1. Harmonise the legal environment on application areas such as electronic identity cards, electronic payments and digital signatures.
2. Ensure harmonisation and legal interoperability among the various member states accreditation schemes currently being put in place. In this effect the mutual recognition of the equivalence of accreditation schemes across Europe must be accelerated. Operating under a common framework, such as EESSI, can significantly contribute to concrete and fast results. Issue documentation to highlight convergence points and conflicting issues in coherence with the Directive and the expectations of the market. Examine and identify jump-start product packages compliant with EESSI standards as project leaders have expressed concerns about the low level of market availability of such products. The reader may view this recommendation in line with a related recommendation under previous section "Technical".
3. Provide guidelines on the practical implications of privacy in PKI in the form of a combination of best practices and existing legislation.
4. Develop elements of analysis regarding the liability issues at stake within PKI projects. Possibly provide, as a first step, general legal reference documents beyond the scope of RFC standards and based on deployed projects to ease set-up of PKI and projects.
5. Work together with insurance experts on guidelines to define appropriate insurance policies.

Annex I

List of Contacted Parties

Citizen Identity Cards

Project Name	Brief description	Contact information	Status
Austrian Citizen Identity Card	The Austrian Citizen card is an electronic identification basing on secure electronic signature using the technology distributed by the social security system. It inherently offers the European dimension according to the legal situation provided by the European signature directive. At the will of the citizen this card can additionally provide a means to carry data that need not relate to the person carrying the card through this technique. As the actual provision of signatures and thus certificates on this card is left to the market this offers a system, which is most open and still allows for maximum interoperability.	Prof. Reinhard Posch http://www.buergerkarte.at/	No answer
Netherlands Citizen Identity card	No further information available	Mr. Marc Gerrard E-mail adress: marc.gerrard@bprbzk.nl	No answer
Finnish Citizen Identity card	The electronic identification card is a secure network key for all on-line services, which require the identification of a person, such as all government and many private sector services. The card enables the service provider to reliably identify the user. The card is also an official travel document for Finnish citizens in 19 European countries. The local police department issues the electronic identification card. The Finnish Population Register Centre supplies the on-board certificates that are used in electronic identification. In addition to the card, a card reader is needed for on-line use. In the future, identification can be done from a mobile device such as a cellular phone equipped with a special chip. The electronic identification card costs FIM 160 and it is valid for three years.	tapio.aaltonen@vrk.intermin.fi Voitto Kiviharju (SC2 TB1) The Population Register Centre PO Box 7, Kellosilta 4, FIN-00521 HELSINKI Tel:+358 9 2291 6616 Fax:+358 9 2291 6718 E-mail: voitto.kiviharju@vrk.intermin.fi http://www.vaestorekisterikeskus.fi/indexen.htm	Interview
Posten AB	Posten AB issues and authenticates electronic identification documents. Posten AB's platform for secure Internet solutions is founded on the technique for PKI and implies the use of one pair of keys for coding and decoding and one certificate containing information about the key owner. The platform consists of tree basic services: identification, signing and coding.	evald.persson@posten.se 08-781 6638	Interview
Italian Citizen Identity card	No further information available	Carlo Penti <cpenti@labs.it> Mr. Roberto Benzi rbenzi@aipa.it http://www.lasercard.com/news/oct19a.htm www.aipa.it	Interview

Health-care systems

Project Name	Brief description	Contact information	Status
France - GIP-CPS – Groupement d'Intrérêt Public Health Professional Cards	The objective of the GIP-CPS is to create the security and trust environment for the electronic exchanges inside the health world independently of the network used. They provide smart cards to French Health Professionals. The Smart Card is PKI based and the GIP-CPS manages the security infrastructure (card issuance, certificates and CRL directory etc.). About 350000 cards have been deployed to date. The main applications are the protection of the Web access and the messages inside the health community.	Gilles Taïb – Général Manager g.taib@gip-cps.fr +33 1 44 53 36 44 Gilbert Abulafya g.abulafya@gip-cps.fr +33 1 44 53 33 86 www.gip-cps.fr	Interview
France - Sesame Vital	No further information available	Noël Nader Noel.Nader@sesam-vitale.fr 02 43 57 42 00	Out of scope -- Not a PKI card
Media@Komm Project, Germany	Health professional card	Juergen, Sembritzki E-mailadres(sen): j.sembritzki@ztg-nrw.de	No answer

Social Security systems

Project Name	Brief description	Contact information	Status
Satakunta Macro projects for Social Insurance cards, Finland	The goal of the Satakunta Macro Pilot is to develop and test a seamless, client centred, independent service chain support model for Social and Health Care Services. The seamless service chain is a functional model where, from the client's point of view, an individual's social and health care services form an integrated whole. The whole is independent of whatever organization is providing services at any given time. The seamless service chain is based on information technology in that a client's social and health care information contained in various data systems is available for the use of professional service providers in all service situations. The system developed for this purpose is known as the regional information system, which uses a "smart card" based social insurance card as a guarantee of data security.	Tuire MIKOLA, Satakunta Macro Pilot tel +358 2 620 4452 fax +358 2 620 4499 email tuire.mikola@makropilotti.fi http://www.makropilotti.fi/english/	Interview
Social Security and Communidad Valenciana public services	Project in Healthcare and social security	Pedro Lagunas <plagunas@dgp.mir.es>	Interview

Financial systems

Project Name	Brief description	Contact information	Status
Identrus	Having recognised interoperable security as the biggest barrier for Business to Business (B2B) e-commerce, Identrus LLC was founded by a consortium of financial institutions, including ABN-AMRO, with th eobjective to create a global interoperable Public Key Infrastructure (PKI) supported as a standard by leading global banks. This resulted in a highly secure solution that: ▪ Provides a global framework for the provision of certificate authority services to securely identify companies via on-line business applications; ▪ Enables financial institutions to extend their full range of practices onto the Internet and become trusted third parties for e-commerce transactions; ▪ Gives businesses the ability to leverage multi-lateral relationships with financial institutions for e-commerce dealings; ▪ Offers businesses and financial institutions a way to proactively manage the risk associated with e-commerce; Offers businesses a highly standardised, cost-efficient solution to trust their business partners on the Internet.	ABN Amro Contact Identrus product management SJOERD.Koster@nl.ABNAMRO.com 0031 - 20 38 37524 http://www.id-key.com http://www.identrus.com	Interview
GTA	No futher information available	Ron van Wolferen Interpay Ron van Wolferen ron.van.wolferen@wxs.n	No answer

Legal Compliance/Legal Profession

Project Name	Brief description	Contact information	Status
Spanish office of Patents and Trade marks	1. Securing access to the registers of user of the OEPM 2. Electronic presentation of orders of payment by the Agents of the industrial Property Project in test phase from June 2000.	Justino Garcia Tel: +91 349 5442 Carmen Gomis, Carmen.gomis@oepm.es Tel: +91 3493011	No answer
Madrid Bar Association	Authentication of identity in sending documentation of the Society of Lawyers and the courts	Felix Ballesteros Rivas felix@icam.es	No answer
DigiNotar, NL	TTP Services	Tony de Bos Beverwijs http://www.diginotar.com/engels.html	No answer
French Notaries	The French notaries have deployed a complete PKI system. The main application is the electronic signature and the authentication	Claude Lemogne claude.lemogne@notaires.fr (01) 44 90 30 39	Interview

Accreditation Schemes and Certificate Authorities

Project Name	Brief description	Contacts & Web Site	Status
TTP.NL	TTP.NL is a self-regulation initiative coordinated by the Electronic Platform Netherlands, ECP.NL. Over the last few years TTP.NL has developed an infrastructure for Certification Authorities (CA) in the Netherlands. CAs can demonstrate their compliance with Directive 1999/93/EC by obtaining a TTP.NL certificate of conformity. The implementation of TTP.NL has been based on ETSI TS 101 456.	J.R. Boersma jacob.boersma@ecp.nl Arie van Bellen arie-van.bellen@ecp.nl Marjolijn Bonthuis-Krijger, marjolijn.bonthuis@ecp.nl	Not in the scope of the project
Tscheme	Industry led accreditation scheme in the United Kingdom	Richard Wilsher rgw_zygma@compuserve.com www.tscheme.org	
NovoTrust	A company offering PKI-solutions combined with smart cards. NovoTrust has also been accepted to offer certificates valid for the public administration in Finland.	Mr. Heikki Sundquist heikki.sundquist@novogroup.com www.novotrust.com	No answer

Local Government

Project Name	Brief description	Contact information	Status
GISA, Catalan Government project for public procurement (Local Government)	Electronic signing of the whole documentation associated with a work contract (contract, levels, endorsement etc.).	Jaime Nart Jne@gisa.es Tel : +93 444 44 44 Xavier Gonzalez Xgl@gisa.es Tel : +93 444 44 44	No answer
Gov. of La Rioja, Spain	1. Sure mail between the Advisors of the Community 2. Digital signing of official documents Project in testing phase since June 2000.	Pedro Samniego Riano, Secretaries General Technical Pedro.samaniego@larioja.org Francisco Javier Aparicio Javier.aparicio@larioja.org	No answer
Xunta of Galicia, Spain	Secure Web site: ▪ Consultation by the companies of the register of contractors of the Xunta ▪ Telematics presentation of parts of occupational illness and accident at work of the Managing Organizations of Social Security	Javier Franco Tubio, prdxosi@xunta.es Rodrigo Carballo, Alvaro.rodriguez.carballo@xunta.es	No answer
Cities project – Marseille (IA 1002 AD) – Other cities include: Brussels – Madrid – Rome	This project experimented a PKI citizen card with the objective for the city of Marseille to provide citizen with access to online services from the municipality.	Dr. Edmond Kouka of Gemplus Edmond.KOUKA@gemplus.com	No answer

Electronic Forms/ Electronic Procedures

Project Name	Brief description	Contact information	Status
TEKES project, Finland	Tekes, the National Technology Agency is the main financing organization for applied and industrial R&D in Finland. The funds for financing are awarded state budget. A project was started by Tekes with the State Research Centre as a customer, Signform Oy and Softplan Oy as solution providers. The aim of the pilot project was to test the use of the electronic identity card launched by the Population Register Centre in Finland as well as the procedures of sending ans receiving the application in electronic form.	Kristiina Laurila – Tekes Customer Service Kristiina.Laurila@tekes.fi Harri Eskola Harri.eskola@tekes.fi Johan Sjoeberg – Signform johan.sjoberg@signform.fi Pekka Kuosmanen – Signform Oy Pekka.kuosmanen@signform.fi	Interview
AdeP (Association for the development of eProcedures in France)	Multi-usage citizen card	Bruno DECROCQ - AdeP Tel : + 33 4 7566 9650 Adep.projet@wanadoo.fr	Interview
Ministry of Agriculture, Spain	Project Land: Consultation and shipment of documentation and protected of the olive-growing ones of Toledo through a page Web	Fernando Bezares, Tel: +91.3475092 Jose Ramon Garcia Tel : +91 347 54 73	No answer

National Contact

Country	Contact	Organisation	Tel.	e-mail	Status
AT	Dieter KRONEGGER	Rundfunk und Telekom Regulierungs-GmbH (RTR)	+43 1 58058-407	Dieter.Kronegger@tkc.at	Answer
BE	Philippe DEGAVRE	Administration de la Qualité et de la Sécurité Division Accréditation Ministère des Affaires économiques	+32 2 206 47 09	philippe.degavre@mineco.fgov.be	No answer
CH	Peter STADLIN	Bundesambt für Metrologie und Akkreditierung (METAS)	+41 31 323 35 30	peter.stadlin@metas.ch	No answer
DE	Jürgen SCHWEMMER, Head of Section Digital Signature	Regulierungsbehörde für Telekommunikation und Post (RegTP)	+49 61 31 18 22 10	juergen.schwemmer@regtp.de	No answer
	Friedrich KÖNIG, Assistant Head of Section Digital Signature	Regulierungsbehörde für Telekommunikation und Post (RegTP)	+49 61 31 18 38 48	friedrich.koenig@regtp.de	No answer
DK	Birgitte HAGELSKJÆR NIELSEN, Legal Adviser	Telestyrelsen DK, National Telecom Agency	+45 35 45 02 84	Bhn@tst.dk	No answer
ES	Antonio RODRÍGUEZ AGEA Gema CAMPILLOS, Fernando FAZIO FERNÁNDEZ de MIRANDA	Dirección General para el Desarrollo de la Sociedad de la Información	+34 9134 949 37	ara3@min.es	No answer Not contacted Not contacted
FI	Kirsi SUNILA-PUTILIN, Legal Counsel/Telenetwork security Timo LEHTIMÄKI, Senior Adviser/Telenetwork security	Telecommunications Administration Center (TAC), National Post & Telecom Agency	+358 9 6966 806 +358 9 6966 815	Kirsi.Sunila-Putilin@thk.fi Timo.Lehtimaki@thk.fi	No answer Answer
FR	Laurent PERDIOLAT	Secrétariat d'Etat à l'Industrie - Direction Générale de l'Industrie, des Technologies de l'Information et des Postes - Ministère de l'Ėconomie, de Finances et de l'Industrie	+33 1 53 44 94 02	laurent.perdiolat@industrie.gouv.fr	Answer
GB	Geoff SMITH Tom Parker	Information Security Policy Unit, Department of Trade & Industry tScheme	+44 20 72 15 29 40	Geoff.Smith@ciid.dti.gov.uk	No answer Not contacted
GR	Ms. Eleni VITOYANNI	National Telecommunications and Post Commission	+30 1 61 51 133	EVytog@EETT.gr	No answer
HU	Istvan RENYI	Hungarian Communication Authority	+36 1 457 74 20	Renyi@hif.fu	No answer
IE	Niall CURRAN	Department of Public Enterprise	+353 1 604 1044	CurranN@tec.irlgov.ie	No answer
IS	Arsaell DORSTEINSSON, Technical Director	Löggildingarstofa, National Accreditation Agency	+354 510 11 00	Arsaell@ls.is	No answer
IT	Dr. Roberto	Autorità per l'informatica nella	+39 06 85	Benzi@aipa.it	Answer

	BENZI	Pubblica Amministrazione (AIPA)	26 42 09		
LU	Carlo WIRTH	Commerce électronique, Accréditation, Promotion de la Qualité,- Ministère de l'Économie	+352. 478 - 4140	Carlo.Wirth@eco.etat.lu	No answer
NL	Ronald VAN DER LUIT	Ministry of Transport, DG Telecommunications & Post	+31 70 351 77 93	Ronald.VDLuit@dgtp.minvenw.nl	No answer
	Rob VAN EIJL	OPTA (Independent Post and Telecommunication Authority	+31 70 315 92 39	r.vaneijl@opta.nl	No answer
	Arie VAN BELLEN	TTP.NL	+31 654 23 43 44	Arie-Van.Bellen@ecp.nl	No answer
NO	Øyvind HAUGEN, Legal Adviser/Market Regulation	Post- og teletilsynet (PT), Norwegian Post and Telecommunications Authority	+47 22 82 46 00	Oyvind.Haugen@npt.no	No answer
PT	Manuel Pedrosa de Barros, Director	Direcção de Equipamentos e Normalização		manuel.barros@icp.pt	No answer
	Pedro VEIGA, Manager	Programa Operacional Sociedado da Informacão, Ministério da Ciéncia e da Tecnologia			Not contacted
	Carlos GONÇALVES, Vogal	Instituto das Tecnologias de Informacão ba Justiça, Ministério da Justiça			Not contacted
SE	Henrik NILSSON,	Post & Telestyrelsen (PTS), National Post & Telecom Agency	+46 8 678 55 24	Henrik.Nilsson@pts.se	No answer
	Kenneth OLOFSSON	Post & Telestyrelsen (PTS), National Post & Telecom Agency	+46 8 678 55 74	Kenneth.Olofsson@pts.se	No answer

Annex II

Questionnaire

General Environment and Organisational Aspects of the Project

QUESTION	*EXAMPLES*
General	
What is the application in your project that is associated with the smart card	
What is the business model supported	*B2B, B2C, B2A, A2B , Other*
Indicate the area of application and the relevance to areas of the Smart Card Charter	*Public Identity* *ePayments* *User Interfaces* *Public Transport* *e-Government* *Healthcare* *Other…*
How would you best describe the geographical scope of your smart card project?	*Cross border* *Regional/local* *National* *EU wide* *Other…*
What is your target audience?	*General public* *Customer/client* *Enterprise*
Who is/are the major stakeholders or driving force behind the project?	*Government* *Business*
Please give details on elements of your business model	*Cost per user range* *charging model* *other…*
Project Deployment	
What is the size of your smart card project	*Number of cards issued* *Number of cards targeted* *Full deployment*
What is the current status of the project?	*Project analysis* *Ongoing pilots* *Operational*
Is your present project rolled over from a pre-existing one?	
If the answer to the question above is, yes, briefly describe your experience from such pre-existing project.	
What are the targeted phases of deployment?	*Timing* *Planning* *Delays experienced*
What significant problems did you encounter?	*Technical* *Political* *Other*
Has the project reached its goals?	*Metrics for success*
Process	
Please describe the smart card personalization & delivery process ?	*Personalisation Management (In house or Outsourced)* *Smart card delivery process (on site, mailed,…)* *Card management system*
Please describe the registration process	*RA procedures* *Verification of identity, requested documentation*
What have been the training requirements for personalisation agents and Registration Authority agents	*Trusted roles*
Please describe your support efforts for the end-user.	*Amount of support requested*

Please describe any documentation you might make available to the end user.	*Paper-based Manual* *Web Site* *Etc*
What has been the user reaction and feedback to your project?	
Archival	
Are there any retention requirements for documents in this project?	*Secure archival*
Are there any time stamping requirements for this project?	
Suppliers	
In your project do you use a single or multiple suppliers for smart cards?	
In your project do you have a single or multiple suppliers for your PKI?	

Conclusion

What were the main lessons learned during the project?

Out of your experience using standards for your project would you have any recommendations for the standards to which cards must comply with on the organizational side?

Technology Used in the Projects

QUESTION	*EXPLANATION*
General	
What technologies have been considered in the project ?	*Alternative solutions to PKI and/or smart card* *Reason for choosing PKI and smart card* *Perceived benefits & drawbacks*
Smart cards	
What are the main features of the smart card?	*Chip* *Memory Size (ROM Size , EEPROM Size,…)* *Technology (Programmable, configurable/customizable,"contact-less" etc.)* *Operating System (JavaCard, Windows for SmartCard, Multos, other,..)*
Does your Smart Card support other applications or is it a single application card?	*single card* *physical secure access* *payment,* *loyalty,* *e-purse,* *other, which ?*
What are the cryptographic features of the smart card in your project?	*Crypto processor* *Asymmetric algorithms: RSA, ECC etc.* *Hasching algorithm: MD5, SHA1 etc.* *Symmetric algorithm: DES,3DES etc.*
What is the PKI related content of your smart card ?	*Number of key pairs* *Number of certificates* *Root certificate stored on the card* *Other features*
If the smart card is used for electronic signing, what is the exact role of the card?	*PKCS 11 in the card* *Onboard key generation*
What authentication mechanisms are used?	*Online PIN verification, stored PIN verification, stored or online biometrics)* *Device that perform the matching*
Are there any other form factors involved ?	*Token USB*
Is the smart card compliant with international security standards?	*FIPS 140-1-2, EAL4+, ITSEC E3, EESSI, Other*
What are the main features of the smart card readers?	*PC/SC* *USB*
Public Key Infrastructure	
How do you manage the issuance of the certificates in house or you outsource it?	*In sourced or Outsourced* *Technology used*
Could you describe the certificate life cycle management in your project?	*Revocation / expiration: CRL, OCSP* *Key recovery* *Publication features: LDAP etc.*
Has interoperability with other PKIs been considered?	*Cross certification*
What are the main CA key management policy aspects that you have taken into account	*Key escrow, usage of third party agents, multiple token storage etc.*
What is the profile of your certificates and the preferred extensions?	*Content of the certificate*
What are the user registration requirements for certificate registration?	*Face to face,* *On-Line etc.*
What are the standards used in your project and for which specific purpose?	*EESSI, X.509v3, LDAP, CRL, PKCS, other*
Client side software	
Are the smart cards used in your project used as Secure Signature Creation Devices?	*Technology used* *Crypto characteristic* *Compliance with standards (FIPS etc.)*
What are the software requirements on the client side?	*Client side PKI software*

Is your PKI directly trusted by known applications?	*Is your PKI embedded in major applications?*
Briefly describe the general technology requirements of your project.	*Browser* *Operating system environment*

Conclusion

Out of your experience using standards for your project would you have any recommendations for the standards to which smart cards or PKI must comply with on the technological side?

Legal Aspects

QUESTION	*EXAMPLES*
General	
Could you describe the legal requirements that were considered in your project ?	Regional, National or European
Digital signature	
Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures?	
What are your plans to roll out qualified certificates?	
Plans to roll into SSCD as specified in CEN-CWA 14167-172	
Has your PKI taken into account any accreditation schemes? Have you planned or accomplished any accreditations?	
Have you planned or accomplished any audits of your project	
Do you make available an insurance policy for your project? Please describe the risks covered and the liability caps.	*Liability caps*
CP/CPS	
Could you describe the main features of your CP / CPS?	*Obligations of CA, Subscriber, relying party, smart card provider* *Liability of CA, Subscriber, relying party, smart card provider*
Do you make available any of the following such as a: - subscriber agreement - relying party agreement - consumer policy - privacy policy	
Describe the approval procedures for your policies. Is there a designated Policy Board?	
Do you foresee any dispute resolution mechanisms?	
Have you undertaken? Planned any cross certification with other CAs?	
Data protection, consumers and confidentiality	
What specific consumer protections do you apply in your project?	
What are the major data protection warranties you offer?	
What remains confidential? For how long?	

Conclusion

Out of your experience using standards for your project would you have any recommendations for the standards to which cards must comply with on the legal side?

General comments on the project and recommendations for the standardisation organisations (CEN/ISSS, ETSI)

Any other general recommendations or comments

References

[CEN/ISSS 02] Scherzer, H. (ed.), *Application interface for smart cards used as secure signature creation devices*, version 0.6, CEN/ISSS, WS E-Sign, Draft CWA, Group K, January 2002.

[EESSI 01] EESSI, *First Set of Deliverables*, http://www.ict.etsi.fr/eessi/ddd.doc

[ETSI 01] *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456, 2001.

[Eymeri 01] Eymeri, J., *The electronic identification of citizens and organisations in the European Union: State of Affairs*, 37th Meeting of the Directors-General of the Public Service of the Member States of the European Union, 26-27 November 2001, Bruges.

[Lei et al. 96] Lei L., Mitrakas A., A Multi disciplinary perspective for electronic commerce, in P. Swatman, J. Gricar, J. Novak, *Electronic commerce for trade efficiency and effectiveness*, 9th international conference on EDI-IOS, 10-12 June 1996, Moderna Organizacija, Kranj, 1996.

[TB1 02], Nilsson, H., Pohjolainen, M., *Requirements for European Public EID-card's Issuers, Supporting PKI and Certificate contents*, eEurope Smart Card Charter Trailblazer 2, January 2002.