Open Smart Card Infrastructure for Europe

v2

Volume 1: **Application white papers and market oriented background documents**

Part 1-3: **eGovernment white paper on smart card applications and evolution: Survey of Secure Smart Card based e-Government Applications**

Authors: **eESC TB10 eGovernment**

PKICUG PROJECT

Public Key Infrastructure for Closed User Groups

Survey of Secure Smart Card based e-Government Applications

Final report: 3AT 05032 AAAA DTZZA
Version Number: 04
BC Department, EDS Answare 2002

TABLE OF CONTENTS

REMARK - Limit of this study

This study has been supported by IDA European commission and was carried out in relation to TB10 objectives to evaluate Smart Cards based e-government actions and programmes.

- A questionnaire has been set up in accordance with TB10 in order to interview key administrations.
- A specific list of answers has been included in this report.

The conclusions and recommendations listed in this evaluation are still under evaluation and comments from TB10 and therefore, they are not definitive and will be updated by TB10 by the end of 2002.

EXECUTIVE SUMMARY

OBJECTIVES AND METHODOLOGY

This report deals with issues related to the survey of Smart Card based e-Government applications.

The goal of that study is to analyse the use of smart cards in G2G (government-to-government), G2B (government-to-business), G2C (government-to-citizens) applications and in e-Procurement for administrations.

The study proposed was led in collaboration with the e-Europe Smart Card Charter (Trail Blazer 10 on e-Government).

In particular, the objectives of the current study are to identify the main organisational, technical and legal issues for the smart cards used in the different European countries.

To reach these objectives, information was collected through a questionnaire sent to the Member States representatives, through complementary meetings with the Member States representatives.

The survey focused on the following elements:
- Existing projects and technologies;
- Security needs;
- Existing common actions and interoperable projects;
- Requirements for trans-border or trans-European interoperability;
- Implementation policies and success and failure factors;
- The use (benefits and options for use) of smart-cards;
- Users (citizens and enterprises, administrations).

OUTCOMES OF THE STUDY

A – GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS

Applications of smart cards in Europe

The main identified applications of smart cards are:

- Support of legally recognised electronic signatures;
- Authentication of authorised personnel (civil servants, health professionals…);
- Identification and authentication of companies by the administrations and public organisms;
- Citizen electronic identity cards;
- Social security identification of insured person;
- Local services (transport, leisure).

What difficulties were encountered within the projects?

The lack of equipment (card readers) of citizens and of small companies is an obstacle to G2C applications.

The configuration of workstations is often considered as not adequate, and most users feel the hardware too expensive for the benefits they expect from smart cards.

On the other hand, technology is felt not yet mature, hence solutions could have to change in the near future.

Furthermore, a kind of reluctance of some categories of users is noted and may outline the problem of changes of habits and in some cases a fear of more control by the administration.

In all cases, after a period of adaptation, the cards were well accepted.

Regarding the project deployment

The projects' coverage is wide and extends from millions of cards to pilots with a few hundreds. Among large systems, only a few are fully operational yet.

Many systems are presently under deployment and major difficulties have not yet been met .

Most systems are not inherited from a preceding one (this is however the case in a few applications) and upwards compatibility is then an important constraint of deployment (in particular technical aspects).

The responsiveness of companies varied according to the project.

What evolution is expected to take place for those smart card projects?

The expected evolution of smart card projects in Europe is believed to depend mainly on the application (standards supported, enrichment of contents, multi-application usage).

Concerning standards, the considered evolution mainly concerns electronic signature taking into account:

- A migration to a qualified certificate scheme;
- Supported algorithms (in particular signature and encryption where supported); and
- Support of XML signature.

In general, relaxing the usage for less demanding applications is not welcomed, but could however be accepted in very precise cases.

Management processes

The registration procedure widely depends on the applicant's profile and on the certificate class; persons are generally identified by reference to a registry of population, sometimes by reference to an alternate registry.

The personalisation of cards is preferably made by the internal services of the issuing authority (the Certification Authority, if there is a PKI), but may also be contracted to an external provider during busy periods.

The delivery process often involves a face-to-face appearance at a public desk (town administration, police station, post office…).

B – TECHNOLOGY USED

Dealing with available technology

Choice of smart card technology in projects was mainly based on:

- Availability in the market;
- Protection of secrets;
- Portability (may be used on any compatible workstation).

No credible competition is to be noticed for the moment and the only drawback identified with available technology was the cost of infrastructure (smart card reader).

About smart cards themselves

The major mentioned features of used smart cards are to:

- Contain identification information, application specific data (profile, rights…), possibly updateable, public key certificates,
- Support simple authentication of device and/or card holder, electronic signature, exchange of encryption keys;
- Create valid electronic signatures, including cryptographic features.

Regarding associated PKIs, when any

Smart card based systems do not always make use of a PKI, as the management of large PKIs is felt very complicated, the most important service there being a simple identification and electronic signature being mainly considered for subsets.

For some of the projects, cross certification with other CAs has been implemented. Nevertheless, European-wide cross certification is considered a complex problem that has to be dealt with at a political level

Client software side

For basic applications, mainly e-mail, the software modules exist and are integrated with the available software.

Regarding Secure Signature Creation Devices, these still have to be defined or implemented: specific tools already exist or are under validation.

Last, integration is generally felt easy. The wide availability of cryptographic libraries for the mostly used algorithms was quoted an asset.

C – LEGAL ASPECTS

Mentioned legal aspects of the projects

Two major legal aspects were mentioned:

- the protection of personal data, following the European Directive 97/66/EC and the related national legislation;
- the electronic signature, following the European Directive 1999/93/EC and the related national legislation.

Considering electronic signature, two approaches are being considered:

- either have a specific legislation to precisely define what electronic signature means;
- or the authorities consider that the general legislation is sufficient or almost sufficient, and that court decisions will define the rules.

For application specific systems, the particular legislation applies.

Considering digital signatures

Digital signature is widely considered a major reason for deploying smart cards.

In some MS, a private key associated with a qualified certificate is mandatory distributed in a secure container, hence in a smart card. Other MS prefer supporting simple advanced signatures before migrating to qualified certificates.

Let us mention that many Member States are taking specific provisions, regarding an agreement scheme for providers of qualified certificates.

For what regards certificate policies

In most cases, no specific policy board has yet been designated.

When a PKI is set up, CPS and CP are generally published. In most cases (but not all) the documents are written down on the basis of RFC 2527. For some projects, the CPS is considered to remain confidential

Data protection matters

Smart cards are considered as offering a better protection of personal data, as:

- information may be kept only electronically, which is better than a paper document;
- it is more difficult to forge.

In fact, data protection mainly depends on the protection of information kept on the master registers.

The laws on the protection of personal data fully apply both to these registers and to smart cards that contain personal data (because of the processing of those data by the card).

CONCLUSION

Some of the main e-Government applications areas based in the Member States were expected to be dealing with:

- E-procurement;
- Health care/ social security cards.
- Electronic citizen and civil servant identification card with e-sign features;

According to people met during this survey:

- Smart cards may not have to play a significant role for e-procurement applications roll-out in the next few years, due to the fact that such an application is not fundamentally associated with mobility of applicants; however, keeping secrets in a removable card is still a significant asset;
- The ability for users, whatever their Member State, to access their individual social security data everywhere across Europe will be a great advantage in future;
- Regarding the administrative co-operation between national European administrations, the identification and authentication of a civil servant by his colleagues from any other MS is also considered as highly interesting (e.g. Customs) ;
- The development of identification/authentication and e-sign facilities for individuals and civil servants across Europe is expected to broadly continue and requires that adopted means be universally recognised in Europe.

To summarise:

- The priority in the user profile for smart card technologies is clearly expected to be:
  - Citizens, as they are the most likely to be mobile;
  - Civil servants; and
  - Companies will also clearly find advantages in using such means.
- To allow smart cards to become fully pertinent as an open and mobile facility for users across Europe, this will require a harmonisation of the technical standards used, which is not the case today;
- It is recommended that MS agree also on harmonised contents for smart cards and associated usage policies (with or without PKIs).
- This would enable a minimum set of information data to be mapped from any MS Information System to another one; this may also require the definition and use of dedicated Object Identifiers.

1. SUBJECT AND STRUCTURE OF THE DOCUMENT

1.1. Context of the study

In 1999, the European Commission proposed the e-Europe initiative to accelerate the transition of the economy to the digital age. An important part of this initiative, e-Europe Smart Cards, is aimed at accelerating the uptake of digital technologies across Europe and ensuring that all Europeans have the necessary skills to use them.

When the e-Europe initiative was created, smart cards were set down as a specific action point on the list of items to be addressed. Those charged with implementing this action point convened a conference of experts to decide on what needed to be done to achieve the aims of e-Europe with respect to smart cards. The Smart Card Charter was born out of this conference.

It was decided to carry out a study about the usage of smart cards in the European countries. The work done aims at investigating the planned and existing applications between European Governments and/or between Member States Administrations, between Administrations and commercial companies and between Administrations and citizens.

This is the final report for this study and it examines the organisational, technical and legal issues involved in the usage of smart cards by the Member States' public administrations. This report summarises the results of the study and identifies potential obstacles and the major directions where the European Union could take advantage of smart card based techniques to establish a EU wide Administrative space.

EDS Answare visited and interviewed a series of Member States' representatives:

- Belgium;
- France;
- Italy;
- Spain;
- Sweden.

These interviews were conducted on the basis of an interview guide (see Annexe).

This guide was also sent to other Member States in order to collect their written feedback on the topic. EDS Answare received written answers from the following MS:

- Germany;
- United Kingdom;
- France;
- Finland.

Representatives contacted in Denmark, Ireland and Iceland answered by a simple statement that they did not have (or not yet) such applications.

The present report is a synthesis of the information collected in these interviews and written feedback.

The questionnaire has been prepared to support investigations and sent in advance to all identified interlocutors. This document was mainly oriented to help MS in their thoughts. This questionnaire is available in the Annex hereafter.

Its content was structured as follows:

- General environment and organisational aspects of the projects:
    - general issues;

  - difficulties;
  - project deployment;
  - transitions to come, under process or completed;
  - process;
  - archival;
  - suppliers;
- Technology used in the projects:
  - general issues;
  - smart card;
  - Public Key Infrastructure;
  - client side software;
- Legal aspects of the projects:
  - general issues;
  - digital signature;
  - CP/CPS (Particularly for e-Procurement);
  - data protection, consumers and confidentiality.

This study summarises in the next chapter the different views of the Member States.

1.2. Presentation of the report

The present document is the final report of the Secure Smart Card based e-Government applications study sub-project.

This report is divided into five main parts:

- Chapter 1 is this introduction;
- Chapter 2 lists applicable and reference documents;
- Chapter 3 gives acronyms used in the report;
- Chapter 4 gives a short description of the projects examined;
- Chapter 5 is a compilation of the answers given by the interlocutors contacted; it follows closely the outline of the questionnaire (see Annex I);
- Chapter 6 provides a synthesis and the conclusion for the study.

In addition:

- Annex I gives the questionnaire that has been communicated to interlocutors;
- Annex II contains the answers given back to our enquiry.

1.3. General statement

The present report is a synthesis and an interpretation of the information collected from many various interlocutors, each with his own view of a particular context. Hence, even in similar domains of application, the answers given were placed at different levels and in different directions.

Therefore, this report cannot be regarded as a coherent and validated vision of the usage of smart cards in e-government context. It rather reflects the very active evolution of that domain.

Most of our interlocutors insisted on the fact that their answers did not commit their administration or organisation.

2. APPLICABLE AND REFERENCE DOCUMENTS

2.1. Applicable Documents

[AD1] Call for Tender, Ref. DGIII/98/053 – PKI -801.01/01/PKICUG, issued 18 July 1998

[AD2] PKICUG, Public Key Infrastructure for Closed User Groups, ATA proposal, Ref. DCS/SXP/PRP/98/003, dated 1 September 1998

[AD3] Framework contract for informatics services in the context of the PKI project, n°501993, dated 23 December 1998

[AD4] Fax numbered ENTR.D.5/AM D(2001) 555674, dated December 12,2001

[AD5] Proposal BC.01-686/PR, date December 13, 2001

[AD6] Contract IDA.20010843, dated December 20, 2001

[AD7] Project Management and Quality Plan, Ref. 3AT 05032 AAAA UQZZA, version 03, dated February 26, 2002

2.2. Reference Documents

[RD1] Minutes of the kick-off meeting, dated January 14, 2002, Ref. BC.01-031/CR

[RD2] Minutes of the TB10 meeting, dated January 31, 2002, Ref. BC.02-068/CR

[RD3] Minutes of the progress meeting, dated March 25, 2002, Ref. BC.02-180/CR

3. ACRONYMS

BS	British Standard
CA	Certification Authority
CBT	Computer Based Training
CEN-CWA	Centre Européen de Normalisation (CEN Workshop Agreement)
CEPS	Common Electronic Purse Specifications
CNAM	Caisse Nationale d'Assurance Maladie
CNIL	Commission Nationale de l'Informatique et des Libertés
CP	Certificate Policy
CPAM	Caisse Primaire d'Assurance Maladie
CPS	Certificate Practice Statement
CSP	Certificate Service Provider
CUG	Closed User Group
(T-) DES	(Triple-) Data Encryption Standard
DG	Directorate General (Direction Générale)
DLL	Dynamic Link Library
EC	European Commission
EEPROM	Electrically Erasable Programmable Read-Only Memory
(E) ID	(Electronic) Identity Card
ETSI	European Telecommunications Standards Institute
EU	European Union
ICD	International Code Designator
ID	Identity
IDA	Interchange of Data between Administrations
IDENT	German IDENTification procedure
ISO	International Standards Organisation
ITSO	Integrated Transport Smart card Organisation
LRA	Local Registration Authority
MD-5	Message Digest – 5 algorithm
MS	Member State
OID	Object Identifier
PC	Personal Computer
PC/SC	PC Smart Card Workgroup

PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
Q&A	Questions and Answers
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest Shamir Alderman
RSS	Réseau Santé Social
SCC	Southampton City Council
SHA-1	Secure Hash Algorithm-1
SSCD	Secure Signature Creation Device

4. APPLICATIONS AND PROJECTS

This section is specifically devoted to a general description of the projects examined during the survey.

4.1. Projects identified

The following table gives a list of the projects that have been identified and contacted; not all of them answered. In most of these latter cases, we could collect information on web sites. However, accuracy of information collected on the web could not always be cross-verified with the issuing organisations.

MS	Project Name	Description/comments	Ans.
Austria	CITIZEN CARD (BÜRGERKARTE)	Common framework social security and other citizen identity cards	N
Belgium	BELPIC	BELgian Personal Identity Card for citizens and civil servants	Y
	SIS	Social security card	N
Finland	FINEID	Finnish identity cards	Y
	SATAKUNKA	Macro-pilot covering health and social security information.	N
	NORTH KARELIAN HOSPITAL DISTRICT	Management and exchange of health data (FINEID card used for authentication)	N
France	TITRE FONDATEUR	Common basis for electronic identity cards, potentially covering: personal identity card, driver licence, other specific cards	Y
	TELEPROCEDURES	Tax teleprocedures	Y
	SESAM VITALE	Identification of insured persons (social security)	Y
	GIP CPS	Health Professional Cards	Y
	ADEP	A group of small and mid-sized towns to test usage of e-procedures with the citizen and with the administrations	N
Germany	MEDIA@KOMM	Initiative for the development of e-procedures in townships and urban districts. The cities of Bremen, Nürnberg and Esslingen are pilots.	N
	Land of Baden-Württenberg	Multifunctional cards to citizen and public e-procurement	Y
	BESCHAFFUNGSAMT	e-procurement for administrations	Y
Ireland	PUBLIC SERVICES BROKER	Secure access to public services.	N
Italy	IEIC	Italian Electronic Identity Card	Y
	AES	Advanced Electronic Signature based on IEIC	Y
	MSC	Multi Services organisation Card based on IEIC	Y
Netherlands	PKI OVERHEID	Government PKI for civil servants	N

MS	Project Name	Description/comments	Ans.
Norway	-	Digital Signature	N
	-	Health project (under development)	N
	-	National betting system (under development)	N
Spain	national PKI	Usage of smart cards in public sector's PKI based applications: identification/authentication + e-sign for civil servants.	Y
Sweden	**id card**	Multipurpose identity card Internal use within the Administration : National Taxboard, Social Insurance Board	Y
U.K.	e-tendering	System to allow UK departments to exchange tendering information (pilot stage)	N
	dfee	Connections card: a scheme for 16-19 year olds in education, covering attendance monitoring, access to facilities, credits, etc.	N
	smartcities	Local services with the City of Southampton as first pilot	Y

4.2. Projects examined

4.2.1. Belgium

The project examined in Belgium was the electronic identity card, with several potential variants:

- civil servant card, for usage in administrative tasks (identification and authentication, signature of internal administrative documents),
- citizen electronic ID card.

4.2.2. Finland

All smart card based applications in Finland exploit the already widely spread out Finnish electronic ID card (FINEID). Here again, the civil servants are the first users of the cards.

Projects quoted by the FINEID agency were:

- the North Karelian Hospital District aims at establishing a network concerning healthcare allowing communication between healthcare professionals and citizens; it participates in a trans-European pilot with Greece and Germany;
- the Satakunta Regional District was selected for a pilot (macro-project) based on the Finnish ID card in the joint sectors of healthcare and of social security.

4.2.3. France

Three major domains were considered:

- the tax TELEPROCEDURES that aim at facilitating administrative procedures between companies (or individuals) and the tax administration. For the time being, the only operational part using smart cards concerns VAT declarations and possibly payment.

- the TITRE FONDATEUR project is centred around a common identification system to be the basis for the issuance of various identity cards with or without ability to electronically sign, with elected representatives and civil servants as priority users.
- the SESAM-VITALE card and the CPS card are designed to work together in the domain of healthcare and social insurance; the first one is used only to identify the insured person and to carry a few information on his/her rights, while the second one, reserved to health professionals, supports electronic signature for administrative purpose and protection of sensitive information.

4.2.4. Germany

Two very different projects were examined in Germany:

- the BESCHAFFUNGSAMT (procurement agency) of the Federal Ministry of Home Affairs aims at implementing qualified electronic signature throughout the whole life cycle of contractual relationship between administrations and providers.
- the LAND OF BADEN-WÜRTTENBERG is experimenting with smart cards for several usages such as car registration, requests for agricultural funding, applications in the department of Justice, the users being either civil servants, citizens or enterprises.

4.2.5. Italy

The projects considered in Italy were all based on the Italian electronic ID card project. The considered applications were the following:

- CIE: network access control throughout the territory, presently for a series of municipalities,
- sectoral administrative applications (Mandato Informatico di Pagamento, Libro Matricola Carabinieri, Protocollo informatico, Ruolo Unico dei Dirigenti,etc.), mostly for electronic signature with qualified certificates,
- multiservice cards for usage in administrations (Presidenza Consiglio Ministri, Ministero Beni Culturali, Ente Nazionale per l'Aviazione Civile) providing identification and authentication, support of qualified signatures, securing of e-mail exchanges.

4.2.6. Spain

In Spain, in the framework of their PKI services to administrations, the Fabrica Nacional de Moneda y Timbre (MINT) provides smart cards with PKI based certificates for identification and authentication and for electronic signature to several administrations.

Presently, the two major users are the Agencia Estatal de Administración Tributaria () and the Seguridad Social (Social Security).

In addition, there is a starting project for the creation of a national electronic ID card.

4.2.7. Sweden

The Swedish system for electronic identification cards is different from the other Member States in the sense that, after having agreed four private providers, any organisation, even outside the administrations, may request from these providers personalised smart cards that are accepted as official identity cards. In the e-

government domain, each agency or administration is free to request these cards with specific personalisation as required, such as additional data and/or certificates.

For civil servants, the major users of these cards in Sweden are the national taxboard and the social insurance board.

4.2.8. United Kingdom

Only one project was considered in the United Kingdom, namely local services based on smart cards in the city of Southampton. That project is the first pilot of the Smartcities initiative, that joins several towns throughout Europe with many partners as providers.

5. OUTCOME OF THE SURVEY

This chapter describes the usage of smart cards in an e-Government context (on the basis of the interview guide given in Annex) for the following issues:

- the general environment and organisational aspects of the projects in the MS;
- the technology used in the projects;
- the legal aspects of the projects.

5.1. General environment and organisational aspects of the projects

5.1.1. General

This section describes existing and planned projects or applications associated with the smart card between European Governments and/or between Member States Administrations, between Administrations and commercial companies, and between Administrations and citizens.

5.1.1.1. Applications using smart cards

See paragraph 4.2 above

5.1.1.2. Role of the smart cards

The role of the smart card in the Finnish projects includes authentication, email encryption and signing. The main task is to educate the users.

In France, for the "TITRE FONDATEUR", the smart card plays a central role to identify and authenticate the holder on many occasions in his/her personal and professional life.

For "SESAM-VITALE", the smart card is used for the identification of the insured person (beneficiaries of reimbursement may be other members of the family).

The CPS cards distributed by the GIP-CPS are used to authenticate the health professional in important steps of his daily work; in particular, the CPS card is required to allow usage of the information contained in the SESAM-VITALE cards.

In the TELEPROCEDURES project, usage of smart cards is optional and aims at providing better protection for the private key it contains. In addition, the Ministry of Finance do not mind people using the card for other electronic signatures.

In Germany, the role of the smart card in the "BESCHAFFUNGSAMT" project focuses on the replacement of the hand-written signature under precise conditions.

In the Land of Baden-Württenberg, the role of the smart card is mainly for identification and authentication, with support of confidential e-mail.

In Sweden, the card is used as an electronic identity, as a carrier for private keys and optionally as a visual identity card.

In UK, the objective is to provide cardholders with one card to access a number of different services.

For certain applications, the card can be used simply for its flash value (concessionary fares), for others like the PKI application the card is used to hold digital certificates and private keys.

5.1.1.3. Multi-purpose cards

In case of a multi-purposes card, the card can offer different options in common to several applications such as a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications.

In Finland, the card is a vehicle for carrying the public key pairs and certificates.

In France, for the "TITRE FONDATEUR", the card allows the identification and authentication of persons, including ability to sign electronically, plus a basic set of access rights. In addition, the TELEPROCEDURES project is considering accepting citizen ID cards for authentication of tax declarations, just as they presently accept their own cards for authentication of companies.

For "SESAM-VITALE", the card is presently considered for the storage of basic health information.

In Sweden, the card offers common identification data and a specific certificate for electronic signatures (non repudiation).

In UK, the card has a common content area: this includes name address, post code & date of birth.

Following a trial of the CEPS E-purse and provided that a high street bank becomes involved the e-purse would be common to a number of different application providers.

5.1.1.4. Who are the card holders?

In Belgium and in Finland, cardholders are potentially any citizen; for the time being, civil servants are the major proportion of cardholders.

Government information unit is responsible for building a generic authentication scheme based on a PKI. This service doesn't include services for the citizen and is produced in co-operation with service providers.

For the French "TITRE FONDATEUR", the French Administration will manage the master registry, based on the book maintained in each town.

The master registry will identify and authenticate each person. The local town halls will continue being the first access point.

For "SESAM-VITALE", any person insured by a Social Security organism in France is a cardholder; a next development will be to hand a card not only to insured persons but to all beneficiaries (for instance to the children from 16 years).

The "SESAM-VITALE" members are the card issuers who are responsible for the issuance of the card to cardholders.

Social security and associated complementary organisms provide update of the data stored in the cards through interactive terminals (borne "SESAM-VITALE").

For GIP-CPS cards, the cardholders are strictly validated health professionals; the registration process is strictly controlled by professional organisations (ordre des médecins, ordre des pharmaciens, etc.) and assessed by the administration.

For the time being, the TELEPROCEDURES project delivers smart cards only to companies; however, there is always a person identified as responsible for holding the card.

In Germany, the cardholders for the "BESCHAFFUNGSAMT" project are staff members of the awarding institution and staff members of a company as tenderer.

Card issuer(s) are all trust centres, who supply qualified digital signatures according to the signature regulations.

In Sweden, the cardholder is always a physical person as an individual or as a representative of an organisation or an employee within one Government agency.

Card issuers are vendors within the PKI market through framework agreements (The Swedish Post, TELIA, NORDEA and INTEGRIS).

Most common card supplier to those vendors are SETEC. Card readers may some times come through the common PC vendors.

In UK, the cardholders are individuals who have an interest in one or many of the applications on the card.

Card issuance is currently carried out by both Southampton City Council (SCC) and the University of Southampton.

The issuance policy/authentication framework has been created by SCC and endorsed by the wider consortium.

The service providers are and will be a mix of private and public organisations. Access providers – currently the infrastructure is provided by the application providers themselves.

In the event that a common e-purse is developed it is likely that this is managed and maintain by the bank or its clearing provider.

The organisational model of different entities for card issuers, service providers, access providers is still being worked on in Southampton.

It is likely that some form of Joint venture company will result following the completion of the EC funded project.

5.1.1.5. Reasons for choosing smart cards solutions

The rationale for using smart card concerns mostly security and privacy.

In Belgium, technology, security, privacy and friendliness were the rationale for using smart cards.

In Finland, the rationale for developing the national electronic ID-scheme is to provide sufficient level of security and privacy to develop governmental online services.

The smart card is used in France for the "TITRE FONDATEUR" because the support is already familiar to most people.

For "SESAM-VITALE", at the time where the choice was made, there were no real concurrent solutions.

Moreover, smart cards allow updating of the contents (in particular the details of rights) through the interactive terminals.

In Germany, the Land of Baden-Württenberg aims to provide e-services for citizen and enterprises to increase the speed and acceptance and to reduce the costs.

The use of smart cards in the "BESCHAFFUNGSAMT" project reflects an obligatory requirement of the German law on public tendering and contracts.

Security and privacy are the elements identified in Italy. Security, privacy and technology were identified in Spain.

In Italy, for the electronic identification card, the rationale for using smart card is security and privacy.

For the advanced signatures with qualified certificates, the rationale for using smart card is security.

The Italian norm states that in order to achieve the requirements for an advanced signatures with Qualified Certificates, the smart card has to meet the ITSEC E3 level.

So the choice of smart card is due to an accurate analysis.

In Spain, security, privacy and technology were identified as reason for using the smart card. User friendliness was not a reason.

In Sweden, security and the possibility for electronic signatures were the given answer with the objective to make the administration of identities easier.

In UK, in the first instance the project was set up to explore what the potential for a smart card in a multi-owner multi-application scheme might be.

Already it has become clear that with effort existing barcode, magnetic stripe and ID cards can be converted to be used with a smart card.

This reduces the need to carry multiple cards. The use of the card for authentication and using full PKI provides excellent security.

Simply introducing a smart card is innovative and has seen increased interest in certain application areas.

Using the card on the toll bridge and for e-purse is very user friendly and much easier than previous methods. For use in schools and on buses there is a reduction in the stigma associated with concessions. Bullying in schools is also reduced.

5.1.1.6. Process for choosing a smart card

The choice of smart card was done at once or through a project analysis.

In Belgium, a study was conducted by a private company (CSC) to analyse the choice of the electronic identity card.

In Finland, the choice was done through analysis. Generic authentication scheme for inter-government use has been established to build up a project because there is no single product available on the market.

In France, the choice was done through analysis – however there was no serious alternative.

In Germany, this was a cabinet decision on the basis of the results of workshops, several working groups and committees.

In Italy, the choice was the result of a careful analysis.

Analysis was also conducted in Italy.

In Spain, the smart card technology was chosen by an expert group to support the services provided by FNMT, according to a Master Plan conducted in 1997.

In UK, the choice was done through project analysis and some previous assumptions.

5.1.1.7. Business model

The question of the business model supported was not always clear for the Member States so the answers are really different. Basically in this domain there is little difference in the business models because the costs are carried in general by Government. Also there is little consideration on business cases. Governments just consider smart cards are a means to enhance services to the citizens and are less concerned about return on investments.

The business model supported in Belgium concerns production and distribution of EID, communication between citizens, government and other partners.

The answer obtained from Finland is that at the moment government funding is the main source of funding for the electronic identity card.

The question of business model was not understood by the French partners.

In Germany, there is a special business model per application.

In Italy for the advanced signatures with Qualified Certificates, there is not a business model because Centro Tecnico acts as a promoter for the dissemination of electronic signatures without charges for Italian Administrations.

In Sweden, there are several business models. Most frequent pay for smart card and some kind of cost for using the smart cards (yearly or transaction based).

The question of business model was not understood by UK.

5.1.1.8. Motives for deploying smart cards

The main motives for deploying smart cards can be political, economical, educational …

In Belgium, it was a decision of the Council of Ministers in November 2000 to ensure e-communication between citizens and government through certificates (EID).

In Finland, the motives were economical and tutorial. The objective was to cut down on the costs of government information gathering and the administration wanted to set an example.

In France, for the "TITRE FONDATEUR", the project is a significant part of the e-government requirements.

For "SESAM-VITALE", it was basically a political decision taken at the highest governmental level (Prime Minister). It works in close connection with the GIP-CPS programme, that was already running since years. SESAM-VITALE was actually a major starter for the wide deployment of GIP-CPS cards as these latter are mandatory to exploit VITALE cards.

The TELEPROCEDURES project is another political choice taken at governmental level. The objective is that any tax payer, either individual or company, could eventually be able to undertake most administrative procedures with the tax administration.

In Germany, the main motives were to reduce costs, to improve the administrational abilities of the state and to meet expectations of citizens.

For the electronic identification card in Italy, the administration wants to set example.

For the advanced signatures with qualified certificates, the main motive for deploying it is political.

In Spain, the main motive given was economical.

In UK, the following motives were given: improving services to the customer, social benefits, political benefits linked to being considered innovative and therefore attracting inward investment, financial savings and reliable digital ids for customers. The e-Envoy governmental agency published a general framework document, but leaves each administration free to choose the best solution for their own usage.

5.1.1.9. Stakeholders and driving forces

To the question about the major stakeholders or driving force behind the projects, the general answer is a governmental initiative.

Governmental decisions are the major driving force for Belgium, Finland.

The French government and in particular the Ministry of Home Affairs is behind the project "TITRE FONDATEUR".

Social security organisms with a wide support of insured persons are the major stakeholders of the "SESAM-VITALE" project and, in a large part for the GIP-CPS as well. After a period of reluctance, this latter is now widely supported by health professionals.

The smart cards projects in Germany are mainly driven by the Federal Ministry of the Interior, the Federal Ministry for Economic and Technology, the Procurement Agency of the Federal Ministry of Interior, Federal Office for Building and Regional Planning.

Central government (Ministry of Innovation and Technology) and local government (Municipalities) are behind the project of electronic identification card in Italy.

In Spain, several Ministries were the initiating/driving force to develop usage of smart cards: Ministry of Economy, Ministry of Finance, Ministry of Science and Technology, and Ministry of home Affairs.

In Sweden, means of electronic identification and electronic signatures is a must for the administration to be able to offer interesting services to the public and to be able to communicate in a secure way with each other.

In UK, the usage of smart cards is supported by the governmental agency for e-government activities, named eEnvoy. However, each project has its driving force. in the case of the SCC project, the major stakeholders are Southampton city council, Southampton University and SCHLUMBERGER SEMA, working in the more general framework of the Smartcities initiative, a European level group of towns and of companies.

5.1.1.10. Geographical scope

The geographical scope of the projects is in general national.

That is the case in Belgium, Finland, Italy, Spain, Sweden.

For the "TITRE FONDATEUR" in France, the whole French territory is concerned and later, when accepted and technically assessed, partner countries.

For "SESAM-VITALE" and GIP-CPS the project concerns any person insured by the members and any health professional equipped with the relevant hardware and software – practically the whole French territory.

The TELEPROCEDURES project concerns any company paying taxes in France, for the time being, it is working mainly on VAT declarations.

In Germany, for the multifunctional cards to citizen, the geographical scope is the region of Baden-Württenberg.

Contrary, the e-procurement project geographical scope ("BESCHAFFUNGSAMT") is EU wide.

In UK, the geographical scope concerns city focused leading to a regional developments.

5.1.1.11. Target audience

In Belgium and Italy, the target audience for the projects is the citizen, with a particular focus on civil servants.

In Finland and France, citizens and companies are concerned; here again civil servants are a priority target.

In Germany, companies, citizen and administration are the target audience.

In Spain, the applications considered concern only civil servants.

In Sweden, two different target audiences were identified: the first group is individuals (citizen) and organisations representatives (probably mainly soft certificates but some smart cards) and the second group is civil servants (mainly smart card based certificates).

In UK, citizens of Southampton are the target audience.

5.1.1.12. Interoperability

For the representatives met, interoperability with other systems did not seem a priority concern. Very generally, project managers focus on the feasibility of their own system before thinking of interconnecting it with other systems, in particular with foreign systems.

About interoperability, the project of "TITRE-FONDATEUR" in France does not consider interoperability of the project with other projects using other smart cards.

However, the card might be used to create electronic signatures.

For "SESAM-VITALE", there are presently two experiments with foreign partner organisations. The scope will remain social security. The cards are used in conjunction with GIP-CPS cards, but this is not a real interoperability.

For German e-procurement, the development of a possible digital identification card is stated as being already taken into account.

In Sweden, they consider interoperability because there are several different vendors/supplier and they consider interoperability with smart cards already issued by vendors such as the Swedish Post and TELIA.

For UK, interoperability is key to the success of not just their project but to the long term viability of smart card schemes generally.

Interoperability needs to be considered from a number of different angles:

- Do you want interoperability between applications? (Transport yes, library perhaps not)
- Is interoperability affected by physical distance?
- Will you issue all cards with the same applications or will you allow all applications to be loaded on to a predefined standard card ?

SmartCities is currently investigating this with a number of cities throughout Europe. This group is known as the SmartCities Interest.

5.1.1.13. Details on business models

In Germany, the procurement agency (Beschaffungsamt) will act as unique application service provider. A detailed business model is on its way and will be presented in approximately 2 months.

Only Sweden provided details on their business model. Each project buys personalised smart cards from four selected providers who have a PKI infrastructure.

The Swedish buys this as a holistic solution and as a service not as products.

The objective is to pay for the certificates or usage of certificates to individuals or organisations' representatives to get a critical volume to make it interesting for the administration to offer and set up e-services.

5.1.2. Difficulties

5.1.2.1. Critical obstacles

The obstacles identified were technical, managerial, economic and human.

For Belgium, not every citizen has the required technology at home for readers and there have to be products for which the EID can be used.

The obstacle for Finland is that technology is not yet ripe.

For the French "TITRE FONDATEUR" project, management is considered an important issue.

For "SESAM-VITALE", there was no critical obstacle – the project has required a long preparation but finally it has been fully and easily accepted.

In contrast, the GIP-CPS project needed a long time before health professionals could be convinced that the proposed applications – in particular social security reimbursement – were beneficial for them. The cost of the required equipment, i.e. adapted software and specific devices with a double card reader, was an obstacle there.

The TELEPROCEDURES project was not compulsory, i.e. companies are free to continue making paper declarations instead. However, most are now using the electronic declaration that is felt easy and money saving.

For Germany, the technology is not felt easy to implement.

The legal requests seem to be exaggerated, so that no easy to use interface for the citizen is possible.

Identification and authentication is possible with an accuracy of only 70%, but 98% is necessary.

Another problem encountered is that only personal signatures are possible but "agency signatures" and "computer generated signatures" are needed too.

Finally, for life event automisation we need a signature card that allows a batch-like processing of a series of e-services after one authentication only.

Today, the citizen has to enter his PIN code for each of the various e-services.

For e-procurement, critical mentioned obstacles are missing interoperability, no structures in other MS.

For Italy, for the electronic identification card, management can be an obstacle.

For the advanced signatures with qualified certificates in Italy, there have been human, deployment and interoperability problems.

In Spain, interoperability and difficulty for the citizen to acquire smart card readers are obstacles.

Earlier in Sweden, there have been some examples where deployment of smart cards to the public for electronic identification and signatures led to a lot of questions to the support/helpdesk, mainly because of the client software and card readers.

The answer from the UK did not identify obstacles butsuggestions.

These suggestions are the following:

- get the user requirement right,
- focus on needs of the people,
- do not under estimate the resource implications and staff training,
- developf an authentication framework,

- authentication levels must be linked to what the card is being used for,
- cards with photo & name have intrinsic ID value,
- cards should look the same social inclusion,
- scalable technical solution,
- remember that technology is changing,
- integrate the smart card into the wider e-government strategy,
- benefits are not necessarily financial.

5.1.2.2. Impact of standards

During the project, new standards can have an impact on the way of working (end users, central application), the co-operation with software companies can vary/be more or less responsive.

In Belgium, the tender still has to be made public. The software companies are responsive.

In Finland, smart card solutions are felt not compatible - readers, drivers and software do not operate trustfully. Moreover, too much knowledge is assumed from the user.

PKI has not yet proved to be a successful business. Software companies are not investing enough on development.

In France, the project of "TITRE FONDATEUR" is still in the preliminary phase so no feedback information is available.

For the "SESAM-VITALE" project, the most important change concerns the way of working – the transmission of the document ("feuille de soins") to the reimbursement centre is not done by the insured person any more but electronically by the health professional.

This procedure shortens the delay in reimbursement.

The most difficult part was to have the system accepted by health professionals.

Customer pressure of was strong and they finally discovered that the new procedures did not add so much work for them.

In Germany, e-procurement is developed from proprietary development. Easy handling was an important criterion for the development

In Italy, for the advanced signatures with Qualified Certificates, there have been many impacts, particularly the interaction between applications and smart card technology.

About co-operation with software companies, there have been some difficulties because of conservative behaviour of some companies and also because of the complexity of the project itself due to the lack of a leading project.

The software companies were not always responsive.

In Spain, they have two classes of certificates and two drivers (one for Microsoft® Windows, one for Apple®). They did not have particular problems with software companies.

In UK, they tried to develop the card so that customers/cardholders use it in an identical or at the very least a similar way to before.

They have adapted an existing department to accommodate the new requirements of the smart card scheme and they expect that department to either grow or merge in line with the scheme.

They have worked well with their commercial partners but they suggest that a single contract is drawn up with the lead partner who is then responsible for the others.

The software companies were responsive when required.

5.1.2.3. Acceptance of smart cards by the users

In France, for the "SESAM-VITALE" and TELEPROCEDURE projects, users were already familiar with smart cards, if only because of bank cards.

The final result of the whole operation was simplification of the procedure and fewer delays – it was very well accepted.

In Germany, the user does not consider the smart card as a token to make things easy.

For e-procurement, easy handling was an important part of the development.

In Italy, the smart card was not accepted easily for the electronic identification card.

For the advanced signatures with Qualified Certificates, the smart card plays a good role in matters of acceptance/friendliness.

For Southampton City Council in UK, the smart card was clearly an evolution from existing accepted card-based schemes and not a revolution.

5.1.2.4. Smart cards as support for privacy

To the question if the usage of smart cards was felt as a support for respect of private information, Belgium has a positive answer.

The cardholder can consult his government held personal data using his personal electronic identity.

In France, for the project "TITRE FONDATEUR", the CNIL (Commission Nationale Informatique et Liberté), responsible for the respect of private information, strongly supports the project that is felt a better protection.

Only a very reduced set of information will appear printed on the card, while extra info recorded in the card will be available only to accredited authorised persons (under the control of their own professional card).

This will be significantly more confidential than the present card.

For the "SESAM-VITALE" project, the usage of smart cards was not particularly felt as a support for respect of private information.

That is not yet the case in Germany.

In Italy and in UK, the usage of smart cards was felt as a support for respect of private information.

5.1.2.5. Alternative technologies considered

Alternative technologies or processes could be used or envisaged as enablers during the meantime.

The general feeling was "what else"?

In Belgium, they have sites like those in Ghent, Bruges, Seneffe. A person can ask for his file and get a copy of his "population file" with his own national identity number.

In Finland ("FINEID"), they are considering at the moment the identification used by banks as an alternative enabler of strong identification and authentication. System is based on changing passwords and already used by about 40% of the population.

In Germany, alternatives are passport services and smart card solutions on a legal basis.

No alternative technology or process used or envisaged as enablers are considered at the moment in Italy.

5.1.3. Project Deployment

5.1.3.1. Size and current status of the projects

The size of the smart card project (number of cards …) is variable. Only a few applications are fully operational (Finland, France).

In Belgium, the potential number of cards is ten million. In the initial phase, the number is 330.000 in eleven municipalities. The project is to be deployed over a five year period. The tender (card and CA) still has to be published.

In Finland, the national electronic identity card was launched in December 1999. Both the governmental and private certification authorities have had problems in marketing their card to general public. The governmental certification authority has issued 14.000 cards and the private authority 700 cards. The smart cards are in use but it has not become the mainstream authentication method. Revaluation of the business model has started.

In France, the project of "TITRE FONDATEUR" represents a potential of 60 million French citizens. The project is still on study.

For "SESAM-VITALE", more than 40 million cards were delivered at the moment and an extra 5 million expected in the near future. The project is fully operational.

For GIP-CPS, 100 000 cards were delivered to health professionals since 10 years.

The French "TELEPROCEDURES" project is conducted by the MINEFI (French Finance Ministry) and addresses long term most of French companies. Providers agreement is under control of the MINEFI: more than 10 providers are today referenced.

In Germany, 1000 cards were delivered in Baden-Württenberg. There are several projects – some are in final acceptance test and some are still to be evaluated.

Three million of smart cards will be delivered before 2003 in Italy for the electronic identification card and then 8/10 million a year. That is the phase 2 of the project. Phase 1 represented 150.000 smart cards that is now completed.

For the advanced signatures with Qualified Certificates, it is planned to deliver about 30.000 smart cards. 3.000 smart cards have been delivered.

In Spain, the project is running/operational for the first users, more particularly in national administrations. The project of national ID card concerns millions of potential users.

In Sweden, they hope that the entire Swedish population will get PKI-based means for electronic identification and signatures.

The highest volumes will probably be soft certificates but some will be smart card based.

There are currently about 160.000 PKI-based smart cards with a general set of data for identification and electronic signatures.

These are not yet used by all Government agencies in their e-services but they will be.

They hope that the number of Government agencies using smart cards within the agencies will grow.

There are currently two large agencies using PKI-based smart cards (about 30.000 cards).

They know that several more are currently setting up PKIs based on smart cards.

There are a couple of agencies using not PKI-based smart cards.

The projects task is to get PKI-based smart cards and other PKI services available for the Government agencies and make them use these services. 1.000 cards were issued in UK. From April to September, at least a further 10.000 cards are planned.

The first demos are completed. This focused on the technical ability of the card to support multiple applications. The next stage is to grow this with additional applications.

5.1.3.2. Origin of projects

First, it must be noted that everywhere where smart cards are used for access control, either to computers or to premises, the system replaces an existing one, based on other technologies (login/password, PIN code, card with magnetic tape, etc.)

In Belgium, example has been taken from the SIS card. In France, Italy, Spain, Sweden and UK the projects are not directly rolled over from a pre-existing one. However, some already have an old story with smart cards (for instance GIP-CPS in France).

In Germany, projects are usually rolled over from a pre-existing one.

5.1.3.3. Targeted phases of deployment

About the targeted phases of deployment, an evaluation will occur in Belgium after a six month period of tests (pilot project) in the 11 municipalities.

The significant problems encountered concern the adaptation of the infrastructure in the 11 municipalities and the National Register.

This is the initial phase so it is too early to tell about reaching its goals.

In Finland, for the "FINEID" project they encountered problems with technology. The project did not reach its goals because the number of smart cards used is not sufficient to encourage new services to be built.

France is not facing significant problems for the project "SESAM-VITALE". They did not encounter significant problems. The project is fully deployed and is considered to be reaching its goals.

Only functional extensions are considered – the next one for May 2002 and these are relatively minor changes.

The targeted phases of deployment are unknown for the project “TITRE FONDATEUR”.

In Germany, the PC configuration of the user is often not adequate. The costs for the cards and card readers are much too high. The critical mass of applications is not in sight. The project has partially reached its goals.

For the electronic identification card in Italy, the targeted phases of deployment are in two phases: phase 2 with 3 million cards and phase 3 with 8 to 30 million of smart cards in the next years.

The significant problems encountered concern the interoperability of cards of different vendors but the project has reached its goals.

For the project of advanced signatures with Qualified Certificates, they plan to distribute about 10,000 smart cards during the current year.

They can feel the need of continuous adjustments of the project and they feel they have not reached their goals yet.

For the e-procurement project, the scheduled phases are the following:

- development of the necessary functional concepts;
- development of the necessary data handling technical concepts;
- technical implementation of the concepts;
- testing phase;
- pilot phase;
- actual operation.

In Sweden, the choice they have made is on the certificate format and key usage, which are the same regardless of soft stored certificates or keys stored on smart cards.

The targeted phases of deployment were the following:

- set up a strategy in September 2000;
- requirements for framework agreements ready in March 2001;
- evaluation of offered solutions and vendors ready in November 2001;
- co ordinate purchases from framework agreements is an ongoing phase.

The project has not reached its goals because the goal is to get a widespread use of PKI within the Government agencies and for individuals' use towards the Governments agencies.

In UK, the targeted phases of deployment were the following: April-September 2000 10,000 cards for loyalty and authentication application, September 2000 cards for school pilots, September-December 6/8000 cards for toll bridge application.

The significant problems encountered were generally issues surrounding the changes in the service delivery rather than the technical issues.

Technical issues were still prevalent. The project has reached its goals but is behind the original schedule.

5.1.3.4. Cost elements

Most generally, the only well known costing element is the unitary cost of a card. Estimations significantly vary from a system to another, as the answers do not always take the same system components into account.

In Belgium, the major cost drivers identified are infrastructure and cards.

The cost of the usage of smart cards was not perceived as high. The cost of the EID and two certificates is estimated at 9 Euro.

In Finland ("FINEID"), maintaining directory services and revocation lists for such a small amount of users is not considered as cost effective.

In the future, the maintenance of revocation lists and directories should be charged from service providers. The cost of the usage of smart cards is perceived as high.

The citizens find the cost high since they have to purchase the card readers and software even though there are not very many services available. The cost is high for government.

In France the cost have not been yet evaluated for the project "TITRE FONDATEUR". The cost drivers are still to be evaluated for the project. The usage of smart cards is not perceived as high compared to the expected benefits.

For "SESAM-VITALE", the cost of the usage of smart cards is not perceived as high. The unit cost of a personalised smart card is estimated 2.30 Euro. The breakdown elements to evaluate the cost of the project are not available.

In Germany, the cost drivers in their project are the smart card support. The cost of the usage of smart cards is perceived as too high. The choice was made anyway because there was no other credible alternative.

In Italy ("CIE"), the cost of smart cards, and the cost of the management infrastructure are considered as the cost drivers.

The cost of the usage of smart cards is perceived as high. That choice was made anyway to gain enough security in network transactions.

The cost for the citizen for a single smart card is estimated at 25 Euro.

For the advanced signatures with qualified certificates, financial law is the cost driver in the project. The cost of the usage of smart cards is perceived as a justified cost.

In Spain, the cost of the card is estimated at 13 Euro for a small project. The price is expected to decrease for larger projects.

In Sweden, the elements identified as cost drivers in the project are the following:

- smart cards and software needed on the client side including electronic signatures;
- cost of registration of people applying;
- cost of availability; and
- services (support/helpdesk, revocation service, directories…).

The costs of the usage of smart cards are perceived as high in comparison with other techniques such as soft certificates.

About the breakdown elements to evaluate the cost of the project, they have a price list from each vendor.

Included in the cost however are the cost of identifying the prospective cardholder and distribution, support and helpdesk. They choose vendors/CA depending of the total cost and degree of requirements they could meet.

Hardware, software, human resources, both managerial and technical, wide geographical distribution of project partners are the cost drivers in the project in UK.

The cost of cards themselves is high and it is not just a perception. The choice of smart cards was made anyway because the project was tasked to establish what the benefits might be if there were any so it was clear that there were risks.

About breakdown elements to evaluate the cost of the project, they are working on a number of different models but they are commercial and in confidence.

5.1.4. Transitions to come, under process or completed

Belgium does not have an answer about new standards or infrastructures they are considering for the near future and midterm.

They consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified certificates).

As new services to their existing application, Belgium is considering the opening of the central database to the public so that everybody can consult his/her file.

In principle, they consider re-using the same smart cards for others applications. The smart card can be used for each application driven by the identity of the user.

Last, they would accept relaxing the usage of the smart cards to less demanding requirements. They do not consider changing the topology of the organisation (from local to global, from centralised to decentralised…) because it is already decentralised.

In Finland ("FINEID"), they consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive but the fact is that actual advanced signatures are not needed in government transaction in many cases.

Most of the time strong enough authentication is what we need. They consider re-using the same smart cards for others applications.

They would accept relaxing the usage of the smart cards to less demanding requirements.

For the project "TITRE FONDATEUR" in France, all the questions were felt irrelevant as the project is still under study.

For the project "SESAM-VITALE", new standards or infrastructures are not considered for the near future and midterm because a major change would be very expensive.

They certainly do not consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive.

They do not consider re-using the same smart cards for additional applications.

In Germany, Land of Basen-Württenberg only use qualified signatures. They consider re-using the same smart cards for others applications because this is necessary to get acceptance.

They would accept relaxing the usage of the smart cards to less demanding requirements but that is not the problem and it does not give the critical mass.

Depending on the application, they consider changing the topology of the organisation.

For the project of electronic identification card in Italy, they are considering the Directive 1999/93/EC for electronic signature and ISO 7816 for smart card.

They consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive.

New services based on the network access are considered in their existing application. They consider re-using the same smart cards for others applications.

They accept relaxing the usage of the smart cards to less demanding requirements.

It is mandatory to change the organisation of back office and front office to supply and manage the data for network application.

Benefits expected from that change are efficiency of the service to citizens, economy of the public service and possibility to move employees from front office to back office.

For advanced signatures with Qualified Certificates, new standards or infrastructures are not considered for the near future and midterm.

They are compliant with the art. 5.1 of the Directive. Client authentication, personal identification and e-mail protection are considered as new services for their existing application.

They have planned to use the same smart card for others applications but only when the memory size will be sufficient for their scope.

They would not accept relaxing the usage of the smart cards to less demanding requirements.

For the time being, they do not consider changing the topology of the organisation.

For e-procurement, it must be noted that the project "Öffentlicher Eink@uf Online" (Public Procurement online) defines new standards and will in further developments adjust to changes of technologies and regulations on contracting

In Spain, new mask to be created to support ISO v.2 standard is considered as new standard for the near future.

They consider re-using the same smart cards for others applications. At the moment, they cannot accept relaxing the usage of the smart cards to less demanding requirements.

They might consider changing the topology of the organisation. Today, the model is a centralised PKI. If the generation of keys evolved to take place on the smart card, this might lead them to adopt a decentralised model.

Flexibility is expected from that change.

In Sweden, they do not consider so many new standards or infrastructures for the near future.

One considered is XML signatures. Sooner or later, they will consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive.

The smart card is only intended for carrying the electronic identity and the possibility for electronic signatures (main reason for PKI).

Since the identity is totally unique and identifies the holder to anyone, it can be used for everything requiring that the card holder identifies him or herself.

They would not accept relaxing the usage of the smart cards to less demanding requirements with two exceptions.

There are however exceptions, for instance within an administration personalisation could include putting a magnetic stripe on the card for passing through doors, etc.

One other exception could be as a token for symmetric cryptography (file encryption) or application specific authentication (could be for example windows log on).

In UK, CEPS/a number of CEN standards, ITSO, Java (open platform) are considered as new standards for the near future.

They have made some tentative explorations in the direction of a migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive.

Their point of departure for data has been the UK Electronic Communications Act 2000.

They are looking at adding a number of other applications to the scheme.

These include ferries, the local football club, electronic voting, etc. They consider changing the topology of the organisation but not specifically linked to the emerging smart card scheme.

5.1.5. Process

5.1.5.1. Smart card personalisation and delivery

In Belgium, personalisation agents and registration Authority agents have to know the procedures of the population registers that are maintained by each municipality.

They also have to learn to use the new software. Training sessions when one takes delivery of the new card and leaflets explaining how the card can be used at home are provided as support efforts to the end user. The user reaction and feedback to the project is not yet known.

The smart card personalisation & delivery process is the following: the data are personalised outside, the chip contains three pairs of keys (third pair for identification of the card).

When a person needs a new ID card, he/she makes an appointment with the population service of the municipality where his/her identity is checked and where the process of delivery of the new card is completed.

In France, for the project "TITRE FONDATEUR", the unique interlocutor for citizens is the town hall.

The request is then forwarded to the Préfecture, which controls the manufacturing process (personalisation).

The card is then returned to the Town Hall where it is handed to the holder.

In other cases, in particular for civil servants and for elected representatives, other Administrations may be the right authority.

For the registration process, whatever the card is requested, the process always begins with the "TITRE-FONDATEUR" procedure that amounts to establish the authentication data of the person.

It is done only once for each person and then re-used for each request for a new card.

There is no central directory of the population.

The "état civil" books remain the basis of the identity of persons.

The data of the "TITRE-FONDATEUR" are kept by the Administration (Préfecture) to support further creation of other cards and for renewal of existing cards.

For the "SESAM-VITALE" project, the smart card is generated by "SESAM-VITALE" upon request of one of its members (usually the CNAM) when rights appear. The requesting organisation delivers the card, usually by registered post.

The GIP CPS personalises their smart cards and delivers them directly to the end users.

In the French "TELEPROCEDURES" project, the use of smart card is only optional and is to be considered by the end user himself. The registration procedure is defined and implemented by each agreed supplier.

In Germany, the Land of Baden-Wüttenberg use the IDENT-procedure of their provider SignTrust for the smart card personalisation and delivery process and for the registration process.

For the "BESCHAFFUNGSAMT" project, the smart card can be purchased by the user from any trusted centre empowered to distribute qualified certificates. In Italy, for the electronic identification card, the personalisation is in charge of organisations that implement security standards similar to (but not so high as) Visa standards.

The Municipality is in charge of delivery .

For the advanced signatures with Qualified Certificates, the smart card personalisation & delivery process is the following: generation of keys inside the card, production of PKCS#10 (certificate request), PKCS#12 treatment, external personalisation, deliver to the final user.

For the registration process, the Italian norm requires that personal identification must be performed by the presentation of identity documents and the submission of an appropriate request form.

In Spain, the registration process consists of two steps: issuance of a certificate request and face-to-face appearance to the RA.

In Sweden, the person applying for a smart card visits the CA/RA or RA appointed by the CA and identifies himself by an accepted mean of identification (ID CARD, passport, Drivers licence).

The RA sends the information necessary to the CA or card issuing company.

When the card is issued, the activation code (PIN) will be sent to the cardholder's official address (from the population register) and the card will be sent by registered post.

This means that the cardholder has to identify him/herself in order to get the card.

In UK, application forms are collected from a number of different locations around the city (this includes both private and public areas).

Completed application forms are taken with the associated documentation to a number of registration locations throughout the city.

These include all libraries and 9 of the 11 housing offices as well as a couple of central offices and the Smartcities bureau itself.

Applicants are expected to take a photo with them but in some offices it is possible to take digital photos instead.

Once the application form has been checked the individual retains his/her personal documents and the completed form is sent to the Smartcities bureau for the card to be created.

In Italy, for the advanced signatures with Qualified Certificates, the Italian norms consider the role of qualified and authorised intermediates that can carry out the work needed for the registration process.

These intermediates are trained by the Centro Tecnico. In every case, the Registration Authority is centralised.

The support efforts for the end user are the following: documentation (reference manual, CBT, public available documents and software), Call centre and electronic message.

Every useful document is available on the Centro Tecnico website `http://www.ctrupa.it` and every user has his own reference manual and CBT.

They have no direct feedback but they are certain of a good reaction because they did not receive any particular claim.

In Spain, the training requirements for personalisation agents and registration Authority agents is constituted by MS Office general knowledge.

To support efforts for the end user, six persons are in the end-user departments and six persons are in a dedicated Call Centre.

Word and PDF documentation are available to the end-user.

The user reaction and feedback to the project is generally fine. The number of questions per week is very low and essentially focused on the smart card, on the version of the software, etc.

In Sweden, the idea of buying the PKI as a service is that the vendor/CA is responsible for support to the cardholder.

In UK, they have given staff specific training on how to accept an application for a SmartCities card.

This has been backed up with comprehensive procedures.

Most of the staff involved have previous experience in dealing with application forms and the registering of customers.

Telephone hotline, website Q & A, face to face customer enquiry desk are support efforts for the end user.

They provide a smart book, a brochure on the services and extensive information on website.

To date the feedback has been very positive. Some individuals have expressed concerns with the Big Brother issue but none of these have been cardholders.

5.1.5.2. Organisation and responsibilities

Each time that the smart card is associated with a PKI, roles and responsibilities are described in one (or several) Certificate Policies published by the Certification Authority. When there is no PKI, equivalent texts are in general published by the service provider.

In Belgium, the organisation and responsibilities for the parties were all taken into account at the beginning by mentioning them in the tender document.

New issues (during the project) are not yet known.

They do not have a published liability scheme yet.

This will happen in the future (CPS in the tender).

In France, for the "TITRE FONDATEUR", the organisation and responsibilities for the parties were taken into account when precisely defining the project.

They do not have a published liability scheme yet. The commitments of each category of partners are the usual commitments concerning official documents.

The TELEPROCEDURES project has set up a series of committing requirements that each agreed provider has to comply with. These requirements are both organisational (under the form of a master CP) and technical (interoperability test bed).

In Italy, for the advanced signatures with Qualified Certificates, the organisation and responsibilities for the parties were all taken into account at the beginning.

This project has been well analysed in respect of specific requirements.

They have taken into consideration other possible uses.

They do not have a published liability scheme but they are working on this perspective.

In UK, the partners have their own public liability insurance schemes.

The draft Certificates Policy includes a liability scheme.

5.1.6. Archival

The question of archival was everywhere understood as concerning time stamping services.

In Belgium, there are some time stamping requirements for the project. They are described in the tender.

In France, for the "TITRE FONDATEUR", in Germany, in UK there are not any retention requirements for documents and there are not any time stamping requirements for the project.

In Germany, for the e-procurement project, there is a retention period of 10 years for contract file including all tenders. In addition, a time-stamping requirement is stated regarding the submission of tenders by the tenderer in due-date time.

In Italy, for the advanced signatures with Qualified Certificates, there are some retention requirements for documents and there are some time stamping requirements for the project.

In Sweden, the time stamping requirements for the project were based on PKIX but no vendor could support a time stamp. Time stamping was however never a requirement of any application based on the Swedish ID cards.

They will develop an offer when there are enough requests.

5.1.7. Suppliers

Belgium can use a single or multiple suppliers for smart cards and they can have a single or multiple suppliers for their PKI.

In Finland ("FINEID"), in Italy (advanced signatures with Qualified Certificates), in UK they use a single supplier for smart cards and they have a single supplier for their PKI.

In France, for "TITRE FONDATEUR", the Home Affairs Administration will be the unique supplier of personalised cards.

It has not been determined yet whether all citizen cards would be supported by a PKI.

The only case where a PKI is found necessary is where electronic signature is expected to be a major feature of the project, in particular civil servants and elected representatives.

In these cases, the PKI would be managed by the relevant Administration.

Entrusting the PKI of an identity card seems difficult (problems linked with the usage of false cards or of stolen cards…).

For citizens, in the case where electronic signature would be found useful, no decision on the organisation of a PKI has been taken yet.

The Ministry of Finance, in particular, is waiting for decisions to decide whether they will extend their PKI-based services for TELEPROCEDURES to individuals.

By definition, SESAM-VITALE and GIP-CPS are providers of personalised cards on behalf of various organisations. In general they buy the blank cards from several providers.

The French "TELEPROCEDURES" project is conducted by the MINEFI (French Finance Ministry) and in the long term addresses most French companies.

Important points to mention for this project are as follows:

- MINEFI outlined a standard Certification Policy;
- a strict providers agreement procedure has been defined and put in place;
- use of the smart card is only optional and is to be evaluated by the end user himself;
- the Registration Procedure is defined and implemented by agreed suppliers;
- A few more than 10 providers are today referenced by MINEFI;
- Companies use this service to notify directly the amount of taxes paid (e.g. VAT).

In Germany, the Land of Baden-Württenberg uses a single supplier for smart cards and a single supplier for their PKI: SignTrust (Deutsche Post).

For the e-procurement project, all trust centres who supply qualified digital signatures according to the signature regulations are suppliers for smart cards.

In Spain, they use a single supplier for smart cards today.

They have a single supplier (Entrust) for their PKI. According to them, one supplier for certification technology with smart cards is not sufficient because the risk is to be tied up with one single provider.

In Sweden, the vendor/CA are responsible.

In practice, there are two card suppliers to their vendors: SETEC and one more. They have six different CAs although there are two to three different technical solutions.

5.2. Technology used in the projects

5.2.1. General

5.2.1.1. Technologies considered

Different technologies have been considered in the projects. Arguments in favour/against a smart card were presented.

In Belgium, an argument against a smart card is that only 25% of the population is connected to Internet.

In Finland ("FINEID"), the argument in favour is security because no better alternative can be found at the moment. The argument against a smart card is that technology is not ripe yet.

In France, for "TITRE FONDATEUR", the technology is not yet decided.

It should however shortly be running smart card systems ("SESAM-VITALE", bank cards …).

There is no credible alternative to smart cards. Among the data stored in the card there will be biometric elements: electronic images of the hand-written signature, of the fingerprint and photograph of the face.

Among these three data, only the photo will be printed on the card.

For "SESAM-VITALE", at the time of the decision, only one available technology was considered mature enough (Bull CP8).

Each healthcare professional is free to choose a hardware and/or software provider of products compliant to a precise specification published by the "SESAM-VITALE".

Access is provided by the RSS network, completely separated from the management of cards. Service providers are members of "SESAM-VITALE".

For "TELEPROCEDURES", the card is recommended for a better protection but remains optional.

In Germany, the Land of Baden-Württenberg rely on the technology provided by SignTrust.

The e-procurement project accepts usage of any card delivered by an authorised provider; they developed specific software components for their application.

In Italy, for the advanced signatures with Qualified Certificates, technologies considered in the project have been PKI based.

Arguments in favour are the robustness, the portability and the potential multiple uses.

In Spain, standard smart cards related technologies have been considered.

The arguments in favour a smart card are security and portability. The argument against is the availability of smart card readers because citizens do not have smart card readers.

In Sweden, soft certificates (pairs) and smart card based certificates have been considered in the project.

A smart card is considered secure but expensive and difficult to deploy to the public.

In UK, the following technologies have been considered in the project: PKI, Smart card-Java, J2EE, CRM, HTTPS, XML, SSL, HTTP.

The arguments in favour of smart cards are processing power, portability, easy of use, security. An argument against the smart card is the cost of infrastructure (readers).

5.2.2. Smart card features

The main features of the smart card in Belgium are the following: eye readability of the information on the inside because the ID card is a valid travel document in the EU, a chip with 3 key pairs (two of them correspond to an identity certificate).

The smart card supports a single application.

The cryptographic features of the smart card in the project are the use of RSA.

The PKI related content of the smart card are root certificate, identity certificate and signature certificate.

The exact role of the card in the signing process is to ensure that one signs as a physical person.

Authentication certificate is used as an authentication mechanism.

Eye format readability is another form factor involved. The smart card is compliant with international security standards.

The use of RSA contributed to the choice of smart card technology chosen in their project.

The main features of the smart card readers are the following: harmonised European standards and acceptance of national equivalent standards in the other 14 EU countries.

In Belgium, example has been taken from the SIS card. The SIS card is only a memory card, not an intelligent card. It is better not to have changeable information on it (not up-to-date) (on the contrary, the French SESAM-VITALE card, that is another passive card, allows updating information through specific interactive terminals – see below).

The main features of the smart card in France ("TITRE-FONDATEUR") are the following: storage of information and in some case support of electronic signature keys and certificates.

The PKI related content of the smart card is to be defined. The exact role of the card in the signing process is the authentication of the holder (provision of the key).

Authentication mechanisms are to be defined. The smart card will probably be compliant with international security standards; it has to be defined.

The choice of smart card technology chosen in their project has still to be defined.

The main features of the smart card readers depend on the usage. The police are experimenting two-reader devices that would allow them to read the information without having to enter the holder's private secret (pin code or other).

The main features of the smart card in France ("SESAM-VITALE") is the storage of information.

The smart card supports a single application card. The smart card in the project does not have cryptographic features.

All readers are potentially input-output devices, but used only in read mode, except the interactive terminals intended for update, located in a limited series of places (usually CNAM/CPAM offices).

The main features of the smart card and the smart card readers in Germany (Beden-Württenberg) are defined by SignTrust.

As regards the e-procurement project, its related smart card features focus mainly on qualified digital signature, the main role of the card being the replacement of the hand-written signature on valid tenders submitted by the tenderer.

This card is also a digital service card and supports other applications, which require digital signatures.

For this project, only smart card readers class 3 are be used because of security reasons. There is a list of compliant products published by the federal regulatory administration for telecoms and the post (Regulierungsbehörde für Telekommunikationen und Post).

In Italy, for the electronic identification card, the card is a SSCD in the sense of Directive 1999/93/EC.

The smart card is compliant with international security standards.

For the advanced signatures with Qualified Certificates, the card performs advanced cryptographic functions.

The smart card supports other applications. The cryptographic features of the smart card in their project are the following: RSA Keys generation, RSA for Signature/Verification and Encryption/Decryption – SHA-1 & MD5 for hashing functions.

Private and public keys, X.509 certificate are the PKI related content of the smart card. The smart card is used for signing the hash of the electronic document.

The authentication mechanism is PIN.

No other form factors are involved. The smart card is compliant with international security standards.

Durability, security and portability were the criteria for choosing the smart card technology.

Interoperability is the main feature of the smart card readers.

The main features of the smart card in Spain are the following:

- RSA keys, 1024 bits long keys,
- SHA-1, DES-3 and proprietary confidentiality mechanisms
- 32 Kb EEPROM – not all the memory is used – FAT 3 KB.

The smart card supports a multi application.

The PKI related content of the smart card is the following: two mandatory certificates and one optional for administrations, for Class 1 certificates – 15 data.

In the signature process, smartcard is used to create the signature itself. Verification and hashing are external.

RSA is used as authentication mechanism.

The smart card is compliant with international security standards (PC/SC and ISO 7816).

Durability, Power, Security are the criteria for choosing the smart card technology chosen in their project. The main features of the smart card readers are the following: PC/SC compliant, for Social Security they have old SC readers (short buffers), National Id Card as a project.

The main features of the smart card in Sweden are the following: authentication/key encipherment certificate and private key, non repudiation certificate and private key, optionally visual ID.

Electronic identification and electronic signatures are supported by the smart card where applicable..

The cryptographic features of the smart card in the project are RSA 1024 bits. The chip is protected according to ITSEC class E4.

The PKI related content of the smart card can be described as follows: PKCS#15 cards with two X.509 version 3 certificates format according to RFC 2459 and private keys (authentication and key encipherment, non repudiation).

The exact role of the card in the signing process is a carrier of the non repudiation private key.

Authentication mechanisms used are primarily client authenticated SSL (class3), sometimes authentication based on server side SSL(class 2) and specific authentication through some kind of challenge response depending on client and sometimes server software.

In UK, for the SCC project, the cryptographic features of the smart card in the project include DES, T-DES, RSA and SHA-1 Microsoft Cryptographic Service Provider.

The application relevant to PKI will be used to authenticate citizens for secure electronic government services using Web certificates.

About the exact role of the card in the signing process, as part of the handshake between the authentication server and the smart card, the card will create a digital signature by producing a one-way hash from data generated randomly during the handshake and known only to the card and the server.

This will be encrypted with the cardholder's private key and sent to the authentication server together with the cardholder's certificate containing his or her public key.

The authentication server checks that the user's digital signature (the hash signed with the cardholder's private key) can be validated with the public key in the cardholder's certificate transmitted with the digital signature i.e. decrypted and the hash values compared.

The authentication mechanisms described before and X509 v3 Digital certificate are used.

The smart card is compliant with international security standards.

The criteria for choosing the smart card technology were led by SCHLUMBERGER SEMA who is a leading card manufacturer.

Card readers must be PC/SC compliant.

5.2.3. Public Key Infrastructure

The issuance of the certificates is outsourced in Belgium. Interoperability with other PKIs is a requirement of the tender.

The user registration requirements for certificate registration are done via the population registers.

The standards used for the card and the readers are European standards.

In France, for the project "TITRE FONDATEUR", most generally the PKI is not determined yet so the following answers are very general directions.

The issuance of the certificates should probably be managed in house.

The user registration requirements for certificate registration are supported by the TITRE FONDATEUR procedure.

The standards used in their project are to be defined.

For "SESAM-VITALE", all that section about PKI is not relevant to the application.

In Germany, about the issuance of the certificates, the Land of Baden-Württenberg uses the IDENT-process of SignTrust and the German Postal Service.

Interoperability with other PKIs has not been considered. The user certificate registration requirements are managed by SignTrust.

For e-procurement, the issuance of certificates is managed by the trust centres.

In Italy for the advanced signatures with Qualified Certificates, they manage the issuance of the certificates in house.

Interoperability with other PKIs has been considered. About the user registration requirements for certificate registration, they register only public employees belonging to Administrations connected to RUPA (Unified Public Administration Network).

The standards used in their project are X.509v3 for certificate format, PKCS#7 for digital signatures, RSA for keys, SHA-1 for hash, Triple DES for encryption.

In Spain, FNMT is the PKI operator; interoperability with other PKIs is under consideration. The registration orocess includes the presence of the requestor at the Registration Authority. All relevant standards are taken in consideration.

In Sweden, the issuance of the certificates is outsourced.

The standards used in their project are the following: requirements based on ETSI QCP to find minimum level for certificate policy, RFC 2459 (soft and smart card based) for interoperability for certificate format, PKCS#7 (soft and smart card based) for signature, PKCS#15 for card.

In UK, the issuance of the certificates is in house.

Interoperability with other PKIs has been considered but no actual work has been done yet.

The user registration requirements for certificate registration are the same as smart card. The standards used in their project are the following: X509v3 for certificates, LDAP for directory services, PKCS#10 and 7 for certificate request and return, also standards already listed.

5.2.4. Client side software

In Belgium, the smart cards are not used in the project used with Secure Signature Creation Devices because no products are available.

PC/SC plugin in the browser are the software requirements on the client side.

For the project “TITRE FONDATEUR” in France, the smart cards are used in some cases (civil servant, elected representative) in the project used with Secure Signature Creation Devices.

The software requirements on the client side are to be defined, it should be chosen for compliance with the smart card requirements. The general technology requirements of the project are to be defined.

In Germany, for the Land of Baden, Württenberg, all these aspects are managed by SignTrust.

For the e-procurement project, a signed Java-Applet was developed which supports the tenderer by submitting his tender.

The tender itself is in PDF format. The self-sign Plug-in from Adobe 5.0 was replaced by a proprietary developed Plug In thus PDF-documents can be validly signed by qualified digital signatures.

Software requirements on the client side are: standard PC, Windows NT or 2000, smart card and card reader.

In Italy, for the advanced signatures with Qualified Certificates, the smart cards are used in the project used with Secure Signature Creation Devices.

About the software requirements on the client side, cryptographic libraries must be compliant to the standards.

In Sweden, there are always some requirements of access control of the private keys regardless of it is about authentication or electronic signature and if stored soft or in a smart card.

This requires some kind of client software or other technique (Java applet CBT). The card requires some kind of CSP (cryptographic service provider).

About software requirements on the client side, they require that the certificate holder always types his/her password or pin to activate a private key.

In UK, on the client side, the smart cards are not used in the project used with Secure Signature Creation Devices.

The software requirements on the client side are Microsoft Cryptographic Service provider DLL, PC/SC Card Reader drivers.

5.3. Legal aspects of the projects

5.3.1. General

Concerning the legal requirements that were considered in the project in Belgium, a legal basis is required: the law concerning the registers of population and the identity card had to be modified.

In Germany, the legal requirements considered in the e-procurement project are related to the Code for Awarding Public Services Contracts, Freelance Performance and Public Works Contracts.

In Finland, the legal requirements for the electronic identity card are the electronic signature directive, the law on government electronic services in Finland (was developed simultaneously with the ID CARD), privacy legislation.

In France, for the “TITRE FONDATEUR”, the legal requirements that were considered in the project are the legislation on equivalent paper documents. Specific texts will probably be necessary (to be considered).

For "SESAM-VITALE", the French regulation of social security fully applies – the deployment of cards has been explicitly requested by the Government.

In Italy, for the advanced signatures with Qualified Certificates, they act in compliance with the legal requirements, particularly the Italian law.

In Spain, there is a series of laws and of decrees on the organisation of administrative work, including provisions on the usage of Information Technology.

In UK, the legal requirements that were considered in the project were primarily liability, the Data Protection Act and the privacy issues.

5.3.2. Digital signature

The project in Belgium supports electronic signatures in the meaning of Directive 99/93 on electronic signatures.

Qualified certificates will be put on the card.

Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172 will be established as soon as possible.

Their PKI has not yet taken into account any accreditation schemes.

It could in the future be imposed by Belgian law to support the highest requirements.

An independent technical audit is planned by a private consulting company. About an insurance policy for the project, the State is in principle its own insurer.

The liability of the Government is of 2,500 Euro per transaction.

In Finland ("FINEID"), the project supports electronic signatures in the meaning of Directive 99/93 on electronic signatures.

About plans to roll out qualified certificates, both governmental and private certification authorities are planning to produce qualified certificates.

Both schemes have gone through BS 7799 audit.

In France, for the project "TITRE FONDATEUR", the project supports electronic signatures in the meaning of Directive 99/93 on electronic signatures.

About plans to roll out qualified certificates, it is not sure that the certificates distributed will be qualified ones, except for civil servants.

Accreditation schemes are to be defined.

An insurance policy for the project is to be defined. Probably not as the only liability is that the card was personalised from verified information and according to written procedures.

In case of loss or theft, the holder is responsible for revoking the card i.e. the corresponding public key certificate.

For "SESAM-VITALE", all that section is not relevant to the application.

The German legislation on electronic signature is strongly related with qualified certificates; therefore, the organisation of PKIs in Germany is organised in two "worlds".

- A strict hierarchy with a PCA (Policy CA) as its root, to distribute qualified certificates. According to the legislation on electronic signature, only the CAs certified by the PCA are allowed to create valid qualified certificates;

  The concerned Certification Authorities may be for public servants, for representatives of companies and for individuals, as soon as they need to electronically sign documents;

  The certificates are mandatory stored into smart cards (or into any equivalent secure container);

- the rest of PKIs distributing non qualified certificates; the partners work with these certificates on a simple conventional basis; they may for instance create enhanced but not qualified signatures.

For the time being, the two "worlds" are not interconnected.

In accordance with the European Directive on electronic signature, qualified certificates are handed only to persons. In the opinion of the German Administration, it should be possible to create certificates for companies or organisations.

For the case of qualified certificates, the legislation enforces precise liability provisions.

For the electronic identification card in Italy, they support the art. 5.1.

They have plans to roll out qualified certificates and to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.

Their PKI has taken into account some accreditation schemes and they have accomplished an audit of their project.

The risks covered by the insurance policy are in charge of Central and Local Governments where applicable.

In Spain, the smart cards distributed allow creation of electronic signatures within the meaning of the European Directive.

In Sweden, the project supports advanced electronic signatures. Qualified certificates will come in the future.

In UK, they don't have plans to roll out qualified certificates or to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.

They are looking to become T Scheme compliant at a later date.

They have accomplished an internal audit of the project. About an insurance policy, there is the existing Southampton City Council public liability insurance.

5.3.3. CP/CPS

They do not have a designated Policy Board and no approval procedures for the project in Belgium.

They foresee some dispute resolution mechanisms – the EID Committee being before a mediator. Until now, they have not planned any cross certification with other CAs.

In Finland ("FINEID"), all the following elements are available: subscriber agreement, relying party agreement, consumer policy, privacy policy.

There is not yet a designated Policy Board.

In France, for the project "TITRE FONDATEUR", the main features of their CP/CPS are to be defined. Subscriber agreement, relying party agreement, consumer policy, privacy policy are to be defined.

A designated Policy Board, dispute resolution mechanisms, some cross certification with other CAs are to be defined.

For "SESAM-VITALE", all that section is not relevant to the application.

The GIP-CPS define and publish their own Certificate Policies. There are actually three such policies, one for servers, one for authentication and electronic signature, and one for confidentiality.

For the TELEPROCEDURES project, each agreed provider defines its own CP and CPS; however, the Ministry of Finance publishes a minimum model (PC type) each provider must conform to.

In Germany, the entire awarding procedure - from determination of requirement to awarding and contract processing - is available for the e-procurement project.

In Italy, for the advanced signatures with Qualified Certificates, their CPS is available on the Web `http://www.ctrupa.it`.

The following elements are available: subscriber agreement, relying party agreement and privacy policy.

There is not a designated Policy Board, any dispute resolution mechanisms. They tested the cross certification with other Italian CAs.

In Spain, the Consejo Superior de Informática act as Policy Board.

In Sweden, the requirements on content of their CP/CPS are ETSI QCP (although no requirements on the structure).

It is more common to have a RFC 2527 structure. Different vendor has different CP/CPS.

About subscriber agreement, relying party agreement, consumer policy and private policy, every vendor has its own but they did put requirements on content and some of these issues are regulated in the framework agreements.

They have not yet planned any cross certification with other CAs but there might be in the future.

In UK, the main features of their CP/CPS are based around RFC 2527.

Subscriber agreement and relying party agreement are made available.

Internal IS Board and legal services are also available.

They do not foresee any dispute resolution mechanisms at this stage.

Existing SCC dispute resolution procedures will be used. They have not officially planned any cross certification with other CAs but they have aspirations in this area.

5.3.4. Data protection, consumers and confidentiality

About specific consumer protections that apply in the project in Belgium, the consumer has an authentication signature certificate.

The major data protection warranties that they offer are not changeable. Private keys remain confidential for five years.

In France, for the project "TITRE FONDATEUR", specific consumer protections that apply in their project is the general legislation on protection of private data.

The major data protection warranties are to be defined if any.

Details about what remains confidential are to be defined.

For "SESAM-VITALE", specific consumer protections that apply in their project is the general legislation on privacy of data.

The interactive terminals in particular allow the card holder to consult/verify the information contained in the card.

Except with the interactive terminals that are located in particular offices, the cards may be read only under the control of a health professional card (bi-reader devices).

For Germany, data privacy is a complex subject that cannot be handled through a questionnaire.

For e-procurement, the tender remains confidential during the tendering period. Thereafter tenders are confidentially evaluated by technical and organisational methods.

In Italy, for the advanced signatures with Qualified Certificates, they grant the confidentiality of the personal information of the users according with the Italian law.

In Spain, they apply the legislation on protection of personal data, i.e. the Law 15/1999 and the associated Royal Decree 994/1999.

In UK, data protection procedures apply in their project.

Information on purposes for which personal data are collected is available on-line, by telephone and by written request.

Information is anonymised prior to cross application/organisation analysis.

Information is encrypted in data warehouse.

Terms and conditions of use give assurances on cardholder protection in so far as they agree not to load any applications on the card without the consent of the cardholder.

SCC has public liability insurance.

They are obliged by law to comply with the Data Protection Act.

Warranties are not required.

It is a requirement of the Data Protection Act that personal information is kept confidential from those not authorised to process it.

Personal data must only be kept as long as is necessary for the purpose for which it is required so it's confidential for as long as it is kept.

The Certificate Policy defines the information that is considered confidential in respect of the PKI and the retention periods for this information.

6. CONCLUSION

On the basis of the survey, smart cards are generally felt as:

- sensibly standardised;
- secure;
- really personal;
- portable;
- already familiar to users;
- largely able to be customised;
- widely offered on the market;
- without credible competition.

As regards strategy, most initiative is left to each project.

An evolution towards some more co-ordination is recommended, in particular on identification.

The recent evolution to more coherence is mainly due to the electronic signature – whether using qualified certificates or not. A movement towards qualified signature has clearly started, however it does not seem a priority in all countries.

The question raised is how to relate the card with a proof of identity of the holder?

As a consequence, a common basis for identity is requested with various cards. This seems to be of major importance for the European domain, as almost all Member States either already have or have definite plans in that direction.

Typical examples of this are the French "TITRE FONDATEUR" and the Swedish system.

In France, the basic registry is held by each local authority (Etat Civil); the necessary identification information of the TITRE FONDATEUR should then be collected and maintained by the territorial administration (préfecture), and the cards should be created from that information by the various competent Administrations.

In the Swedish system, the identity of persons is based on the unique registry of population maintained since centuries by the National Taxboard, the cards are defined by various organisations and the certificates are signed by various CAs.

That requirement for a unique identifier is relaxed by privacy protection. Indeed, in several Member States, the uniqueness of identifiers is considered a threat to freedom and, for instance in France, the social security identifier cannot be the same as a possible personal identity code (if any, what is not the case). This should result in each person, group or organisation having a few different identifiers, each of which must unambiguously be associated with that person, group or organisation.

Some other open issues about smart cards are as follows:

- General purpose cards versus dedicated cards
- What must be the contents of a card?
  - Only identification/authentication data?
  - Application specific data?
- How many certificates?
  - Two key pairs? Which usage?
  - Three key pairs?
  - Extra key pairs?

Some of the main based e-Government applications areas in the Member States were expected to be dealing with:

- E-procurement;
- Health care/ social security cards.
- Electronic citizen and civil servant identification card with e-sign features;

According to people met during this survey:

- smart cards may not have to play a significant role for the roll-out of e-procurement applications in the next few years, due to the fact that such an application is not fundamentally associated with mobility of applicants; however, keeping the secrets in a removable card is still a significant asset;
- the ability for users, whatever their Member State be, to have access to their individual social security data everywhere across Europe will be a great advantage in future; other similar European-wide usage has not yet been identified;
- as regards the administrative co-operation between national European administrations, the identification and authentication of a civil servant by his colleagues from any other MS is also considered highly interesting (e.g. Customs);
- the development of identification/authentication and e-sign means for individuals and civil servants across Europe is expected to broadly continue and adopted means should be universally recognised in Europe.

To conclude:

- the priority in user profile for smart cards technologies is clearly expected to be:
  1. Citizens, as they are the most likely to be mobile;
  2. Civil servants; and
  3. Companies will also clearly find advantages in using such a means.
- to allow smart cards to become fully relevant as an open and mobile means for users across Europe, this will require a harmonisation of used technical standards, what is not the case today;
- it is recommended that MS agree also on harmonised contents for smart cards and associated usage policies (with or without PKIs).
- this would enable a minimum set of information data to be mapped from any MS Information System to another one; this may also require the definition and use of dedicated Object Identifiers.

END OF DOCUMENT

ANNEX I: QUESTIONNAIRE

A - GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

What is/are the application(s) in your project that is/are associated with the smart card?

Will the smart card be a single or multi purposes one? In case of a multi-purposes card, what are they?

What is the role of the smart card in your project?

In case of a multi-purposes card, what will the card offer in common to several applications? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications…?

In your project, who will act as:

> Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer?
>
> Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders …?
>
> Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications?
>
> Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)

In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared?

What is the rationale for using smart card (technology, security, privacy, friendliness, etc)?

Was this chosen at once or through analysis / project analysis?

What is the business model supported?

Could you prioritise the main motives for deploying it? (political, economical, tutorial, the administration to set the example, etc)

Who is/are the major stakeholders or driving force behind the project?

How would you best describe the geographical scope of your smart card project?

What is your target audience?

Do you consider inter-operability of your project with other projects using other smart cards? If yes, how do you deal with this issue?

Please give details on elements of your business model.

Difficulties

What were the critical obstacles to choose using smart cards (example: management, human aspects…)?

During the project:

What were the impacts of the new standards on the way of working (end users, central application)?

How was the cooperation with software companies?

Were the software companies responsive?

What role did the smart card play in matters of acceptance/friendliness?

Was usage of smart cards felt as a support for respect of private information?

Alternative technologies or processes used or envisaged as enablers, during the meantime? If so, how did you organise the transition to full-wedged electronic transactions?

Project Deployment

What is the size of your smart card project (number of cards …)?

What is the current status of the project?

Is your present project rolled over from a pre-existing one?

If so, briefly describe your experience from such pre-existing project.

What are the targeted phases of deployment?

What significant problems did you encounter?

Has the project reached its goals?

What are the cost drivers in your projects?

Is the cost of the usage of smart cards perceived as high?

If that is the case, why did you decide to make that choice anyway?

Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution…)?

Transitions to come, under process or completed

Which new standards or infrastructures are you considering for the near future and midterm?

Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates)?

Which new services are considered in your existing application?

Do you consider re-using the same smart cards for additional applications?

Can you accept relaxing the usage of the smartcards to less demanding requirements?

Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised…)?

Which benefits are you expecting from that change?

Process

Please describe the smart card personalization & delivery process.

Please describe the registration process.

What have been the training requirements for personalisation agents and Registration Authority agents?

Please describe your support efforts for the end user.

Please describe any documentation you might make available to the end user.

What has been the user reaction and feedback to your project?

Were the organisation and responsibilities for the parties all taken into account at the beginning? How?

Which new issues did you discover (during the project)?

Do you have a published liability scheme?

What are the commitments of each category of partners?

Archival

Are there any retention requirements for documents in this project?

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 (if any)?

B - TECHNOLOGY USED IN THE PROJECTS

General

What technologies have been considered in the project?

What were the arguments in favour/against a smart card?

Smart card

What are the main features of the smart card?

Does your Smart Card support other applications or is it a single application card?

What are the cryptographic features of the smart card in your project?

What is the PKI related content of your smart card?

If the smart card is used for electronic signing, what is the exact role of the card in the signing process?

What authentication mechanisms are used?

Are there any other form factors involved?

Is the smart card compliant with international security standards?

What were the criteria for choosing the smart card technology that was chosen in your project? (durability, power, security, etc.)

What are the main features of the smart card readers?

Public Key Infrastructure

Do you manage the issuance of the certificates in house or do you outsource it?

Has interoperability with other PKIs been considered? Particularly for e-Procurement?

What are the user registration requirements for certificate registration?

What are the standards used in your project and for which specific purpose?

Client side software

Are the smart cards used in your project used with Secure Signature Creation Devices?

What are the software requirements on the client side?

Briefly describe the general technology requirements of your project.

C - LEGAL ASPECTS OF THE PROJECTS

General

Could you describe the legal requirements that were considered in your project?

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 Secure Signature Creation Devices 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.

CP / CPS (Particularly for e-Procurement)

Could you describe the main features of your CP / CPS?

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?

END OF THE QUESTIONNAIRE

ANNEX II: ANSWERS RECEIVED

The following table summarises the organisations and persons who provided us with information, either:

- in a face-to-face meeting (M); or
- by phone contact (P); or
- by a filled in questionnaire sent back by e-mail (Q).

In some cases, our correspondents forwarded back information collected from other persons. We give here only the name of our direct contact.

MS	Project	Organisation	Contacts	Ans.
BE	BELPIC	FEDICT Ministry of Home Affairs	Mr. Ben SMEETS Prof. Geert DE SOET Mr. Erik VANZUUREN Mr. M. Luc VANNESTE	M
FI	FINEID	FINEID TAC representative	Mr. Terho ARJA Mr. Seppo RIIHIMAKI	Q
FR	TITRE FONDATEUR	Ministry of Home Affairs	Mr. Michel AUBOUIN	M
FR	TELEPROCEDURES	Ministry of Finance	Mr. Jean-Louis FERRACCI Mr. CARREL	M
FR	SESAM-VITALE	SESAM-VITALE	Mr. Dominique BARRET	P
FR	GIP-CPS	GIP-CPS	Mr. Gilles TAÏB	P
DE	Land of Baden-Württenberg	TAC representative	Mr. Georg SCHÄFER	Q
DE	E-procurement	Beschaffungsamt	Ms. Monika ELSCHNER	Q
IT	IEIC/AES/MSC	CT-RUPA	Mr. Mario TERRANOVA Mr. Ubaldo BUSSOTTI Mr. Adriano ROSSI	M
ES	ID CARD	Ministry of Public Administration / CSI MINT	Mr. Miguel AMUTIO Mr. F LOPEZ-CRESPO Mr. D. HERNANDEZ Mr. V. RAMIREZ	M
SE	ID CARD	Statskontoret	Mr. Björn SCHARIN Mr. Wiggo ÖBERG	M
UK	SCC	e-Envoy	Mr. Ian ASCOUGH	Q

Belgium

There is already a wide smart card based system running in Belgium: the SIS card, i.e. a card for identification of insured persons in the Belgian social security system; it is managed by mutual insurance companies. We unfortunately could not contact authorised responsible persons. According to the general information available, this is a simple identification card without authentication (electronic signature) abilities.

At federal level, the FEDICT agency has been entrusted the definition and deployment of a general-purpose card, that will eventually cover both the citizen identity card, with ability of signing, and the civil servant card. The FEDICT card will be PKI based. For the time being, the effort is more particularly directed towards the civil servants, in particular in federal instances.

The FEDICT system is still a project.

The following pages are the answers given by FEDICT representatives, collected by our consultant and completed by information drawn from their web site `http://www.fedict.be` ; they were not explicitly approved by .

Survey of Secure Smart Card based eGovernment Applications

Answer given by the Belgian Service Public Fédéral Technologie de l'Information et de la Communication (FEDICT)

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

What is/are the application(s) in your project that is/are associated with the smart card ?
The Electronic Identity Card (EID).

Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
Single purpose one, enabling to access several applications

What is the role of the smart card in your project ?
Identification and authentication of individuals

In case of a multi-purposes card, what will the card offer in common to several applications ? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?
3 key pairs (& certificates)

In your project, who will act as :

Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?
Individuals

Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?
CA (to be selected)

Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?
CA (to be selected)

Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)
Municipalities

In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
See above

What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
Technology, security, privacy, friendliness – see article on website: `www.Rijksregister.Fgov`.

Was this chosen at once or through analysis / project analysis ?
Via a study conducted by CSC (Computer Sciences Corporation).

What is the business model supported?
Production + distribution of EID + communication between citizens, government and other partners.

Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
The main motives are explained in the before mentioned article + decision of the Council of Ministers of 22 November 2000: to ensure e-communication between citizens and government through certificates => has become the EID.

Who is/are the major stakeholders or driving force behind the project ?
Government; it is the government which regulates how an identity is determined => history: a surname was introduced by Francis I, king of France, in 1539: has since ??? Decision Council of Ministers of 22 November 2000.

How would you best describe the geographical scope of your smart card project ?
Belgium + belgium abroad.

What is your target audience?
All citizens 18 years and older.

Do you consider inter-operability of your project with other projects using other smart cards ? If yes, how do you deal with this issue ?
No.

Please give details on elements of your business model.
Belpic => `http://www.mazfp.fgov.be/copernicus` *: modernization of the curl services.*

Difficulties

What were the critical obstacles to choose using smart cards (example: management, human aspects…)?
1 – readers: general technology disposal at home: not every citizen has the required technology at home;

2 – there have to be products for which the EID can be used

- During the project :

What were the impacts of the new standards on the way of working (end users, central application) ?
The tender still has to be made public

How was the cooperation with software companies ?
No problems.

Were the software companies responsive ?
Yes.

What role did the smart card play in matters of acceptance/friendliness ?
To try to open traditional databases on physical persons

Was usage of smart cards felt as a support for respect of private information ?
Yes, one can with his EID only consult his file.

Alternative technologies or processes used or envisaged as enablers, during the meantime ?
If so, how did you organise the transition to full-wedged electronic transactions ?
Yes, sites like those from Ghent, Bruges, Seneffe => one can ask his file and get then a copy of his "population file" with his own national identity number.

Project Deployment

What is the size of your smart card project (number of cards …) ?
The number is 10 million; in the initial phase, the number is 330.000 (= 11 municipalities) – the project is to be deployed over a 5 years period.

What is the current status of the project ?
The tender (card and CA) still has to be published.

Is your present project rolled over from a pre-existing one ?
Example has been taken on the SIS-card.

If so, briefly describe your experience from such pre-existing project.
The SIS-card is only a memory card, not an intelligence card. It is better not to have changeable information on it (not up to-date).

What are the targeted phases of deployment ?
An evaluation will happen after a 6 month period of tests (pilot project) in the 11 municipalities.

What significant problems did you encounter ?
Adaptation of the infrastructure in the 11 municipalities and the National Register.

Has the project reached its goals?
We are only in the initial phase => as a consequence, too early to tell.

What are the cost drivers in your projects ?
Infrastructure, cards, readers.

Is the cost of the usage of smart cards perceived as high?
No.

If that is the case, why did you decide to make that choice anyway ?
See answer on the previous question.

Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Yes, but not now yet the cost of the EID and 2 certificates is estimated at 9 €.

Transitions to come, under process or completed

Which new standards or infrastructures are you considering for the near future and midterm?
No answer yet.

Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates)?
Yes.

Which new services are considered in your existing application ?
Opening of the central data base to the public, so that everybody can consult his file.

Do you consider re-using the same smart cards for others applications?
Yes, in principle, the smartcard can be used for each application driven by the identity of the user.

Can you accept relaxing the usage of the smartcards to less demanding requirements?
Yes.

Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised…)?
No, is already decentralised.

Which benefits are you expecting from that change?
=> see answer on the previous question.

Process

Please describe the smart card personalization & delivery process.
The data are personalised on the outside; inside, the chip with 3 pairs of keys is added (third pair for identification of the card).

Please describe the registration process.
The citizen is registered in the population registers of the municipality. When he needs a new EID, he makes an appointment with the population service of the municipality, where his identity is checked and where the process of deliver of the new card is completed.

What have been the training requirements for personalisation agents and Registration Authority agents?
They have to know the procedures of the population registers; they have also to learn to use the new software.

Please describe your support efforts for the end user.
Training sessions when one takes delivery of the new card + leaflets how the card can be used at home + citizen kiosk.

Please describe any documentation you might make available to the end user.
=> see answer on the previous question.

What has been the user reaction and feedback to your project?
Not yet known.

Were the organisation and responsibilities for the parties all taken into account at the beginning? How?
Yes, by mentionning them in the tender document.

Which new issues did you discover (during the project)?
Not yet known.

Do you have a published liability scheme?
Not yet, this will happen in the future (CPS in the tender).

What are the commitments of each category of partners?
Cf. website mentioned on page 1 of the questionnaire.

Archival

Are there any retention requirements for documents in this project?
No answer.

Are there any time stamping requirements for this project?
Yes they are described in the tender.

Suppliers

In your project do you use a single or multiple suppliers for smart cards ?
Both are possible.

In your project do you have a single or multiple suppliers for your PKI (if any) ?
Both are possible.

B. TECHNOLOGY USED IN THE PROJECTS

General

What technologies have been considered in the project?
Cf. tender + open standards interoperability.

What were the arguments in favour/against a smart card?
Against: only 25% of the population is connected to the Internet -> municipalities

Smart card

What are the main features of the smart card ?
Eye readability of the information on the inside because the ID card is a valid travel in the EU + chip with 3 key pairs; 2 of them correspond with an identity certificate.

Does your Smart Card support other applications or is it a single application card?
It is in the beginning a single card.

What are the cryptographic features of the smart card in your project ?
RSA .

What is the PKI related content of your smart card ?
Roots certificate, identity certificate and signature certificate.

If the smart card is used for electronic signing, what is the exact role of the card in the signing process?
To ensure that if one signs as a physical person.

What authentication mechanisms are used ?
= *authentication certificate*

Are there any other form factors involved ?
Eye format readability.

Is the smart card compliant with international security standards ?
Yes.

What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Use of RSA.

What are the main features of the smart card readers ?
Harmonised European standards + acceptance of national equivalent standards in the other 14 EU - countries

Public Key Infrastructure

Do you manage the issuance of the certificates in house or do you outsource it ?
Outsource.

Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
Yes, the interoperability is a requirement of the tender.

What are the user registration requirements for certificate registration?
Via the population registers.

What are the standards used in your project and for which specific purpose?
The standards used for the card and the readers are European standards.

Client side software

Are the smart cards used in your project used with Secure Signature Creation Devices ?
No products available.

What are the software requirements on the client side ?
PC/SC plugin in the browser.

Briefly describe the general technology requirements of your project.
No answer given.

C. LEGAL ASPECTS OF THE PROJECTS

General

Could you describe the legal requirements that were considered in your project ?
A legal basis is required; as a result, the law concerning the registers of population and the identity card had to be modified.

Digital signature

Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes.

What are your plans to roll out qualified certificates ?
They will be put on the card.

Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
As soon as available.

Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
Not yet, it could be in the future imposed by Belgian law, for example, to enable to support highest requirements.

Have you planned or accomplished any audits of your project ?
An independent audit is planned; a technical audit. The realisation will happen in private consulting.

Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
In principle, the State is its own insurer. The liability of the Government is of 2500 € per transaction.

CP / CPS (Particularly for e-Procurement)

Could you describe the main features of your CP / CPS ?
Cf. Belpic website for CP.

Do you make available any of the following such as a :

- subscriber agreement
- relying party agreement
- consumer policy
- privacy policy ?

See above.

Describe the approval procedures for your policies. Is there a designated Policy Board ?
No approval procedures ; no designated policy board.

Do you foresee any dispute resolution mechanisms ?
Yes. The EID Committee being before a mediator.

Have you undertaken ? Planned any cross certification with other CAs ?
Not until now, in the Belpic context.

Data protection, consumers and confidentiality

What specific consumer protections do you apply in your project ?
The consumer has an authentication signature certificate.

What are the major data protection warranties you offer ?
Not changeable.

What remains confidential ? For how long?
Private keys, for 5 years.

Finland

Finland have had an operational system for several years already: the FINEID system. It is an electronic identity card that may be adapted to particular purpose of specific applications of user groups. FINEID cards are PKI based and may therefore be used for electronic signature, not qualified yet.

There are two major domains where FINEID cards are mainly used at the moment:

- for civil servants, mainly for access to applications
- in the health ans social insurance domain, to exchange authenticated and confidential data between healthcare professionals, and between professionals and patients.

Two reports were given back by Finnish representatives: one by the TAC delegate, and one by FINEID themselves.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the TAC representative

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

- What is/are the application(s) in your project that is/are associated with the smart card ?
In Fi there are many on going projects and many which are in production;

1 `http://www.tyvi.org` *information available in Swedish*

`http://www.mol.fi` *Fineid based personal service for employers*

2. `http://www.pkshp.fi` *North Karelian Hospital District . Organisation use eSign in patients reports. Future information is available via personal contact with permission of the organisation*

`mailto:seppo.soininen@pkshp.fi` *IT manager*

3 At GV level we are building a generic Access Management System based on organisational PKI card . `http://www.fineid.fi/civilservent` *profile and also we will use GSM-PKI (Sonera) and GSM-WIM (Radiolinja)authentications*

4 In district administration level, communal etc. there are several different kind of projects based on citizen card.

- Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
Citizen card includes;

- authentication and form signing. No email encryption without additional software components.

Role based, organisation card, card will include multipurpose functionality

- authentication

- email encryption

- signing

- What is the role of the smart card in your project ?
It will include all mentioned above.

Main task is educate the user's. First will be authentication and remote use.

In case of a multi-purposes card, what will the card offer in common to several applications ?
Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?

Card is a vehicle for carrying the public key pairs and certificates

- In your project, who will act as :

  . Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?
  Government workers, at the first

  . Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?
  Population Office of Finland is RA. LRA is the security Office of the Government

  GSM PKI there are operators Sonera and Radiolinja

  . Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?
  Government information unit is responsible to built a generic AMS based an PKI

  These service doesn't include service for citizen. Those service are produced with co-operation with service providers

  . Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)

- In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
--

- What is the rationale for using smart card (technology, security, privacy, friendliness, etc) ?
Generic security tool, scalable and global

- Was this chosen at once or through analysis / project analysis ?
Chose through analysis. Generic AMS for inter Government use we have established a project to build it up. Mainly because there are no single product available on a market.

- What is the business model supported ?
Virtual Government

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
- Hard question to answered in one sentence

- Who is/are the major stakeholders or driving force behind the project ?
For Government; Government information unit

- How would you best describe the geographical scope of your smart card project ?
Including Commission, Council etc inter organisational inside EU. Ref CA -Bridging

- What is your target audience ?
The workers of the "Virtual Government"

- Do you consider inter-operability of your project with other projects using other smart cards ? If yes, how do you deal with this issue ?
Let's see what the CA Bridging will give for it

- Please give details on elements of your business model.
Architectural model in power point form see addendum

Difficulties (and following)
These questions I postpone at this moment.

Survey of Secure Smart Card based eGovernment Applications

Answer given by FINEID

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

- What is the application in your project that is associated with the smart card ?
We have national electronic identity card, launched December 1999.

The national registration center is the certification authority and the card is issued by local police.

More information can be found at :

`http://www.sahkoinenhenkilokortti.fi/default.asp?todo=setlang&lang=uk`

We also have one commercial certification authority.

Both the governmental and private certification authorities have had problems in marketing their cards to general public. The governmental certification authority has issued 14 000 cards and the private authority 700 cards.

There are some public services available with smart-card identification:

- *citizen can change their address in the population register and check the information about themselves in the register*
- *citizen can make an application for their child's day care in two municipalities*
- *citizen can update their information at the employment office*
- *citizen can fill in applications to some higher education institutes*
- *citizen can check his future retirement pay*
- *companies can fill in applications for government R&D funding*
- *companies can send their mandatory reports to authorities electronically*
- *companies can send information regarding their employees to retirement insurance companies*

Commercial services using smart card identification are scarce. One of the banks is offering also smart card identification. (All the biggest banks are offering identification based on changing passwords. This is used by more than 2 million customers.)

Since the smart-card technology is still quite challenging for citizens to maintain at their home computers, the smart card identification is not widely used in the above mentioned applications.

- What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
The rationale for developing the national electronic ID –scheme has been enabling sufficient level of security and privacy to develop governmental online services.

- Was this chosen at once or through analysis / project analysis ?

- What is the business model supported ?
The ID-card costs 29 euros and is valid for 3 years. Directory services are free for the service providers. At the moment government funding is the main source of funding for the scheme.

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
Economical: the objective was to cut down on the costs of government information gathering.
Tutorial: the administration should set the example.

- Who is/are the major stakeholders or driving force behind the project ?
Government.

- How would you best describe the geographical scope of your smart card project ?
Countrywide.

- What is your target audience ?
Citizens and companies.

- Please give details on elements of your business model.
At the moment we are re-evaluating the business model.

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
Technology, it is not ripe yet.

- During the project :

- What were the impacts of the new standards on the way of working (end users, central application) ?

- How was the cooperation with software companies ?

- Were the software companies responsive ?
Smart card solutions are not compatible. Readers, drivers and software do not operate trustfully. To much knowledge is assumed from the user.

PKI has not proven to be a successful business yet. Software companies are not investing enough on development.

- What role did the smart card play in matters of acceptance/friendliness ?

- Was usage of smart cards felt as a support for respect of private information ?

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
At the moment we are considering the identification used by banks as an alternative enabler of strong identification and authentication. System is based on changing passwords and already used by about 40 % of the population.

Project Deployment

- What is the size of your smart card project (number of cards …) ?
See answers above.

- What is the current status of the project ?
The smart cards are in use, but it has not become the mainstream authentication method. Revaluation of the business mode has started.

- Is your present project rolled over from a pre-existing one ?

- If so, briefly describe your experience from such pre-existing project.

- What are the targeted phases of deployment ?

- What significant problems did you encounter ?
Technology.

- Has the project reached its goals ?
No, the amount of smart cards used is not sufficient to encourage new services to be built.

-What are the cost drivers in your projects ?
Maintaining directory services and revocation lists for such a small amount of users is not cost-effective. In future the maintenance of revocation lists and directories should be charged from service providers.

- Is the cost of the usage of smart cards perceived as high ?
Yes. The citizens find the cost high since they have to purchase the card readers and software even though there are not very many services available. The cost is high for government.

- If that is the case, why did you decide to make that choice anyway ?

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Yes, we know the elements and are reassessing them.

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
See answers above.

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
Yes, but the fact is, that actual advanced signatures are not needed in government transaction in many cases. Most of the time strong enough authentication is what we need.

- Which new services are considered in your existing application ?

- Do you consider re-using the same smart cards for others applications ?
Yes.

- Can you accept relaxing the usage of the smart cards to less demanding requirements ?
Yes.

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?

- Which benefits are you expecting from that change ?
--

Process
See: http://www.fineid.fi/default.asp?todo=setlang&lang=uk

Archival

- Are there any retention requirements for documents in this project ?

- Are there any time stamping requirements for this project ?

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
Single.

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
Single.

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
See answers above.

- What were the arguments in favour/against a smart card ?
Favour: security, no better alternative can be seen at the moment

Against: technology not ripe yet.

Smart card
See: http://www.fineid.fi/default.asp?todo=setlang&lang=uk

Public Key Infrastructure
See: http://www.fineid.fi/default.asp?todo=setlang&lang=uk

Client side software
See: http://www.fineid.fi/default.asp?todo=setlang&lang=uk

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
The electronic signature directive, the law on government electronic services in Finland (was developed simultaneously with the ID-card), privacy legislation.

Digital signature

- Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes.

- What are your plans to roll out qualified certificates ?
Both governmental and private certification authorities are planning to produce qualified certicicates.

- Plans to roll into Secure Signature Creation Devices 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 ?
Both schemes have gone through BS7799 audit.

- Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
--

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?

- Do you make available any of the following such as a :

  - subscriber agreement

  - relying party agreement

  - consumer policy

  - privacy policy ?

All are available.

- Describe the approval procedures for your policies. Is there a designated Policy Board ?
Not yet.

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 ?

France

The situation in France is multiple. Several initiatives were taken separately and are not likely to converge.

Most generally, two domains of identification of persons have been defined: one for general identity (typically for identity cards) and one for the social security and possibly healthcare domains. There is a clear commitment of the authorities to keep these two domains separate and to never allow cross-referencing (except incidentally, and then under very careful control and protection).

The four investigations made for France concern either of these domains.

In social security and healthcare domain, there is an already old history with smart cards, that started in the very early nineties with the first versions of the CPS (card of the healthcare professional). It is now a PKI based system that allows full protection of data, as well as authentication and electronic signature, by almost all professionals of the sector. It is mainly used to control the information carried by the second major frebnch system, namely the Vitale card.

The Vitale card is presently the major smart card application in France. Its role is the identification of insured persons and the storage of their social security rights. 40 millions of such cards have already been issued and its usage is fully operational.

In the domain of identity, the Ministry of Home Affairs is studying a common basis of identification intending at the creation of many categories of cards, a part of them being PKI based, such as a civil servant card or a elected representative card.

In the domain of taxation, companies, and potentially citizens, are concerned by the teleprocedures project of the Ministry of Finance, that aims at authenticating tax payers when they issue declarations, and possibly for payment as well. It is actually a PKI project that allows distribution of smart cards, but software storage of keys is possible as well.

The four following files summarise the answers of:

- the GIP-CPS group, that distributes the CPS card,
- the SESAM-Vitale group, that distributes the Vitale card,
- the Ministry of Home Affairs, for the ID card project,
- the Ministry of Finance, for the tax teleprocedures.

Survey of Secure Smart Card based eGovernment Applications

Phone discussion with the Manager of the French Groupe d'Intérêt Professionnel GIP-CPS

SUMMARY

This summary is provided for the understanding of non French speaking persons. Accurate information must be searched for only in the French text.

The GIP-CPS was created in year 1993 with the aim to provide healthcare professionals with smart cards able to help them in creating a secure and trusted context for their electronic exchanges.

The major usage of the CPS (Carte du Professionnel de Santé – health professional's card) is in connection with the Vitale card, not only with the professionals themselves, but with their staff as well.

Particular care is taken to the respect of the role and responsibilities of each actor.

In particular, the GIP-CPS personalises the cards only after formal approval of an authorised person guaranteeing the truth of information and after verification of rightfulness by the authorities (State, professional organisation). The card guarantees the identity of its holder and the link with the associated public keys contained in certificates. The GIP-CPS manages the whole life cycle of the card.

The GIP does not develop any application, except those necessary for the management of the cards. it publishes to application managers the information required for the usage of the cards (repository of certificates, revocation lists).

The GIP is therefore not involved in the relationship between the application manager and each card holder. Its role ids just that of a trusted third party.

From the beginning the GIP-CPS constantly made the technical solutions evolve according to the standarss, but always keeping upwards compatibility with older solutions. For the time being, the certificates distributed are intended for three kinds of usage according to three certificate policies:

- authentication and signature
- confidentiality (secure exchange of encryption keys) (note that the confidentiality keys are not stored in the card but in the work station; the card is however necessary to unlock it)
- application servers (for securing of on-line communications).

Since the beginning, around 400000 cards have been distributed to the various categories of users.

The services supported by CPS cards may be:

- authentication of the holder
- integrity (non corruption) of a message

- guarantee of origin (electronic signature)
- guarantee of a server's authenticity and encryption upon transfer
- electronic mail with encryption and/or signature
- management of access rights

The major running applications are:

- support of Vitale cards (distributed by GIE SESAM-VITALE) for electronic transfer of reimbursement information to the social security organisms
- several hospitals for securing of their internal information system, including access control
- securing of information centres (web and/or data bases)
- securing of specialised portals reserved to authorised professionals
- securing of the GIP-CPS information centre

Other applications are starting up or under consideration.

Considering acceptance by the end users, the combined usage of the Vitale card was a starter for the CPS. Other positive aspects were:

a good support provided to card holders

training and information on the stakes of information security

upwards compatibility with previous version

The smart card was chosen to be the support as a good compromise between mobility and standardisation; the important thing is to provide users with a container for their certificates.

Note that the interoperability of the cards has been tested with users located in the Netherlands (keys stored in the work station). These tests did not take into account the difference of assurance level between smart cards and software certificates.

The GIP-CPS is committed topermanent keep upwards compatibility with the previous systems. The standards are now felt sufficient and the next evolutions should be extension to new applications and to new usage in the existing applications. The only technical evolution considered is the possible addition of new algorithms or extension of the length of keys. Support of single sign on is considered as well.

The next version of the system is planned for year 2005.

INTRODUCTION

Les Nouvelles Technologies de l'Information et de la Communication représentent un enjeu majeur pour tous les intervenants de la santé et pour l'ensemble des patients. Le caractère sensible des échanges de données dans ce secteur nécessite que soient mis en œuvre les moyens juridiques, techniques et organisationnels garantissant la confidentialité des informations mais également leur interopérabilité entre les différents intervenants. De ce point de vue, une préoccupation majeure est de pouvoir apporter des réponses techniques et organisationnelles au problème majeur que pose l'internet, à savoir garantir l'identité et la qualité des différents intervenants du système de soins et de santé.

Le GIP-CPS (Groupement d'Intérêt Public – Carte de Professionnel de Santé) regroupe l'ensemble des principaux organismes et institutions représentatifs du secteur de la santé français (Etat, Organismes d'assurances maladie obligatoires et complémentaires, Ordres professionnels, syndicats pofessionnels, établissements de santé et Service de Santé des Armées). Il a pour mission de fournir à l'ensemble des professions du secteur de la santé et plus largement des intervenants de ce secteur des cartes électroniques leur permettant de créer les conditions de la sécurité et de confiance de tous les échanges électroniques du secteur santé, et ceci dans le respect des compétences dévolues à chacun des acteurs.

L'entretien avait pour but d'apporter des éléments complémentaires par rapport à l'entretien réalisé en 2001 par un membre du comité e-smartcards TB2.

Personnes interrogée :

M. Gilles TAÏB, Directeur

Information complémentaire trouvée sur le site internet:

www.gip-cps.fr

CONTEXTE

Le GIP-CPS existe déjà depuis de nombreuses années (création en 1993). Si dés la conception du système il a été pris en compte la nécessaire ouverture et usage pour l'ensemble des services informatiques du secteur (prises en charge administrative, continuité des soins, santé publique, accès sécurisé à des serveurs professionnels), son déploiement a été en particulier associé à l'application de la carte Vitale (Loi de 1996) qui a introduit la CPS auprès de l'ensemble des professionnels de santé (médecins, pharmaciens, chirurgiens dentistes, infirmiers, ……) ayant une activité libérale et à leurs collaborateurs non forcément professionnels de santé (aujourd'hui plus de 400.000 cartes ont déjà été distribuées et concerne notamment plus des deux tiers des professionnels concernés).Le positionnement du GIP « CPS » vis à vis des professionnels de santé et des responsables des différentes applications a été clairement définie dés la conception du système.

Des choix organisationnels ont été effectués garantissant le respect des responsabilités de chacun des acteurs.

Ainsi, **vis à vis du professionnel de santé**, le GIP n'émet une carte qu'après signature (accord formel) d'un professionnel garantissant la véracité des informations le concernant et après visa des Institutions ayant mission, par le législateur, du contrôle de l'exercice (Etat, Ordres professionnels). Une carte émise, ainsi que les certificats associés garantissent l'identité du porteur, sa qualité et la clé publique associée. Dans sa relation avec le professionnel de santé, le GIP gère la vie de la carte (perte, vol, continuité du service,

renouvellement en fin de vie de la carte, prise en compte de l'évolution des informations concernant le professionnel,….). Le professionnel de santé à le libre choix et la responsabilité de son équipement informatique, de son provider, mais également de l'usage de sa carte vis à vis des différentes applications.

Vis à vis des responsables des différentes applications, le GIP n'est pas juge et partie, à ce titre il ne développe aucune application (autre que celles concernant les stricts services liés à gestion de la carte et des certificats associés). Le GIP met à disposition, dans le cadre d'une convention le liant au responsable de l'application les composants nécessaires à l'utilisation des cartes CPS (Liste d'opposition, annuaire des cartes émises, certificats applicatifs,….).

Ainsi, le GIP garantit à une application la validité des cartes émises et la qualité des porteurs, par contre, il relève de chaque application de définir et de gérer les habilitations (droits) qu'il accorde à tel ou tel professionnel de santé.

La relation qui s'instaure entre les professionnels de santé et les applications est par conséquence indépendante du GIP et ne relève pas de sa responsabilité. A ce titre, le GIP « CPS » assure un rôle de tiers partie de confiance.

Le contexte législatif et réglementaire :

Sous les effets de l'évolution de la société, des enjeux économiques et industriels, de l'existence du système CPS (pour les textes relatifs au secteur de la santé), de la réglementation européenne en matière de reconnaissance de la signature électronique, le législateur a été amené à faire évolué l'environnement législatif et réglementaire. Sans faire une liste exhaustive, nous pouvons indiquer les principaux domaines concernés :

- Libéralisation de l'utilisation des moyens de cryptologies (1997 – 1998) ;
- Reconnaissance de la signature électronique (Directives européennes et loi d'application française – 2001) ;
- Textes relatifs à l'informatique et aux libertés ainsi qu'au respect de la vie privée ;
- Textes relatifs à l'organisation et au fonctionnement de la santé en France (Ordonnance de 1996 , loi du 4 mars 2002 sur le droit du patient et la modernisation du système de soins.

Le contexte technologique

Le contexte technologique a fortement évolué depuis la conception initiale du système CPS. Ces évolutions, principalement, marqué par l'émergence et la popularisation de l'internet (40% des ménages français sont internautes en fin 2001), la libéralisation des moyens et outils de cryptologie, la stabilisation de standards, comme par exemple les certificats au format X509, des protocoles s-mime ou encore SSL, ont conduit le GIP à faire évoluer, progressivement, son système « d'une gestion de carte » à celle « d'infrastructure de gestion de clé – PKI ».

Aujourd'hui, le GIP « CPS » a rendu publique ces différentes politiques de certification (accessibles sur son site WEB) :

- Politique de certification « authentification – signature » ;
- Politique de certification « confidentialité » ;
- Politique de certification « serveur applicatif »

LES APPLICATIONS

Compte tenu de la flexibilité du système CPS, chaque application peut mettre en œuvre de manière indifférenciée les différentes fonctions offertes par le système CPS et ceci dans le cadre des différents protocoles standards (TCP-IP, SSL, S-mime, et demain XML) :

- Authentification et sa validité (accès aux CRL publiées dans l'annuaire) ;
- Intégrité d'un message et garantie de l'origine (signature électronique) ;
- Certificat pour son serveur (certificat mode SSL ou S-mime) ;
- Chiffrement du message en mode SSL ;
- Chiffrement et/ou signature dans les différents produits de messagerie du marché ;
- Gestion des délégations et des droits associés ;
- Mise en œuvre d'un annuaire propre à sos ou ses applications en «cohérence » avec celui du GIP (LDAP).

La large diffusion des cartes à l'ensemble des acteurs du secteur présente de nombreux avantages pour les applications : économique (évite la gestion des mots de passe ainsi que les vérifications nécessaires à leurs attributions), garantie de cohérence dans le temps (compatibilité ascendante) et interopérabilité des échanges, possibilité dès disponibilité d'une application de la mettre à disposition de l'ensemble de la communauté et ceci de manière sûre, indépendance du choix de son provider,……

Les principales applications utilisant le système CPS aujourd'hui :

- la principale application, de portée nationale, utilisant le système CPS est SESAM – VITALE (plus de 100 000 professionnels de santé transmettent leurs feuilles de soins électroniques quotidiennement) ;
- d'autres applications utilisent également le système CPS :
  - le Centre Hospitalier de Macon, sécurisation d'accès et des échanges du Système d'Information Hospitalier (en cours d'extension pour favoriser les échanges avec les professionnels du secteur libéral) ;
  - les Hôpitaux Universitaires de Strasbourg, l'ensemble du personnel dispose aujourd'hui de leur carte (sécurisation du Système d'Information des Hôpitaux Universitaires – 5 établissements -, horaires variables,….) ;

- l'application HC Forum de l'université Fournier à Grenoble, serveur sécurisé associant plus de 200 chercheurs dans le domaine de la génétique en Europe et au niveau International ;
- accès sécurisé au bouquet de services du Réseau Santé Social appelé « forteresse » ;
- accès sécurisé aux bases de données reservèes aux professionnels de santé (bases d'informations sur les médicaments, laboratoires GLAXO) ;
- intégration dans des portails sécurisés développés par des industriels (ICSF, Netsanté,…) ;
- Annuaire du GIP (accès sécurisés sur critères) et Espace Membres du Web du GIP réservé aux Administrateurs.

Les applications dont l'intégration du système CPS est en cours :

- Messageries sécurisées (France Telecom, Réseau Santé Social, MSI et Medsys) s'appuyant sur des produits du marché et répondant aux spécifications fonctionnelles du secteur (interopérabilité et gestion des délégations) ;
- Réseau d'Hémovigilance de l'Agence Française de Sécurité Santiare ;
- Gestion des dons et des receveurs des greffes (Agence Française des Greffes) ;
- Réseau Santé GT69 (toxicologie et SIDA) associant les professionnels de santé de la région lyonnaise libéraux et hospitaliers ;
- Réseau Santé C-link de la région Provence Côtes d'Azur (réseau cancer) ;
- Système d'Information du Service de Santé des Armées
- Réseau de cancérologie de la région Aquitaine

Les perspectives d'applications et d'usages :

- diverses applications en télémédecine ;
- accés et gestion sécurisé des dossiers médicaux (application de la loi du 4 mars 2002) ;
- communication des résultats de laboratoires d'analyse ;
- réseaux d'alerte sanitaires ;
- réseaux épidémiologiques ;
- diverses réseaux santé (plus de 500 actuellement identifiés en France) ;
- serveurs professionnels, accès à des bases de données réservées aux professionnels ;
- formations spécialisées y compris gestion du cursus ;
- ……..

ACCEPTATION PAR LES UTILISATEURS

L'argument majeur pour faire accepter un outil tel que la CPS est qu'il offre des réponses pratiques et simples à des besoins de sécurité et de confiance de tous échanges électroniques nécessaires à la pratique des différentes catégories de professionnels de santé.

En conséquence, il faut allier deux objectifs complémentaires la plus large diffusion de cartes à l'ensemble des professionnels de santé indépendamment de leurs situations d'exercices, et la multiplication des applications s'appuyant sur le système (ce deuxième objectif nécessite une définition précise des responsabilités entre le GIP et les applications).

Ces objectifs sont le point d'être atteint en France, en effet le déploiement de la carte CPS concomitamment avec la montée en charge de SESAM-VITALE a permis l'accélération du développement de l'informatisation dans le secteur de la santé et la mise en œuvre d'une infrastructure d'IGC (PKI) commune. Cette situation crait les conditions favorables aux développement cohérent et répondant aux besoins des applications et qui peuvent être facilement satisfaits avec la même carte.

D'autres conditions jouent également un rôle important dans l'appropriation :

- la qualité des services (assistance téléphonique, gestion des remplacements par exemple) rendus aux professionnels de santé ;
- prise en compte dans la formation initiale et continue de l'importance des questions liées à la sécurisation des systèmes et de leurs apports dans l'exercice quotidienne ;
- maintien de la qualité et de la sécurité du système dans le temps sans conséquences pour les utilisateurs et les applications (compatibilité ascendante) ;
- ……

CHOIX DU SUPPORT ET INTEROPERABILITE

Il n'y a aucun a priori dans le choix de la carte à puce plutôt que d'un autre type de support. il se trouve seulement que la carte à puce offre actuellement un bon compromis entre différents aspects (standardisation, mobilité). Ce qui est important n'est pas tant le support que l'existence d'un certificat qui crée un espace de confiance et de sécurité:

a) choix du support :

- pour obtenir les meilleurs garanties de sécurité et de flexibilté pour l'utilisateur , la carte à puce est apparu comme le meilleur compromis. Elle est liée à une personne physique, indépendante du poste de travail. Le Professionnel peut l'utiliser dans ses différentes activités et même éventuellement chez lui (similaire aux cartes des téléphones mobiles). Les

cartes à puce permettent également une évaluation sécuritaire « critères communs » afin de se prémunir contre d'éventuelle attaque 'au reagrd de l'état de l'art) ;

- Ainsi, les certificats d'authentification et de signature sont dans la carte ;
- Par contre les certificats de confidentialité sont dans le poste, mais le déchiffrement ne peut être réalisé qu'après une authentification par carte.

B) Interopérabilité et choix des standards :
L'interopérabilité s'analyse par rapport à différents critères et aux choix des standards :

- Carte conforme ISO 7816 ;
- Lecteur de cartes : protocoles indifférenciés (PC/SC ou par exemple protocole propriétaire du secteur santé français (Protocole Santé Social) ;
- communication :
  - choix des protocoles TCP-IP, S-mime V3, SSL-V3/TLS…. ;
  - Annuaire LDAP, X500 indépendant des providers, interrogation via l'internet et ouvert, en requête, unitaire, aux porteurs de carte ou non ;
- échanges sécurisés :
  - choix d'algorithmes à clé publique standards : RSA, SHA ;
  - format des certificats X509
- syntaxe et sémantique des informations : *Ne relève pas de la compétence du GIP « CPS » ;*

Il est à noter que l'interopérabilité des clés et des certificats X.509 contenus dans les cartes avec des systèmes à clés stockées sur les postes de travail a déjà été testée avec succès avec des utilisateurs localisés aux Pays-Bas. Ces tests purement techniques ne prenaient pas en compte la différence des niveaux d'assurance entre la carte à puce et des certificats logiciels.

EVOLUTIONS

Depuis sa création, la carte CPS a toujours assuré une compatibilité ascendante de la solution "propriétaire" initiale à la technologie actuelle. Ceci sera conservé avec les évolutions prochaines, l'objectif étant d'assurer une totale transparence aux utilisateurs.

Aujourd'hui, après le basculement réussi du système CPS aux standards actuellement les plus utilisés. La gestion du système « CPS » a subi une modification profonde passant ainsi « d'une gestion carte » à une «gestion d'IGC –PKI ». La carte n'étant plus que le média sécurisé des certificats.

Les évolutions qui peuvent être envisagées aujourd'hui, ne portent plus des refontes du système , mais par contre sur :

- extension des usages dans les différentes applications ;
- évolution fonctionnelles souhaitées par les professionnels de santé et les applications ;
- maintien du niveau de sécurité et de qualité au regard de l'évolution de l'état de l'art (implémentation de l'algorithme AES ou allongement de la longueur des clés asymétriques de 768 bits à 1024 bits par exemple;
- assurer autant que possible, le support du single sign-on ;
-

La prochaine version du système est prévue pour 2005 ;

En conséquence : les efforts du GIP CPS dans les toutes prochaines années porteront essentiellement à créer les conditions de l'appropriation. Par exemple, en application de la Loi « droit du patient » du 4 mars 2002, en permettant, via l'annuaire, à un patient d'envoyer un message chiffré (sans que ce dernier dispose d'une carte de type CPS) à son médecin traitant et que celui-ci sera le seul à pouvoir déchiffrer
D'autres axes sont à l'étude actuellement, comme par exemple le mise en œuvre d'autorité de certification délégué, ou encore la reconnaissance d'autres IGC.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the French economic interest group GIE SESAM-VITALE

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

Most information may be found on the Web site:
`http://www.sesam-vitale.fr`

- What is/are the application(s) in your project that is/are associated with the smart card ?
Social security – reimbursement of health expenses

- Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
Single purpose –carrying some extra information is being considered

- What is the role of the smart card in your project ?
Identification of the insured person (beneficiaries of reimbursement may be other members of the family)

Presently under distribution: extension cards handed to all beneficiaries over 16 years.

In case of a multi-purposes card, what will the card offer in common to several applications ? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?
Mainly identification information (NIR number). The card is considered for the future: storage of basic health information

- In your project, who will act as :

. Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?
Any person insured by a Social Security organism in France (i.e. almost everybody)

. Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?
The SESAM-Vitale members

. Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?
Social security (Caisses d'Assurance Maladie) and associated complementary organisms provide update of the data stored in the cards through interactive terminals (borne SESAM-Vitale)

. Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)
Each healthcare professional is free to choose a hardware and/or software provider of products compliant to a precise specification published by the SESAM-Vitale GIE

- In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
Access is provided by the RSS network, completely separate from the management of cards

Service providers are members of SESAM-Vitale

- What is the rationale for using smart card (technology, security, privacy, friendliness, etc) ?
At the time where the choice was made, there were no real concurrent solutions. Moreover, smart cards allow updating the contents (in particular the details of rights) through the interactive terminals

- Was this chosen at once or through analysis / project analysis ?
Through a short analysis

- What is the business model supported ?
Question not understood

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
Was basically a political decision taken at the highest governmental level (Prime Minister)

- Who is/are the major stakeholders or driving force behind the project ?
Social Security organisms, with a wide support of insured persons

- How would you best describe the geographical scope of your smart card project ?
No geographical scope – concerns any person insured by the members and any health professional equipped with the relevant hardware and software. – practically the whole French territory.

- What is your target audience ?
See above.

- Do you consider inter-operability of your project with other projects using other smart cards ? If yes, how do you deal with this issue ?
There are presently two experiments with foreign organisms. The scope will anyway always remain social security.

- Please give details on elements of your business model.
No answer

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
No critical obstacles – the project required a long preparation but finally is has become fully accepted.

- During the project :

  - What were the impacts of the new standards on the way of working (end users, central application) ?
  Major change of the way of working as the transmission of the document (feuille de soins) to the reimbursement centre is not done by the insured person any more but electronically by the health professional. This helped shortening the delay of reimbursement.

  The most difficult was to have the system accepted by health professionals. However the pressure of customer was strong and they finally discovered that the new procedures did not add so much more work to them.

  - How was the cooperation with software companies ?
  SESAM-Vitale is submitted to the French regulation of public contracts; so, two types of invitations to tender were and still are periodically launched:

  in (now) most cases, provision of virgin cards that are personalised by SESAM-Vitale

  mainly at the beginning, and now in some cases, for provision of fully personalised cards, including routing to the holders.

  - Were the software companies responsive ?
  The software is developed or adapted by providers based on free libraries provided by SESAM-Vitale, and then directly sold to health professionals. Each release is tested and certified by SESAM-Vitale. Professional expect the products to be certified. So, software companies simply have to be responsive.

- What role did the smart card play in matters of acceptance/friendliness ?
Users were already familiar with smart cards; as the final result of the whole operation was simplification of the procedure and better delays, it was very well accepted

- Was usage of smart cards felt as a support for respect of private information ?
Not particularly

Alternative technologies or processes used or envisaged as enablers, during the meantime ?
If so, how did you organise the transition to full-wedged electronic transactions ?
--

Project Deployment

- What is the size of your smart card project (number of cards …) ?
More than 40 million cards at the moment – extra 5 million expected in the near future

- What is the current status of the project ?
Fully operational

- Is your present project rolled over from a pre-existing one ?
No

- If so, briefly describe your experience from such pre-existing project.
N/AP

What are the targeted phases of deployment ?
Fully deployed – only functional extensions considered – the next one for May 2002 – these are relatively minor changes

- What significant problems did you encounter ?
None

- Has the project reached its goals ?
Yes

-What are the cost drivers in your projects ?
Did not answer

- Is the cost of the usage of smart cards perceived as high ?
No. The unit cost of a personalised smart card is estimated 2,30

- If that is the case, why did you decide to make that choice anyway ?
N/AP

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Not available

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
Not in the mid term – a major change would be very expensive

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
Certainly not

- Which new services are considered in your existing application ?
See above

- Do you consider re-using the same smart cards for additional applications ?
No

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
N/AP

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
N/AP

- Which benefits are you expecting from that change ?
N/AP

Process

- Please describe the smart card personalization & delivery process.
The smart card is generated by SESAM-Vitale upon request of one of its members (usually the CNAM) when rights appear

- Please describe the registration process.
N/AP

- What have been the training requirements for personalisation agents and Registration Authority agents ?
N/AP

- Please describe your support efforts for the end user.
N/AP

- Please describe any documentation you might make available to the end user.
See Sesam-vitale Web site

- What has been the user reaction and feedback to your project ?
Excellent for the insured persons

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
N/AP

- Which new issues did you discover (during the project) ?
N/AP

- Do you have a published liability scheme ?
N/AP

- What are the commitments of each category of partners ?
N/AP

Archival

- Are there any retention requirements for documents in this project ?
Out of scope – concerns the application itself

- Are there any time stamping requirements for this project ?
N/AP

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
see above

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
No PKI

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
By the time of the decision, there was only one available technology considered mature enough (Bull CP8)

- What were the arguments in favour/against a smart card ?
See above

Smart card

- What are the main features of the smart card ?
Only storage of information

- Does your Smart Card support other applications or is it a single application card ?
No

- What are the cryptographic features of the smart card in your project ?
None

- What is the PKI related content of your smart card ?
None

- If the smart card is used for electronic signing, what is the exact role of the card in the signing process ?
N/AP

- What authentication mechanisms are used ?
N/AP

- Are there any other form factors involved ?
N/AP

- Is the smart card compliant with international security standards ?
N/AP

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
See above

- What are the main features of the smart card readers ?
All readers are potentially input-output devices, but used only in read mode, except the interactive terminals intended for update, located in a limited series of places (usually CNAM/CPAM offices)

Public Key Infrastructure

All that section is not relevant to the application.

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
N/AP

- What are the software requirements on the client side ?
Specific software (see above)

- Briefly describe the general technology requirements of your project.
See above

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
The French regulation of social security fully applies – the deployment of cards has been explicitly requested by the government

Digital signature

All that section is not relevant to the application.

CP / CPS (Particularly for e-Procurement)

All that section is not relevant to the application.

Data protection, consumers and confidentiality

- What specific consumer protections do you apply in your project ?
General legislation on privacy of data. The interactive terminals in particular allow the card holder to consult/verify the information contained in the card.

- What are the major data protection warranties you offer ?
Except with the interactive terminals that are located in particular offices, The cards may be read only under the control of a health professional card (bi-reader devices)

- What remains confidential ? For how long ?
N/AP

Survey of Secure Smart Card based eGovernment Applications

Answer given by the French Ministry of Home Affairs

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

- What is/are the application(s) in your project that is/are associated with the smart card ?
The project is a basis for many applications:

- *electronic identity card, allowing in particular access to e-government services where a proof of identity is requested*
- *electronic passport (through a chip inserted in the cover)*
- *voter card*
- *driver licence, including special features for truck drivers*
- *civil servant card, possibly including special rights (police…) and professional usage (access to premises or to data, electronic signature of administrative documents)*
- *elected representative card, providing access to particular administrative services*

In most cases, the same card (support) may play two or several of the roles listed above.

- Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
See above

- What is the role of the smart card in your project ?
Central – identify (and possibly authenticate) the holder in many occasions of his/her personal and professional life

- In case of a multi-purposes card, what will the card offer in common to several applications ? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?
Identification and authentication of persons, including possible ability to electronically sign, plus a basic set of access rights

- In your project, who will act as :

. Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?
See above the description of the various possible cards

. Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?
The French Administration (Préfectures) will manage the master registry, based on the book maintained in each town (état civil). the master registry will identify and authenticate each person

The local town halls will continue being the first access point

. Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?
According to the application.

. Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)
According to the application.

- In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
To be better defined later in the project

- What is the rationale for using smart card (technology, security, privacy, friendliness, etc) ?
Support already familiar to most people

- Was this chosen at once or through analysis / project analysis ?
Through analysis – however there was no serious alternative.

- What is the business model supported ?
Not relevant

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
The project is a significant part of the e-government requirements

- Who is/are the major stakeholders or driving force behind the project ?
The French government, and in particular the Ministry of Home Affairs (Ministère de l'Intérieur)

- How would you best describe the geographical scope of your smart card project ?
The whole French territory and, later when accepted and technically assessed, partner countries

- What is your target audience ?
All French citizens

- Do you consider inter-operability of your project with other projects using other smart cards ? If yes, how do you deal with this issue ?
Not precisely – however the card might be used to create electronic signatures

- Please give details on elements of your business model.
N/AP

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
The management is considered an important work, but not much more than the present procedures.

- During the project :
The project is still in preliminary phase, so no feedback information is available

- Was usage of smart cards felt as a support for respect of private information ?
The CNIL (Commission Nationale Informatique et Liberté), responsible for the respect of private information, strongly supports the project that is felt a better protection. Indeed, only a very reduced set of information will appear printed on the card, while extra info recorded in the card, will be available only to duly authorised people (under the control of their own professional card). This will be significantly more confidential than the present identity card.

Project Deployment

- What is the size of your smart card project (number of cards …) ?
Potentially, 60 million French citizens

- What is the current status of the project ?
Still on study

- Is your present project rolled over from a pre-existing one ?
No

- If so, briefly describe your experience from such pre-existing project.
N/AP

- What are the targeted phases of deployment ?
Unknown

- What significant problems did you encounter ?
N/AP

- Has the project reached its goals ?
N/AP

-What are the cost drivers in your projects ?
Still to be evaluated

- Is the cost of the usage of smart cards perceived as high ?
No, compared to the expected benefits

- If that is the case, why did you decide to make that choice anyway ?
N/AP

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
N/AP

Transitions to come, under process or completed

All these questions are felt irrelevant as the project is still under study

Process

- Please describe the smart card personalization & delivery process.
For citizens, the unique interlocutor is the town hall. The request is then forwarded to the préfecture, which controls the manufacturing process (personalisation). The card is then returned to the town hall where it is handed to the holder.

In other cases, in particular for civil servants and for elected representatives, other Administrations may be the right authority.

- Please describe the registration process.
Whatever the card requested, the process always begins with the "titre-fondateur" procedure that amounts to establish the authentication data of the person. It is made only once for each person, and then re-used for each request of a new card. There is no central directory of the population. The "état civil" books remain the basis of the identity of persons. The data of the "titre fondateur" are kept by the Administration (Préfecture) to support further creation of other cards and for renewal of existing cards.

- What have been the training requirements for personalisation agents and Registration Authority agents ?
N/AP

- Please describe your support efforts for the end user.
N/AP

- Please describe any documentation you might make available to the end user.
Working document: "Un projet du ministère de l'intérieur: le titre-fondateur et la refonte des titres d'identité" (Mr. Michel Aubouin, Ministère de l'Intérieur)

- What has been the user reaction and feedback to your project ?
N/AP

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
To be taken into account when precisely defining the project

- Which new issues did you discover (during the project) ?
N/AP

- Do you have a published liability scheme ?
Not yet

- What are the commitments of each category of partners ?
Usual commitments concerning official documents

Archival

- Are there any retention requirements for documents in this project ?
See above – archival of the data of the "titre fondateur"

- Are there any time stamping requirements for this project ?
No

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
To be defined

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
It has not been determined yet whether all citizen cards would be supported by a PKI. The only case where a PKI is found necessary is where electronic signature is expected to be a major feature of the applications, in particular for civil servants and elected representatives. In these cases, the PKI would be managed by the relevant Administration. Entrusting the PKI of an identity card requires careful risk management (problems linked with the usage of false cards or of stolen cards…)

For citizens, in the case where electronic signature would be found useful, no decision on the organisation of a PKI has been taken yet. The Ministry of Finance, in particular, is waiting for decisions to decide whether they will extend their PKI-based services to persons.

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
Not yet decided – should however be close to presently running smart card systems (SESAM-Vitale, bank cards…)

- What were the arguments in favour/against a smart card ?
No credible alternative

Note that among the data stored in the card there will be biometric elements: electronic images of the hand-written signature, of the fingerprint and photograph of the face; among these three data, only the photo will be printed on the card. Others are securely stored in the chip (non retrievable).

Smart card

- What are the main features of the smart card ?
Secure storage of information

In some cases, support of electronic signature keys and certificates

- Does your Smart Card support other applications or is it a single application card ?
See above

- What are the cryptographic features of the smart card in your project ?
According to the case – see above

- What is the PKI related content of your smart card ?
To be defined according to the project

- If the smart card is used for electronic signing, what is the exact role of the card in the signing process ?
Authentication of the holder (using a private key)

- What authentication mechanisms are used ?
To be defined

- Are there any other form factors involved ?
No answer

- Is the smart card compliant with international security standards ?
Certainly – to be defined

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Technology still to be chosen

- What are the main features of the smart card readers ?
Depends on the usage.

The police is experimenting two-readers devices that would allow them to read the authorised informationwithout having to enter the holder's private secret (pincode or other)

Public Key Infrastructure

Most generally, the PKI is not determined yet, so the following answers are very general directions.

- Do you manage the issuance of the certificates in house or do you outsource it ?
Should probably be managed in house

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
No answer

- What are the user registration requirements for certificate registration ?
Supported by the titre fondateur procedure

- What are the standards used in your project and for which specific purpose ?
To be defined

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
In some cases (civil servant, elected representative)

- What are the software requirements on the client side ?
To be defined – should be chosen for compliance with the smart card requirements (see DCSSI's requirements as well)

- Briefly describe the general technology requirements of your project.
To be defined

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
All legislation on equivalent paper documents, in particular the Code Civil

Decree on electronic signature (30 March 2001)

Specific texts will probably be necessary (to be considered)

Digital signature

- Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes, where supported

- What are your plans to roll out qualified certificates ?
It is not sure that the certificates distributed will be qualified ones, except for civil servants

- Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
No answer

- Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
To be defined (see the decree and refer to SGDN/DCSSI)

- Have you planned or accomplished any audits of your project ?
No answer

- Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
To be defined – however, probably not as the only liability is that the card was personalised from verified information and according to the written procedures.

In case of loss or theft, the holder is responsible for revoking the card, hence the corresponding public key certificate.

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
To be defined

- Do you make available any of the following such as a :

  - subscriber agreement

  - relying party agreement

  - consumer policy

  - privacy policy ?

To be defined

- Describe the approval procedures for your policies. Is there a designated Policy Board ?
To be defined

- Do you foresee any dispute resolution mechanisms ?
To be defined

- Have you undertaken ? Planned any cross certification with other CAs ?
To be defined

Data protection, consumers and confidentiality

- What specific consumer protections do you apply in your project ?
General legislation on protection of private data

- What are the major data protection warranties you offer ?
To be defined, if any

- What remains confidential ? For how long ?
Details yet to be defined.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the French Ministry of Finance

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

The TeleTVA project aims at generalising the collection of VAT data through a web site instead of the pre-existing EDI procedure with benefits for the companies (more flexible payment) and for the administrations (less errors due to copy).

It is a consequence of the Carcenac report.

The goal is to develop usage of electronic signature through referencing.

General

What is the application in your project that is associated with the smart card ?
Providing electronic (secure) procedures for tax declarations and possibly payment

What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
All agreed certification providers offer storage of the private keys in a smart card. However the usage of smart cards is optional and left to a decision of the end user.

Was this chosen at once or through analysis / project analysis ?
Left to the choice of agreed providers.

What is the business model supported ?
Two major ways of communication are proposed:

- *asynchronous communication (EDI type) through an intermediate operator; that solution does not use electronic signatures and therefore does not need smart cards.*
- *synchronous communication (electronic forms) directly connected to a web server; in that case, authentication of the declaring company through a Public Key Certificate is mandatory; usage of smart cards to protect the private key is optional.*

The major advantages generally expected are flexibility, reduction of errors and compliance with a strategy. In addition, the second solution and in particular the usage of smart cards are considered more user friendly.

The teleprocedures are a particular case illustrating e-government in France.

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
Benefits and comfort for the user, reduction of errors, compliance with a strategy.

Who is/are the major stakeholders or driving force behind the project ?
For establishing e-procedures, the Ministry of Finance.

For usage of smart cards, the holder decides.

- How would you best describe the geographical scope of your smart card project ?
All companies paying taxes in France (presently the VAT)

- What is your target audience ?
Enterprises only, now with income above 17 million euro and later all (at a time to be defined)

- Please give details on elements of your business model.
See above.

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
Not applicable

- During the project :

  What were the impacts of the new standards on the way of working (end users, central application) ?
  No answer concerning smart cards.

  - How was the cooperation with software companies ?
    Companies are interested in knowing the difficulties to integrate certificates and use those that are in the smart card (not standardised)

  - Were the software companies responsive ?
    Yes in general.

- What role did the smart card play in matters of acceptance/friendliness ?
No direct contact with users

Two real difficulties encountered :

- installation of the reader

- difficulty to extract the public key as the key pair is generated in the card; for security reasons, the policy prohibits generating the keys outside of the card, which would be easier

Average two (nominative) certificates per company were distributed. Around one third of users chose smart card.

- Was usage of smart cards felt as a support for respect of private information ?
No information (should be asked to CSPs).

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
The EDI declaration is still available and widely used by the larger companies..

Project Deployment

- What is the size of your smart card project (number of cards …) ?
--

- What is the current status of the project ?
Fully operational for the VAT (first stage).

- Is your present project rolled over from a pre-existing one ?
Yes, if we consider prior solutions such as the EDI.

If so, briefly describe your experience from such pre-existing project.
Not relevant for what concerns smart cards.

- What are the targeted phases of deployment ?
Not unavailable.

- What significant problems did you encounter ?
Unsufficient standardisation of cards to support electronic signature and lack of interoperability with IT systems. The problem is increased by the number of applications considered..

- Has the project reached its goals ?
Yes

-What are the cost drivers in your projects ?
Hotline is a significant consumer of work load – however the total load slightly decreases.

- Is the cost of the usage of smart cards perceived as high ?
Should be asked to users.

- If that is the case, why did you decide to make that choice anyway ?
--

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Should be asked to the Certification service Providers – it is their responsibility to include it into their costing analysis

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
Multicard reader should trigger the evolution.

Better standardisation of applications (there are many non standard interfaces but no real reason preventing standardisation initiatives)

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
Not yet

- Which new services are considered in your existing application ?
Should be analysed in the context of the creation of other services – interoperability and unique reader are requested.

- Do you consider re-using the same smart cards for others applications ?
Idem

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
--

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
--

- Which benefits are you expecting from that change ?
--

Process

- Please describe the smart card personalization & delivery process.
Depends on the provider (subject to the respect of referencing rules). A minimum set of requirements is given in the model Certificate Policy (PC type) published by the DGI.

- Please describe the registration process.
The company prove their existence through their identity. The managers of the company appoint a representative who personally identifies himself to the provider.

What have been the training requirements for personalisation agents and Registration Authority agents ?
--

- Please describe your support efforts for the end user.
Numerous publications available on the web site:

`www.impots.gouv.fr/e_services/tele_tva/accueil_teletva.htm`

- Please describe any documentation you might make available to the end user.
On the web et through a CD ROM

- What has been the user reaction and feedback to your project ?
Very positive

Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
Detailed in the PC type document (published on the Internet)

- Which new issues did you discover (during the project) ?
New difficulties (see other points in this answer)

- Do you have a published liability scheme ?
Detailed in the PC type document

- What are the commitments of each category of partners ?
Detailed in the PC type document

Archival

- Are there any retention requirements for documents in this project ?
Normal rules of the tax administration for the declarations and payment sheets. The declaring party must keep electronic archives at least for 4 years.

For what concerns PKI related aspects, the following items are required: configuration files, CPS, certification policies, agreements with other CAs (cross-certification if any), public key certificates, CRLs, receipts and notices, evidence documents provided by certificate holders.

- Are there any time stamping requirements for this project ?
Date and time are given by the application according to the contract between the company and the tax administration (actually, time of the server) – no signed timestamping but the time of transaction is archived.

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
Each PKI supplier may provide personalised smart cards.

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
Several agreed providers.

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
--

- What were the arguments in favour/against a smart card ?
--

Smart card

- What are the main features of the smart card ?
Secure storage of keys, generation of keys inside the card

Does your Smart Card support other applications or is it a single application card ?
The smart cards are intended for the sole usage of the tax teleprocedures, but the holders are free to use them for other applications if they wish so. Other usage of the certificate is favoured subject to the contractual terms between the CA and the holder (this is a strong asset for economical viability)

- What are the cryptographic features of the smart card in your project ?
Minimum described in the PC type document – minimum key length 1024 bits – key pair generation inside the card

- What is the PKI related content of your smart card ?
Standard certificate profile, i.e. the PKC of the provider. Minimum contents are given in the PC type document

- If the smart card is used for electronic signing, what is the exact role of the card ?
Signature of a MIME format which is archived by DGI.

- What authentication mechanisms are used ?
SSL V3

- Are there any other form factors involved ?
--

- Is the smart card compliant with international security standards ?
Depends on the provider

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Idem

- What are the main features of the smart card readers ?
Idem

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
Left to a series of up to ten agreed providers

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
No – the application directly recognises each Certificate Authority

- What are the user registration requirements for certificate registration ?
- *a request form*
- *a mandate signed by an authorised responsible of the company*
- *a copy of the companie's statutes*
- *two evidences of identity of the person who will be the declared certificate holder*

- What are the standards used in your project and for which specific purpose ?
X.509 V3 (certificates) RFC2459 (PC type)

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
No

- What are the software requirements on the client side ?
Any SSL V3 compliant web browser

- Briefly describe the general technology requirements of your project.
--

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
--

Digital signature

Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
No. Truth is based on the establishment of a authenticated and trusted channel.

- What are your plans to roll out qualified certificates ?
Not for the moment

Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
--

- Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
A specific accreditation scheme for the tax procedures. It processes in three stages:

- *analysis of the proposed CPS and CP for a pre-accreditation,*
- *audit through an independent office,*
- *technical assessment against a test bed.*

Accreditation is finally achieved through a decision of a particular committee.

- Have you planned or accomplished any audits of your project ?
Yes, for each in the accreditation process. Around 10 CSPs have been referenced up to now.

Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
--

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
The Ministry does not publish a CPS. there is a model CP (PC type) describing a set of minimum requirements for these documents. Finalisation and publication is the responsibility of each provider.

- Do you make available any of the following such as a :
  - *subscriber agreement* *Left to the provider*
  - *relying party agreement* *No (the only relying party is the application server)*
  - *consumer policy* *Left to the provider*
  - *privacy policy ?* *Left to the provider*

- Describe the approval procedures for your policies. Is there a designated Policy Board ?
The policies are validated against the model PC

- Do you foresee any dispute resolution mechanisms ?
--

- Have you undertaken ? Planned any cross certification with other CAs ?
No requirement in that sense.

Data protection, consumers and confidentiality
Data protection is left to each provider, that must always conform to the general legislation.

Germany

The major effort in Germany is oriented towards the usage of electronic signature. Indeed, the federal law includes precise provisions on the ways to establish – in particular – electronic signatures based on qualified certificates. The German legislation states, in particular, that qualified certificates are mandatory use in conjunction with secure signature creation devices – which may be translated by smart cards.

For these reason, most initiatives in e-Government are based on the usage of "qualified signatures'" i.e. electronic signatures falling under Article 5.1 of the European Directive on electronic signature.

The two domains investigated were:

- at regional (Land) level, the various usage that a government draws from standard smart cards in various administrative domains;
- at federal level, the public e-procurement project that should start operating in year 2002.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the German Land of Baden-Württenberg

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

What is the application in your project that is associated with the smart card ?
We test several applications: interactive e-services likes car registration, requests for agricultural funding, applications in the department of justice, e-mail.

What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
The objective is to provide e-services for citizen and enterprises to increase the speed and acceptance and to reduce the costs.

Was this chosen at once or through analysis / project analysis ?
This was a cabinet decision on the basis of the results of workshops, several working groups and commitees.

What is the business model supported ?
There is a special business model per application.

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
Cost reduction, improvement of administrational abilities of the state, meet expectations of citizens.

Who is/are the major stakeholders or driving force behind the project ?
Reform of the administration driven by the Ministry of Interior

- How would you best describe the geographical scope of your smart card project ?
state wide in Baden-Württemberg

- What is your target audience ?
enterprises, citizen, administration

- Please give details on elements of your business model.
see above: there is no general business model.

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
The technology is not yet easy to be implemented. Identification and authentication is possible with an accuracy of only about 70%, but 98% is necessary. Another problem encountered is that only personal signatures are possible, but "agency signatures" and "computer generated signatures" are needed, too. Finally, for life event automatization we need a signature card, that allows a batch-like processing of a series aof e-services after one authentication only; nowadays the citizen has to enter his pin for each of the various e-services.

- During the project :
These questions seem not much relevant.

- What were the impacts of the new standards on the way of working (end users, central application) ?

- How was the cooperation with software companies ?

- Were the software companies responsive ?

- What role did the smart card play in matters of acceptance/friendliness ?
The user doesn't consider the smart card as a token to make things easy.

- Was usage of smart cards felt as a support for respect of private information ?
Not yet.

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
Alternatives are passport services and smart card solutions on a legal basis, that allows an improvement as described above.

Project Deployment

- What is the size of your smart card project (number of cards …) ?
1000

- What is the current status of the project ?
There are several projects, some are in final acceptance test, some are still to be evaluated.

- Is your present project rolled over from a pre-existing one ?
Usually yes.

If so, briefly describe your experience from such pre-existing project.
--

- What are the targeted phases of deployment ?
2002-2003

- What significant problems did you encounter ?
The PC configuration of the user is often not adequate. The costs for the cards and card readers are much too high. The critical mass of applications is not in sight.

- Has the project reached its goals ?
Partially

-What are the cost drivers in your projects ?
Smart card support

- Is the cost of the usage of smart cards perceived as high ?
Yes, too high

(a smart card for electronic signature, valid for one year, is sold around 25 euro by SignTrust)

- If that is the case, why did you decide to make that choice anyway ?
What's the alternative?

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
--

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
??

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
We use qualified signatures, only

- Which new services are considered in your existing application ?
see our Action Plan in "`www.verwaltungsreform-bw.de`*"*

- Do you consider re-using the same smart cards for others applications ?
Yes, this is necessary to get accetance

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
Yes, but that is not the problem and it doesn't give the critical mass

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
depends on the application

- Which benefits are you expecting from that change ?
--

Process

- Please describe the smart card personalization & delivery process.
We use the IDENT-procedure of SignTrust (public provider). Please see details in the Internet

- Please describe the registration process.
We use the IDENT-procedure of SignTrust. Please see details in the Internet

What have been the training requirements for personalisation agents and Registration Authority agents ?
--

- Please describe your support efforts for the end user.
--

- Please describe any documentation you might make available to the end user.
--

- What has been the user reaction and feedback to your project ?
--

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
--

- Which new issues did you discover (during the project) ?
--

- Do you have a published liability scheme ?
--

- What are the commitments of each category of partners ?
--

Archival

- Are there any retention requirements for documents in this project ?
No

- Are there any time stamping requirements for this project ?
No

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
SignTrust only

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
SignTrust only

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
SignTrust only

- What were the arguments in favour/against a smart card ?
--

Smart card

- What are the main features of the smart card ?
please contact SignTrust

Does your Smart Card support other applications or is it a single application card ?
please contact SignTrust

- What are the cryptographic features of the smart card in your project ?
please contact SignTrust

- What is the PKI related content of your smart card ?
please contact SignTrust

- If the smart card is used for electronic signing, what is the exact role of the card ?
please contact SignTrust

- What authentication mechanisms are used ?
please contact SignTrust

- Are there any other form factors involved ?
please contact SignTrust

- Is the smart card compliant with international security standards ?
please contact SignTrust

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
please contact SignTrust

- What are the main features of the smart card readers ?
please contact SignTrust

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
We use the IDENT – process of SignTrust and the German Postal Service

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
No

- What are the user registration requirements for certificate registration ?
please contact SignTrust

- What are the standards used in your project and for which specific purpose ?
??

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
please contact SignTrust

- What are the software requirements on the client side ?
please contact SignTrust

- Briefly describe the general technology requirements of your project.
please contact SignTrust

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
--

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 ?
Out of legal requirements we only use qualified signatures.

Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
??

- Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
please contact SignTrust

- Have you planned or accomplished any audits of your project ?
Yes

Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
No

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
--

- 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
Data privacy is a complex subject. It cannot be handled this way.

- 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 ?

Survey of Secure Smart Card based eGovernment Applications

Answer given by the German agency for public procurement (Beschaffungsamt)

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

- What is/are the application(s) in your project that is/are associated with the smart card ?
electronic illustration of the law on public tendering and contracts (VOL, VOF, VOB)

- Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
single purpose smart card

- What is the role of the smart card in your project ?
replacement of the handwritten signature

- In case of a multi-purposes card, what will the card offer in common to several applications ? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?
--

- In your project, who will act as :

. Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?
staff member of the awarding institution, staff member of a company as tenderer

. Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?
all trust centers who supply qualified digital signatures according to the signature regulations

. Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?
--

. Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)
--

- In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
--

- What is the rationale for using smart card (technology, security, privacy, friendliness, etc) ?
obligatory requirement of the law on public tendering and contracts

- Was this chosen at once or through analysis / project analysis ?
--

- What is the business model supported ?
--

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
requirement of the law on public tendering and contracts, political intention

- Who is/are the major stakeholders or driving force behind the project ?
Federal Ministry of the Interior, Federal Ministry for Economic and Technology, Procurement Agency of the Federal Ministry of Interior, Federal Office for Building and Regional Planning

- How would you best describe the geographical scope of your smart card project ?
EU wide

- What is your target audience ?
tenderers

- Do you consider inter-operability of your project with other projects using other smart cards ? If yes, how do you deal with this issue ?
digital identification card; the development is already taken into account

- Please give details on elements of your business model.
Procurement agency will act as applications service provider. A detailed business model is on its way and will be presented in approx. 2 month

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
missing interoperability, no structures in other EU member states

- During the project :

What were the impacts of the new standards on the way of working (end users, central application) ?
delayed introduction of ISIS-MTT Standard. Missing specification details

- How was the cooperation with software companies ?
proprietary development and therefore no problems

- Were the software companies responsive ?
--

- What role did the smart card play in matters of acceptance/friendliness ?
easy handling was an important part of the development

- Was usage of smart cards felt as a support for respect of private information ?
--

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
--

Project Deployment

- What is the size of your smart card project (number of cards …) ?
not foreseeable since all tenderers who want to submit an electronic offer need to use a smart card

- What is the current status of the project ?
the first publication was on May 3rd. The first electronic tenders are expected by July 17th

- Is your present project rolled over from a pre-existing one ?
No

If so, briefly describe your experience from such pre-existing project.
--

- What are the targeted phases of deployment ?
development of the necessary functional concepts,

development of the necessary DV-technical concepts

technical implementation of the concepts

testing phase

pilot phase

actual operation

- What significant problems did you encounter ?
the project is a pilot project; therefore no comparable experience

- Has the project reached its goals ?
this question can only be answered at the end of the pilot phase in summer 2002

-What are the cost drivers in your projects ?
since a fixed price was agreed upon there are no price drivers at this time

- Is the cost of the usage of smart cards perceived as high ?
No

- If that is the case, why did you decide to make that choice anyway ?
--

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
--

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
The project "Öffentlicher Eink@uf Online" (Public Procurement online) defines new standards and will in further developments adjust to changes of technologies and regulations on contracting

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
these signatures are already part of the project

- Which new services are considered in your existing application ?
--

- Do you consider re-using the same smart cards for additional applications ?
yes, in the project "digital service card"

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
--

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
--

- Which benefits are you expecting from that change ?
--

Process

- Please describe the smart card personalization & delivery process.
the smart card can be purchased by the user at a trust center

- Please describe the registration process.
--

- What have been the training requirements for personalisation agents and Registration Authority agents ?
--

- Please describe your support efforts for the end user.
documentation, e-learning, hotline

- Please describe any documentation you might make available to the end user.
the documentation is part of the application

- What has been the user reaction and feedback to your project ?
so far quite positively

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
yes, because the important user of the system are the tenderers

- Which new issues did you discover (during the project) ?
the main point of discussion is a possible change of the law on public tendering and contracts

- Do you have a published liability scheme ?
--

- What are the commitments of each category of partners ?
see general terms and conditions (AGBs) under `http://www.e-vergabe.bund.de` *(Registrierung)*

Archival

- Are there any retention requirements for documents in this project ?
retention period of 10 years for contract file including all tenders

- Are there any time stamping requirements for this project ?
yes, submission of tenders by the tenderer in due-date time

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
all trust centers who supply qualified digital signatures according to the signature regulations

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
PKI is a proprietary development

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
internet technology, PDF documents

- What were the arguments in favour/against a smart card ?
obligatory requirement for use according to the law on public tendering and contracts

Smart card

- What are the main features of the smart card ?
qualified digital signature

- Does your Smart Card support other applications or is it a single application card ?
digital service card and other application which require digital signatures

- What are the cryptographic features of the smart card in your project ?
--

- What is the PKI related content of your smart card ?
--

- If the smart card is used for electronic signing, what is the exact role of the card in the signing process ?
replacement of the handwritten signature on valid tenders submitted by the tenderer

- What authentication mechanisms are used ?
--

- Are there any other form factors involved ?
--

- Is the smart card compliant with international security standards ?
yes

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
--

- What are the main features of the smart card readers ?
only smart card readers class 3 will be used because of security reasons

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
this task is managed by the trust centers

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
interoperability was an obligatory requirement of our project and is technically realized

- What are the user registration requirements for certificate registration ?
--

- What are the standards used in your project and for which specific purpose ?
available standards are integrated

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
yes, a signed Java-Applet was developed which supports the tenderer by submitting his tender. The tender itself is in PDF. The self-sign PlugIn from Adobe 5.0 was replaced by a proprietary developed PlugIn thus PDF-documents can be validly signed by qualified digital signatures

- What are the software requirements on the client side ?
standard PC, Windows NT or 2000, smart card and card reader

- Briefly describe the general technology requirements of your project.
see attached brochures

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
Code for Awarding Public Services Contracts, Freelance Performance and Public Works Contracts

Digital signature

- Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
yes

- What are your plans to roll out qualified certificates ?
already

- Plans to roll into Secure Signature Creation Devices 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 ?
currently a pilot operation is performed to test the realization

- Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
--

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
--

- Do you make available any of the following such as a :

  - subscriber agreement

  - relying party agreement

  - consumer policy

  - privacy policy ?

the entire awarding procedure - from determination of requirement to awarding and contract processing

- 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 ?
the tender remains confidential during the tendering period. Thereafter tenders are confidentially evaluated by technical and organizational methods

Italy

In Italy, the electronic identity card has been chosen as the major and common support of most applications requiring identification and authentication of users. The technical solution chosen is complete and complex and supports, in particular, qualified certificates.

Although initially conceived as able to support all kinds of usage, including local services to the citizen, the Italian smart cards are mainly used in the public administration. Several domains and applications use them, mainly for access control.

Following are three separate answers to the questionnaire that all have been collected by the CT-RUPA (Centro Tecnico per la Rete Unitaria per la Pubblica Amministrazione).

Survey of Secure Smart Card based eGovernment Applications

Answer given by the Italian Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione (CT-RUPA)

Network access control

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

What is the application in your project that is associated with the smart card ?
The main application is the « network access control »

What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
Security, privacy

Was this chosen at once or through analysis / project analysis ?
Yes

What is the business model supported ?
--

Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
The administartion to set the example

Who is/are the major stakeholders or driving force behind the project ?
Central Government (Ministry of Internal and Innovation and Technology), Local Government (Municipalities)

How would you best describe the geographical scope of your smart card project ?
All territory. In this phase thirty minicipalities

What is your target audience ?
Citizens

- Please give details on elements of your business model.
--

Difficulties

What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
Management,

- During the project :

  What were the impacts of the new standards on the way of working (end users, central application) ?
  Application

  How was the cooperation with software companies ?
  The cooperation must be high

  Were the software companies responsive ?
  The cooperation is medium

What role did the smart card play in matters of acceptance/friendliness ?
Is not accepted easily

Was usage of smart cards felt as a support for respect of private information ?
Yes

Alternative technologies or processes used or envisaged as enablers, during the meantime ?
If so, how did you organise the transition to full-wedged electronic transactions ?
None, at the moment

Project Deployment

What is the size of your smart card project (number of cards …) ?
Three millions until the beginning of next year and then 8/10 millions a year

What is the current status of the project ?
Phase 2 ; three millions of smart cards

Is your present project rolled over from a pre-existing one ?
No. But we had a phase 1 with 150.000 smart cards

If so, briefly describe your experience from such pre-existing project.
Not applicable

What are the targeted phases of deployment ?
Phase 2 : 3 millions Phase 3 : 8 millions until 30 millions of smart cards in the next 4 years

What significant problems did you encounter ?
Interoperability of cards of different vendors

Has the project reached its goals ?
Yes

-What are the cost drivers in your projects ?
The cost of smart cards and of the management infrastructure

Is the cost of the usage of smart cards perceived as high ?
Yes

If that is the case, why did you decide to make that choice anyway ?
To gain enough security in network transactions

Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
During the next phase we consider the cost for the citizen for single smart card. This cost is of 25 euro.

Transitions to come, under process or completed

Which new standards or infrastructures are you considering for the near future and midterm ?
We are considering the Directive 1999/93/EC for electronic signature and ISO 7816 for smart card.

Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
Yes

Which new services are considered in your existing application ?
Services based on the network access

Do you consider re-using the same smart cards for others applications ?
Yes

Can you accept relaxing the usage of the smartcards to less demanding requirements ?
Yes

Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
It's mandatory to change the organization of back office and front office to supply and manage the Data for network application

- Which benefits are you expecting from that change ?
Efficiency of the service to citizens, economicity of the public service and possibility to move employees from front office to back office.

Process

Please describe the smart card personalization & delivery process.
The personalization is on charge to organizations that implement security standards similar (but non so high) to Visa standards. The delivery is on charge to Municipality

Please describe the registration process.
--

- What have been the training requirements for personalisation agents and Registration Authority agents ?
--

- Please describe your support efforts for the end user.
--

- Please describe any documentation you might make available to the end user.
--

- What has been the user reaction and feedback to your project ?
--

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
--

- Which new issues did you discover (during the project) ?
--

- Do you have a published liability scheme ?
--

- What are the commitments of each category of partners ?
--

Archival

- Are there any retention requirements for documents in this project ?
--

- 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 (if any) ?
--

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
--

- What were the arguments in favour/against a smart card ?
--

Smart card

- What are the main features of the smart card ?
--

- Does your Smart Card support other applications or is it a single application card ?
--

- What are the cryptographic features of the smart card in your project ?
--

- What is the PKI related content of your smart card ?
--

If the smart card is used for electronic signing, what is the exact role of the card ?
The card is a SSCD in the sense of Directive 1999/93/EC

- What authentication mechanisms are used ?
--

- Are there any other form factors involved ?
--

Is the smart card compliant with international security standards ?
Yes

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
--

- What are the main features of the smart card readers ?
--

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
--

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
--

- What are the user registration requirements for certificate registration ?
--

- What are the standards used in your project and for which specific purpose ?
--

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
--

- What are the software requirements on the client side ?
--

- Briefly describe the general technology requirements of your project.
--

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
--

Digital signature

Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes, support article 5.1 signature

What are your plans to roll out qualified certificates ?
Yes

Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
Yes

Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
Yes

Have you planned or accomplished any audits of your project ?
Yes

Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
The risks are in charge of Central and Local Government where applicable

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
--

- 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 ?
--

Survey of Secure Smart Card based eGovernment Applications

Answer given by the Italian Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione (CT-RUPA)

Project number 1: Advanced signatures with Qualified Certificates

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

- What is the application in your project that is associated with the smart card ?
Many applications use smart card technology. The most important are "Mandato Informatico di Pagamento", "Libro Matricola Carabinieri", "Protocollo informatico", "Ruolo Unico dei Dirigenti". In total about 20.000 smart cards.

- What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
--

- Was this chosen at once or through analysis / project analysis ?
The rationale for using smart card is security; infact the italian norm states that, in order to achieve the requirements for an advanced signatures with Qualified Certificates, the smart card has to meet the ITSEC E3 level. So the choice of smart card is due to an accurate analisys.

- What is the business model supported ?
--

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
There is not a business model, because Centro Tecnico acts as a promoter for the dissemination of electronic signatures, without charges for Italian Administrations. So the main motive for deploying it is the political one.

- Who is/are the major stakeholders or driving force behind the project ?
Technological improvements and optimization of administrative processes.

- How would you best describe the geographical scope of your smart card project ?
It involves Central and Local Administrtations.

- What is your target audience ?
The mangers responsible of administrative processes.

- Please give details on elements of your business model.
Not applicable.

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
There have been human, deployment and interoperability problems.

- During the project :

  - What were the impacts of the new standards on the way of working (end users, central application) ?
  There have been many impacts, particularly the interaction between applications and smart card technology (PKCS#11, CSP).

  - How was the cooperation with software companies ?
  There have been some difficulties, because of conservative behaviour of some companies and also because of the complexity of the project itself, due to the lack of a leading project.

  - Were the software companies responsive ?
  Not always.

- What role did the smart card play in matters of acceptance/friendliness ?
A good one.

- Was usage of smart cards felt as a support for respect of private information ?
Yes.

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
Not applicable.

Project Deployment

- What is the size of your smart card project (number of cards …) ?
About 30.000 Smart cards.

- What is the current status of the project ?
3000 Smartcards.

- Is your present project rolled over from a pre-existing one ?
No.

- If so, briefly describe your experience from such pre-existing project.
Not applicable.

- What are the targeted phases of deployment ?
We plain to distribute about 10.000 smart cards during the current year.

- What significant problems did you encounter ?
The need of continuos adjustements of the project.

- Has the project reached its goals ?
Not yet.

-What are the cost drivers in your projects ?
Financial law.

- Is the cost of the usage of smart cards perceived as high ?
It's perceived as a justified cost.

- If that is the case, why did you decide to make that choice anyway ?
Not applicable.

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
We are working in this perspective.

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
None.

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
We are compliant.

- Which new services are considered in your existing application ?
Client authentication, personal identification, e-mail protection.

- Do you consider re-using the same smart cards for others applications ?
We have planned to use the same smart card for other applications, but only when the memory size will be sufficient for our scopes.

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
No.

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
Not now.

- Which benefits are you expecting from that change ?
Not Applicable.

Process

- Please describe the smart card personalization & delivery process.
Generation of keys inside the card, production of PKCS#10 (certificate request), PKCS#12 treatment, external personalisation, deliver to the final user.

- Please describe the registration process.
The italian norm requires that it must be performed a personal identification by the presentation of identity documents, and the subscription of an apposite request form.

- What have been the training requirements for personalisation agents and Registration Authority agents ?
The italian norms consider the role of qualified and authorized intermediates that can carry out the work needed for the registration process. These intermediates are trained by the Centro Tecnico. In every case the Registration Authority is centralized.

- Please describe your support efforts for the end user.
Documentation (Reference Manual, CBT, publicy available documents and software), Call Center and Electronic Messaging.

- Please describe any documentation you might make available to the end user.
Every useful documents are available on the Centro Tecnico website at `http://www.ctrupa.it` *and every user has his own reference manual and CBT.*

- What has been the user reaction and feedback to your project ?
A: We have not direct feedback, but we are certain of a good reaction, because we did not receive any particular claim.

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
Yes. As we said, this project has been well analyzed in respect of specific requirements.

- Which new issues did you discover (during the project) ?
We have taken in consideration other possible uses.

- Do you have a published liability scheme ?
No, but we are working in this perspective.

- What are the commitments of each category of partners ?
Not applicable.

Archival

- Are there any retention requirements for documents in this project ?
Yes.

- Are there any time stamping requirements for this project ?
Yes.

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
Single.

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
Single.

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
PKI based.

- What were the arguments in favour/against a smart card ?
The robustness, the portability, the potential multple uses.

Smart card

- What are the main features of the smart card ?
It performs advanced cryptographic funcions.

- Does your Smart Card support other applications or is it a single application card ?
Yes.

- What are the cryptographic features of the smart card in your project ?
RSA Keys generation, RSA for Signature/Verification and Encryption/Decryption - SHA-1 & MD5 for hashing functions .

- What is the PKI related content of your smart card ?
Private and public keys, X.509 certificate.

- If the smart card is used for electronic signing, what is the exact role of the card ?
It is used for signing the hash of the electronic document.

- What authentication mechanisms are used ?
The CHV is PIN.

- Are there any other form factors involved ?
No.

- Is the smart card compliant with international security standards ?
Yes.

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Durability, Security and portability.

- What are the main features of the smart card readers ?
Interoperability.

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
We manage the issuance in house.

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
Yes.

- What are the user registration requirements for certificate registration ?
We register only public employees belonging to administrations connected to RUPA (Unified Public Administration Network) .

- What are the standards used in your project and for which specific purpose ?
X.509v3 for certificate format, PKCS#7 for digital signatures, RSA for keys, SHA-1 for hash, TripleDes for encryption.

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
Yes.

- What are the software requirements on the client side ?
Cryptographic libraries must be compliant to the standards described above.

- Briefly describe the general technology requirements of your project.
Not applicable.

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
We act in compliance with the legal requirements, particularly the italian law.

Digital signature

- Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes, we supply advanced signatures with Qualified Certificates.

- What are your plans to roll out qualified certificates ?
See the above answer.

- Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
Yes.

- Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
We met the accreditation scheme specified in the italian law.

- Have you planned or accomplished any audits of your project ?
Yes.

- Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
No.

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
Our CPS is available at:

`http://www.ctrupa.it/firmadigitale/manualeoperativo.`

- Do you make available any of the following such as a :

- subscriber agreement

- relying party agreement

- consumer policy

- privacy policy ?

Not the consumer policy.

- Describe the approval procedures for your policies. Is there a designated Policy Board ?
No.

- Do you foresee any dispute resolution mechanisms ?
No.

- Have you undertaken ? Planned any cross certification with other CAs ?
We tested the cross certification with other italian CAs.

Data protection, consumers and confidentiality

- What specific consumer protections do you apply in your project ?
We grant the confidentiality of the personal information of the users, according with the italian law.

- What are the major data protection warranties you offer ?
Electronic data encryption and phisical protection in recording of documents.

- What remains confidential ? For how long ?
All the registration data not publicy available. Accordingly to the italian law.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the Italian Centro Tecnico per la Rete Unitaria della Pubblica Amministrazione (CT-RUPA)

Project number 2 : Multiservices organization card

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

- What is the application in your project that is associated with the smart card ?
There are three Organizations (Presidenza Consiglio Ministri, Ministero Beni Culturali, ENAC) that use smart card as organisation card, with function of advanced signatures with Qualified Certificates, personal identification (external personal data and photo, magnetic stripe), encryption, e-mail protection, authentication. In total about 10.000 smart cards.

- What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
--

- Was this chosen at once or through analysis / project analysis ?
The rationale for using smart card is security; infact the italian norm states that, in order to achieve the requirements for an advanced signatures with Qualified Certificates, the smart card has to meet the ITSEC E3 level. So the choice of smart card is due to an accurate analisys.

- What is the business model supported ?
--

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
There is not a business model, because Centro Tecnico acts as a promoter for the dissemination of electronic signatures, without charges for Italian Administrations. So the main motive for deploying it is the political one.

- Who is/are the major stakeholders or driving force behind the project ?
Technological improvements and optimization of administrative processes.

- How would you best describe the geographical scope of your smart card project ?
It involves Central and Local Administrtations.

- What is your target audience ?
The mangers responsible of administrative processes.

- Please give details on elements of your business model.
Not applicable.

Difficulties

- What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
There have been human, deployment and interoperability problems.

- During the project :

  - What were the impacts of the new standards on the way of working (end users, central application) ?
  There have been many impacts, particularly the interaction between applications and smart card technology (PKCS#11, CSP).

  - How was the cooperation with software companies ?
  There have been some difficulties, because of conservative behaviour of some companies and also because of the complexity of the project itself, due to the lack of a leading project.

  - Were the software companies responsive ?
  Not always.

- What role did the smart card play in matters of acceptance/friendliness ?
A good one.

- Was usage of smart cards felt as a support for respect of private information ?
Yes.

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
Not applicable.

Project Deployment

- What is the size of your smart card project (number of cards …) ?
about 30.000 Smart cards.

- What is the current status of the project ?
100 Smartcards (only for testing purposes).

- Is your present project rolled over from a pre-existing one ?
No.

- If so, briefly describe your experience from such pre-existing project.
Not applicable.

- What are the targeted phases of deployment ?
We plain to distribute about 10.000 smart cards during the current year.

- What significant problems did you encounter ?
The need of continuos adjustements of the project.

- Has the project reached its goals ?
Not yet.

-What are the cost drivers in your projects ?
Financial law.

- Is the cost of the usage of smart cards perceived as high ?
It's perceived as a justified cost.

- If that is the case, why did you decide to make that choice anyway ?
Not applicable.

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
We are working in this perspective.

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
Client authentication, personal identification, e-mail protection.

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
We are compliant.

- Which new services are considered in your existing application ?
Client authentication, personal identification, e-mail protection.

- Do you consider re-using the same smart cards for others applications ?
We have planned to use the same smart card for other applications, but only when the memory size will be sufficient for our scopes.

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
No.

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
Not now.

- Which benefits are you expecting from that change ?
Not Applicable.

Process

- Please describe the smart card personalization & delivery process.
Generation of keys inside the card, production of PKCS#10 (certificate request), PKCS#12 treatment, external personalisation, deliver to the final user.

- Please describe the registration process.
The italian norm requires that it must be performed a personal identification by the presentation of identity documents, and the subscription of an apposite request form.

- What have been the training requirements for personalisation agents and Registration Authority agents ?
The italian norms consider the role of qualified and authorized intermediates that can carry out the work needed for the registration process. These intermediates are trained by the Centro Tecnico. In every case the Registration Authority is centralized.

- Please describe your support efforts for the end user.
Documentation (Reference Manual, CBT, publicy available documents and software), Call Center and Electronic Messaging.

- Please describe any documentation you might make available to the end user.
Every useful documents are available on the Centro Tecnico website at `http://www.ctrupa.it` *and every user has his own reference manual and CBT.*

- What has been the user reaction and feedback to your project ?
We have not direct feedback, but we are certain of a good reaction, because we did not receive any particular claim.

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
Yes. As we said, this project has been well analyzed in respect of specific requirements.

- Which new issues did you discover (during the project) ?
We have taken in consideration other possible uses.

- Do you have a published liability scheme ?
No, but we are working in this perspective.

- What are the commitments of each category of partners ?
Not applicable.

Archival

- Are there any retention requirements for documents in this project ?
Yes.

- Are there any time stamping requirements for this project ?
Yes.

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
Single.

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
Single.

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
PKI based.

- What were the arguments in favour/against a smart card ?
The robustness, the portability, the potential multple uses.

Smart card

- What are the main features of the smart card ?
It performs advanced cryptographic funcions.

- Does your Smart Card support other applications or is it a single application card ?
Yes.

- What are the cryptographic features of the smart card in your project ?
RSA Keys generation, RSA for Signature/Verification and Encryption/Decryption - SHA-1 & MD5 for hashing functions .

- What is the PKI related content of your smart card ?
Private and public keys, X.509 certificate.

- If the smart card is used for electronic signing, what is the exact role of the card ?
It is used for signing the hash of the electronic document.

- What authentication mechanisms are used ?
The CHV is PIN.

- Are there any other form factors involved ?
No.

- Is the smart card compliant with international security standards ?
Yes.

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Durability, Security and portability.

- What are the main features of the smart card readers ?
Interoperability.

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
We manage the issuance in house.

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
Yes.

- What are the user registration requirements for certificate registration ?
We register only public employees belonging to administrations connected to RUPA (Unified Public Administration Network) .

- What are the standards used in your project and for which specific purpose ?
X.509v3 for certificate format, PKCS#7 for digital signatures, RSA for keys, SHA-1 for hash, TripleDes for encryption.

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
Yes.

- What are the software requirements on the client side ?
Cryptographic libraries must be compliant to the standards described above.

- Briefly describe the general technology requirements of your project.
Not applicable.

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
We act in compliance with the legal requirements, particularly the italian law.

Digital signature

- Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes, we supply advanced signatures with Qualified Certificates.

- What are your plans to roll out qualified certificates ?
See the above answer.

- Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
Yes.

- Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
We met the accreditation scheme specified in the italian law.

- Have you planned or accomplished any audits of your project ?
Yes.

- Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
No.

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
Our CPS is available at:

`http://www.ctrupa.it/firmadigitale/manualeoperativo.`

- Do you make available any of the following such as a :

  - subscriber agreement

  - relying party agreement

  - consumer policy

  - privacy policy ?

Not the consumer policy.

- Describe the approval procedures for your policies. Is there a designated Policy Board ?
No.

- Do you foresee any dispute resolution mechanisms ?
No.

- Have you undertaken ? Planned any cross certification with other CAs ?
We tested the cross certification with other italian CAs.

Data protection, consumers and confidentiality

- What specific consumer protections do you apply in your project ?
We grant the confidentiality of the personal information of the users, according with the italian law.

- What are the major data protection warranties you offer ?
Electronic data encryption, phisical protection in recording of documents.

- What remains confidential ? For how long ?
All the registration data not publicy available. Accordingly to the italian law.

Spain

In Spain, the programmes for the creation of an electronic identity card and for the provision of smart cards to support identification and authentication of civil servants are presently separate.

The national PKI that distributes private key certificates to the civil servants, both at central and at national level, is managed by the Fabrica Nacional de Monedas y Timbres, usually abbreviated by MIN or by FNMS.

It has begun distributing smart cards to some categories of users, according to the requirements

The folowing are the results of a joint meeting with the Ministry of Public Administration and with representatives of the MINT.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the Spanish Ministry of Public Administration - Consejo Superior de Informatica (MAP/CSI) and the Fabrica Nacional de Moneda y Timbre (MINT)

FOREWORD

Law in Spain has evolved in 1992 so that electronic procedures may acquire a full legal value.

The following has to be considered:

1. General security policy for the General State Administration is provided by the Consejo Superior de Informática. Particularly the 'Criteria of security' (see `http://www.map.es/csi/criterios/index.html`)
2. Fabrica Nacional de Moneda y Timbre is one provider of certification services among others, though it has a special status by RD 1317/2001 in a free market environment. Currently main services of FNMT are provided for the Agencia Estatal de Administración Tributaria and for the Seguridad Social. (see also `http://www.cert.fnmt.es/mapa.htm` section 'Aplicaciones').

The following questions are not answered for a specific application but taking into account the previous two points.

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

What is the application in your project that is associated with the smart card ?
It is not restricted to a specific application; services considered are citizen´s card, civil servant´s card, eGovernment services, etc.

What is the rationale for using smart card ? (technology, security, privacy, friendliness, etc) ?
1 - Security

2 - Privacy

3 - Technology

Friendliness was not a reason

Was this chosen at once or through analysis / project analysis ?
In the case of services provided by FNMT, the SC technology was chosen by an expert group according to a Master Plan conducted in 1997

What is the business model supported ?
N/A

Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
1 - Economical

Who is/are the major stakeholders or driving force behind the project ?
Ministry of the Economy, Ministry of Public Administrations, Ministry of Science and Technology, Ministry of Internal Affairs

How would you best describe the geographical scope of your smart card project ?
National

What is your target audience ?
All Spanish citizens

Please give details on elements of your business model.
N/A

Difficulties

What were the critical obstacles to choose using smart cards (example: management, human aspects…)?
Interoperability,

Difficulty to buy SC reader for the citizen

During the project :

What were the impacts of the new standards on the way of working (end users, central application) ?
i.e. Re-engineering, new procedures ? "Technical answer" => Flexible use of smartcards,
Two drivers (1 for MS, 1 for Apple), two class of certificates

Difficulty to buy SC for the citizen

How was the cooperation with software companies ?
As usual, no particular problems

Were the software companies responsive ?
As usual

What role did the smart card play in matters of acceptance/friendliness ?
--

Was usage of smart cards felt as a support for respect of private information ?
--

Alternative technologies or processes used or envisaged as enablers, during the meantime ?
If so, how did you organise the transition to full-wedged electronic transactions ?
N/A

Project Deployment

What is the size of your smart card project (number of cards …) ?
Potentially millions of users

What is the current status of the project ?
Running, operational, mainly in Social Security

Is your present project rolled over from a pre-existing one ?
No

If so, briefly describe your experience from such pre-existing project.
N/A

What are the targeted phases of deployment ?
According to Master Plan

What significant problems did you encounter ?
N/A

Has the project reached its goals ?
Yes, according to expectations

What are the cost drivers in your projects ?
N/A

Is the cost of the usage of smart cards perceived as high ?
No : Cards cost ~13 € for a small project. The price to decrease for larger projects

If that is the case, why did you decide to make that choice anyway ?
N/A

Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Cards cost ~13 € for a small project

Transitions to come, under process or completed

Which new standards or infrastructures are you considering for the near future and midterm?
New mask to be created to support ISO v.2 standard

Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates)?
Yes

Which new services are considered in your existing application ?
General use for eGovernment services

Do you consider re-using the same smart cards for others applications?
Yes

Can you accept relaxing the usage of the smartcards to less demanding requirements?
Not at the moment

Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised…)?
Under consideration

Which benefits are you expecting from that change?
Interoperability between different Administrations

Process

Please describe the smart card personalization & delivery process.
--

Please describe the registration process.
1. Certificate request, 2. Presence to the registration authority.

What have been the training requirements for personalisation agents and Registration Authority agents?
MS Office general knowledge

Please describe your support efforts for the end user.
~ 6 persons in the end-user departments

~ 6 persons in a dedicated Call Center

Please describe any documentation you might make available to the end user.
Word + PDF documentation

What has been the user reaction and feedback to your project?
Very positive – number of questions per week very low -> essentially focused on the SC, version of software…

Were the organisation and responsibilities for the parties all taken into account at the beginning? How?
Yes, according to Master Plan

Which new issues did you discover (during the project)?
Not identified

Do you have a published liability scheme?
RD 1317/2001

What are the commitments of each category of partners?
RD 1317/2001

Archival

Are there any retention requirements for documents in this project?
Law 14/1999

Are there any time stamping requirements for this project?
Time stamping services are available

Suppliers

In your project do you use a single or multiple suppliers for smart cards ?
A single one today – a new mask is created for a future second one -> Objective: ID card

In your project do you have a single or multiple suppliers for your PKI (if any) ?
A single supplier: Entrust – IMPORTANT REMARK: one supplier for certification technology with SC is not sufficient. The risk is to be tied up with one single provider.

B. TECHNOLOGY USED IN THE PROJECTS

General

What technologies have been considered in the project?
Standard SC related technologies

What were the arguments in favour/against a smart card?
In favour: security, portability

Against: availability of SC readers
IMPORTANT REMARK: CITIZENS DO NOT HAVE SC READERS

Smart card

What are the main features of the smart card ?
RSA Keys, 1024 bits long keys, SHA-1, DES-3 + proprietary confidentiality mechanisms

32 Kb EEPROM – not all the memory is used – FAT 3 KB

Does your Smart Card support other applications or is it a single application card?
Multi application

What are the cryptographic features of the smart card in your project ?
See above

What is the PKI related content of your smart card ?
2 mandatory certificates + 1 optional for administrations

For Class 1 certificates – 15 data more

If the smart card is used for electronic signing, what is the exact role of the card ?
The SC signs ; verification + hashing are external

What authentication mechanisms are used ?
RSA

Are there any other form factors involved ?
Not identified

Is the smart card compliant with international security standards ?
PC/SC + ISO 7816

What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Durability, power, security

What are the main features of the smart card readers ?
PC/SC compliant

Social Security: old SC readers -> short buffers

National Id Card: project

Public Key Infrastructure

Do you manage the issuance of the certificates in house or do you outsource it ?
--

Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
Yes, under consideration

What are the user registration requirements for certificate registration ?
Presence of the Registration Authority

What are the standards used in your project and for which specific purpose ?
All relevant standards

Client side software

Are the smart cards used in your project used with Secure Signature Creation Devices ?
--

What are the software requirements on the client side ?
--

Briefly describe the general technology requirements of your project.
--

C. LEGAL ASPECTS OF THE PROJECTS

General

Could you describe the legal requirements that were considered in your project ?
Law 30/1992, RD 263/1996, RD 1317/2001; see `http://www.map.es/csi/pg3413.htm`

Digital signature

Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Yes

What are your plans to roll out qualified certificates ?
--

Plans to roll into Secure Signature Creation Devices 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.
TBC

CP / CPS (Particularly for e-Procurement)

Could you describe the main features of your CP / CPS ?
--

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 ?
Yes, the Consejo Superior de Informática

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 ?
Law 15/1999 on the protection of personal data, RD 994/1999 Regulation on the adoption of measures to protect personal data

What remains confidential ? For how long?
--

Sweden

The Swedish government chose a strategy rather different from the other Member States: they fully externalised provision of smart cards enabling electronic signature to a series of providers, among which, however, the Swedish post, still an administration, is the major one.

These providers are allowed to produce PKI based cards with personalised information, that are considered as a valid identity card as well.

The distribution of signature enabling smart cards is fully operational in Sweden. Qualified signature is not supported yet, but plans are ongoing in that direction.

The report hereafter summarises the answers given by the Swedish agency for public administration (Statskontoret).

Survey of Secure Smart Card based eGovernment Applications

Answer given by the Swedish national agency for public administration (Statskontoret)

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

The National Taxboard has a commission from the Ministry of Justice in this area. The goal is that one individual will only need one "electronic identity" to reach all of the government services.

The strategy is to get induviduals certificates for electronic identification and signatures through framework agreements within the current PKI-market. There are currently framework agreements with 5 service vendors for citizens certificates and 3 service vendors for certificates within the administration. The focus is mainly on the electronic identity and not on the carriers of the private keys. The electronic identity will be useful in different sectors for different purposes, for example e-government services, e-commerce and e-procurement etc. We think that the fast way to provide electronic identities to a large number of citizens is to start with mainly soft certificates but some will be smart card based.

There are two types of vendors for certificates to the public:

1. Banks wich already has a large number of Internet bank customers (3,5 million) already electronically identified

2. Vendors (The Swedish Post and Telia) wich has established PKIs and infrastructures to identify people regardless of location

There are three vendors of PKI services within the administration (smart card based):

1. Integris

2. Telia

3. The Swedish Post

General

What is/are the application(s) in your project that is/are associated with the smart card ?
All e-government services that will be available to the public through electronic identification and signatures. These will mainly be based on soft certificates but some might be on smart cards.

General electronic identities and electronic signatures and some times special electronic identities and signatures within the administration.

Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
Primary keys for electronic identities and signatures and within the administration sometimes secondary certificates based on the primary certificates key pairs.

What is the role of the smart card in your project ?
As an electronic identity

As a carrier for private keys.

Optionally as a visual ID-card

- In case of a multi-purposes card, what will the card offer in common to several applications ? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?
Common identification data and a specific certificate for electronic signatures (non repudiation). Some times secondary certificates.

- In your project, who will act as :

. Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?
Always a physical person as an individual or as a representative of an organisation or an employee within one Government agency.

. Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?
Vendors within the PKI market through framework agreements (The Swedish Post, Telia, Nordea and Integris). Most common card supplier to those vendors are Setec.

. Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?
The same vendors as mentioned above.

. Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)
The same as above with the exception of card readers which may some times come through the common PC vendors.

- In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
--

What is the rationale for using smart card (technology, security, privacy, friendliness, etc) ?
Security and the possibility for electronic signatures. To make the administration of identities easier.

- Was this chosen at once or through analysis / project analysis ?
--

What is the business model supported ?
There are several business models. Most frequent pay for smart card and some kind of cost for using the smart cards (yearly or transaction based etc)

Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
All of the above.

- Who is/are the major stakeholders or driving force behind the project ?
Means of electronic identification and electronic signatures is a must for the administration to be able to offer interesting services to the public and be able to communicate in a secure way with each other.

How would you best describe the geographical scope of your smart card project ?
National

What is your target audience ?
Two different:

Individuals (citizens etc) and organisations representatives (probably mainly soft certificates but some smart cards)

Civil servants (mainly smart card based certificates)

Do you consider inter-operability of your project with other projects using other smart cards ?
If yes, how do you deal with this issue ?
Yes since there are several different vendors/supplier and we consider interoperability with smart cards already issued by the vendors mentioned above.

Please give details on elements of your business model.
Buy from the existing PKI and smart card vendors within the market. Those who has an infrastructure or those who already has a lot of people already identified by electronic means.

We buy this as a holistic solution and as a service not as products.
Pay for the certificates or usage of certificates to individuals or organisations representatives to get a critical volume to make it interesting for the administration to offer and set up e-services.

Difficulties

What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
Earlier there have been some example where deployment of smart cards to the public for electronic identification and signatures led to a lot of questions to the support/helpdesk. This was mainly because of the client software and card readers.

- During the project :
- What were the impacts of the new standards on the way of working (end users, central application) ?

How was the cooperation with software companies ?
--

- Were the software companies responsive ?
--

- What role did the smart card play in matters of acceptance/friendliness ?
--

- Was usage of smart cards felt as a support for respect of private information ?
--

- Alternative technologies or processes used or envisaged as enablers, during the meantime ? If so, how did you organise the transition to full-wedged electronic transactions ?
--

Project Deployment

What is the size of your smart card project (number of cards …) ?
We hope that the entire Swedish population will get PKI-based means for electronic identification and signatures. The highest volumes will probably be soft certificates but some will be smart card based. There are currently about 160 000 PKI-based smart cards with a general set of data for identification and electronic signatures. These are not yet used by the Government agencies in their e-services but they will be.

We hope that the number of Government agencies using smart cards within the agencies will grow. There are currently two large agencies using PKI-based smart cards totaly about 30 000 cards. We know that several more are currently setting up PKI:s based on smart cards. There are a couple of agencies using not PKI-based smart cards.

- What is the current status of the project ?
The projects task is to get PKI-based smart cards and other PKI services available for the Government agencies and make them use these services.

- Is your present project rolled over from a pre-existing one ?
A lot of activities is going on and the project is not and have not been a pre-existing one.

- If so, briefly describe your experience from such pre-existing project.
--

- What are the targeted phases of deployment ?
Set up strategy ready September 2000.

Requirements for Framework agreements, ready March 2001

Evaluation of offered solutions and vendors, ready November 2001

Co-ordinate purchases from framework agreements, ongoing

First major purchases, August 2002 about 100 000 certificate pairs for Governments use and the first for The National Insurance Boards services to Parents

- What significant problems did you encounter ?
--

Has the project reached its goals ?
No the goal is to get a wide spread use of PKI within the Government agencies and for individuals use towards the Governments agencies. We're progressing in that direction.

-What are the cost drivers in your projects ?
Smart cards and software needed on the client side CSP (Cryptographic Service Providers/PKCS#11 support) and for electronic signatures.

Cost of registration of people applying

Cost of availability and services:

Support/helpdesk

Revocation service

Directories

etc

- Is the cost of the usage of smart cards perceived as high ?
Yes in comparison with other techniques such as soft certificates.

If that is the case, why did you decide to make that choice anyway ?
We have not made that choice. The choice we have made is on the certificate format and key usage which are the same regardless of soft stored certificates or keys stored on smart cards.

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Yes we have a pricelist from each vendor. Included in the cost however are the cost of indentifying the coming cardholder and distribution and support and helpdesk.

We choose vendors/CA depending of the total cost and degree of requirements they could meet.

Transitions to come, under process or completed

Which new standards or infrastructures are you considering for the near future and midterm ?
Really not that many, one considered is XML-signatures.

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
We will sooner or later

- Which new services are considered in your existing application ?
--

- Do you consider re-using the same smart cards for additional applications ?
The smart card is only intended for carrying the electronic identity and the possibility for electronic signatures (main reason for PKI). Since the identity is totally unique and identify the holder to anyone it can be used for everything requiring that the card holder identifies him or herself.

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
No with some exceptions if for example within the administration one chooses to put a magnetic stripe on the card for passing through doors etc. One other exception could be as a token for symmetric cryptography (file encryption) or application specific authentication (could be for example windows log on).

- Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
--

- Which benefits are you expecting from that change ?
--

Process

- Please describe the smart card personalization & delivery process.

- Please describe the registration process.
The person applying for a smart card visit the CA/RA or RA appointed by the CA and identify himself by an accepted mean of identification (ID-card, passport, Drivers licens).

The RA sends the information necessary to the CA or card issuing company.

When the card is issued the activation code (PIN) will be sent to the Cardholders official address (from the population register) and the card will be sent by recommended mail. This means that the cardholder have to identify him- or herself in order to get the card.

- What have been the training requirements for personalisation agents and Registration Authority agents ?
--

- Please describe your support efforts for the end user.
The idea of buying the PKI as a service is that the vendor/CA is responsible for support to the cardholder.

- Please describe any documentation you might make available to the end user.
--

- What has been the user reaction and feedback to your project ?
--

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
--

- Which new issues did you discover (during the project) ?
--

- Do you have a published liability scheme ?
--

- What are the commitments of each category of partners ?
--

Archival

- Are there any retention requirements for documents in this project ?
--

Are there any time stamping requirements for this project ?
There were based on PKIX but no vendor could support a time stamp yet but they will develop it when the demands are high enough.

Suppliers

In your project do you use a single or multiple suppliers for smart cards ?
The vendor/CA are responsible. In practice there are two card suppliers to our vendors Setec and one more.

In your project do you have a single or multiple suppliers for your PKI (if any) ?
We have six different CA's alltough there are only two to three different technical solutions.

B. TECHNOLOGY USED IN THE PROJECTS

General

What technologies have been considered in the project ?
Soft certificates (pairs)

Smart card based certificates

What were the arguments in favour/against a smart card ?
Secure but expensive and difficult to deploy to the public.

Smart card

- What are the main features of the smart card ?
Authentication/key encipherment certificate and private key

Non repudiation certificate and private key

Optionally visual ID

- Does your Smart Card support other applications or is it a single application card ?
Electronic identification and electronic signatures where applicable

- What are the cryptographic features of the smart card in your project ?
RSA 1024 bits

The chip is protected according to ITSEC class E4

- What is the PKI related content of your smart card ?
PKCS#15 cards with two X.509 version 3 certificates format according to RFC 2459 and private keys:

Authentication and key encipherment

Non repudiation

- If the smart card is used for electronic signing, what is the exact role of the card in the signing process ?
Carrier of the non repudiation private key.

What authentication mechanisms are used ?
Primarily client authenticated SSL (class 3).

Sometimes authentication based on server side SSL (class 2) and specific authentication through some kind of challenge response. Depending on client and sometimes server software.

- Are there any other form factors involved ?
--

- Is the smart card compliant with international security standards ?
- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)

- What are the main features of the smart card readers ?
--

Public Key Infrastructure

- Do you manage the issuance of the certificates in house or do you outsource it ?
Outsource

- Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
--

What are the user registration requirements for certificate registration ?
See above

What are the standards used in your project and for which specific purpose ?
Certificate policy: Requirements based on ETSI QCP to find minimum level

Certificate format: RFC 2459 (soft and smart card based) for interoperability

Signature: PKCS#7 (soft and smart card based)

Card: PKCS#15

Client side software

- Are the smart cards used in your project used with Secure Signature Creation Devices ?
There always requirements of access control of the private keys regardless of if it is about authentication or electronic signature and if stored soft or in a smart card. This require some kind of client software or other technique (Java applet CBT). The card require some kind of CSP (cryptographic service provider).

What are the software requirements on the client side ?
We require that he certificate holder always has to type password or pin to activate a private key.

- Briefly describe the general technology requirements of your project.
--

C. LEGAL ASPECTS OF THE PROJECTS

General

- Could you describe the legal requirements that were considered in your project ?
--

Digital signature

Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
Advanced electronic signatures

What are your plans to roll out qualified certificates ?
It will come in the future

- Plans to roll into Secure Signature Creation Devices 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.
--

CP / CPS (Particularly for e-Procurement)

- Could you describe the main features of your CP / CPS ?
Requirements on content: ETSI QCP (altough no requirements on the structure) more common to have a RFC 2527 structure.

Different vendor has different CP:s /CPS

- Do you make available any of the following such as a :

  - subscriber agreement

  - relying party agreement

  - consumer policy

  - privacy policy ?

Every vendor has it's own but we did put requirements on content and some of these issues are regulated in the framework agreements

- 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 ?
Not yet but there might be in the future.

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 ?
--

United Kingdom

The United Kingdom kas a precise policy that is defined and maintained by the eEnvoy agency, a service of the Cabinet Office. In particular, eEnvoy published policy papers that each administration, national or local, must keep to. It is the case of a document named smart card framework that is freely accessible on the web site of the british government.

Provided that their solution complies with the framework, each application manager is responsible for acquiring the services from a provider and for defining their own policy.

To illustrate a typical application, eEnvoy described in the following pages the pilot project presently running in Southampton for the provision of local services.

Southampton happens to be the pilot site of a European initiative called Smartcities where a group of industries are experimenting such a usage of smart cards. Göteborg, in Sweden, is the second participating town.

Survey of Secure Smart Card based eGovernment Applications

Answer given by the British Cabinet Office on behalf of Southampton City Council (Smartcities)

A. GENERAL ENVIRONMENT AND ORGANISATIONAL ASPECTS OF THE PROJECT

General

What is/are the application(s) in your project that is/are associated with the smart card ?
Library

Leisure

University SmartCard

Public Transport- Specifically Bus

Toll Bridge

E-purse

PKI/Authentication

Loyalty

Schools catering & attendance monitoring

Will the smart card be a single or multi purposes one ? In case of a multi-purposes card, what are they ?
Multi-application and multi-owner. See above

What is the role of the smart card in your project ?
To provide cardholders with one card to access a number of different services. For certain applications the card can be used simply for its flash value (concessionary fares) for others like the PKI application the card is used to hold digital certificates and private keys.

- In case of a multi-purposes card, what will the card offer in common to several applications ? Only a vehicle for carrying data, a set of common identification data, key pairs and certificates, additional data or applications … ?
The card has a common content area: this includes name address, post code & DOB. Following our trial of the CEPS E-purse and provided that a high street bank becomes involved the e-purse would be common to a number of different application providers.

- In your project, who will act as :

. Cardholders (a physical person, i.e. an individual human being not a company/legal structure) who has been issued a smart card by a card issuer ?

. Card issuer(s), responsible for the issuance of smart cards to cardholders, defining the issuance policy, registering cardholders … ?

. Service Provider(s), responsible for providing services to the cardholder when using the smart card as an identification token and/or a secured environment in which to execute specific card applications ?

. Access provider(s), responsible for deploying and maintaining the infrastructure required for reading smart cards and accessing the services made available by the service provider(s)
The cardholders are individuals who have an interest in one or many of the applications on the card. The card issuance is currently carried out by both Southampton City Council (SCC) and the University of Southampton. The issuance policy/authentication framework has been created by SCC and endorsed by the wider consortium.

The service providers are and will be a mix of private and public organisations

Access providers- currently the infrastructure is provided by the application providers themselves. In the event that a common e-purse is developed it is likely that this is managed and maintain by the bank or its clearing provider.

In case the card issuer(s), service provider(s), access provider(s) are different entities, how are the relationships organised and responsibilities shared ?
This organisational model is still being worked on in Southampton. It is likely that some form of Joint venture company will result following the completion of the EC funded project.

What is the rationale for using smart card (technology, security, privacy, friendliness, etc) ?
In the first instance the project was setup to explore what the potential for a smart card in a multi-owner multi-application scheme might be. Already it has become clear that with effort existing barcode/magstripe and ID cards can be converted to be used with a smart card. This reduces the need to carry multiple cards. The use of the card for authentication and using full PKI provides excellent security. Simply introducing a smart card is innovative and has seen increased interest in certain application. Using the card on the toll bridge and for e-purse is very user friendly and much easier than previous methods. For use in schools and buses there is a reduction in the stigma associated with concessions. Bullying in schools is also reduced.

- Was this chosen at once or through analysis / project analysis ?
Through project analysis and some previous assumptions

What is the business model supported ?
Unsure of the question? Could you provide some explanation please

- Could you prioritise the main motives for deploying it ? (political, economical, tutorial, the administration to set the example, etc)
1 - Improving services to the customer

2 - Social benefits

3 - Political benefits linked to being considered innovative and therefore attracting inward investment.

4 - Financial savings

5 - Reliable digital ids for customers

- Who is/are the major stakeholders or driving force behind the project ?
Southampton city council, Southampton University, SchlumbergerSema

- How would you best describe the geographical scope of your smart card project ?
City focused leading to a regional developments

What is your target audience ?
Citizens of Southampton

- Do you consider inter-operability of your project with other projects using other smart cards ? If yes, how do you deal with this issue ?
Yes interoperability is key to the success of not just our project but to the long term viability of smart card schemes generally. Interoperability needs to be considered from a number of different angles: Do you want interoperability between applications? (Transport yes library perhaps not? Is interoperability affected by physical distance. Will you issue all cards with the same applications or will you allow all applications to be loaded on to a predefined standard card. SmartCities is currently investigating this with a number of cities throughout Europe. This group known as the SmartCities Interest

Please give details on elements of your business model.
Still undefined at this point.

Difficulties

What were the critical obstacles to choose using smart cards (example : management, human aspects …) ?
I have added not just difficulties but some suggestions

Get the user requirements right

Focus on needs of the people! - Marketing and focus groups

Do not under estimate the resource implications and staff training

Development of an authentication framework

Authentication levels must be linked to what the card is being used for

Cards with photo & name etc have intrinsic ID value- Authentication levels must be high

Cards should look the same-social inclusion

Scalable technical solution

Remember that technology is changing

Integrated the smart card into the wider E-government strategy

Benefits are not necessary financial

- During the project :

- What were the impacts of the new standards on the way of working (end users, central application) ?
We have tried to develop the card so that customers/cardholders use it in an identical or at the very least a similar way to before. We have adapted an existing department to accommodate the new requirements of the smart card scheme and we expect that department to either grow or merge in line with the scheme.

How was the cooperation with software companies ?
We have worked well with our commercial partners but we would suggest that a single contract is drawn up with the lead partner who has the responsibilities of the others.

Were the software companies responsive ?
Yes when required

- What role did the smart card play in matters of acceptance/friendliness ?
For Southampton City Council it was clearly an evolution from existing accepted card-based schemes and not a revolution.

Was usage of smart cards felt as a support for respect of private information ?
Yes

Alternative technologies or processes used or envisaged as enablers, during the meantime ?
If so, how did you organise the transition to full-wedged electronic transactions ?
Sorry I am unsure of the question

Project Deployment

- What is the size of your smart card project (number of cards …) ?
1000 cards issued. From April to September at least a further 10,000 cards planned

What is the current status of the project ?
First demo complete- This focused on technical ability of the card to support multiple applications. The next stage is to grow this with additional applications.

- Is your present project rolled over from a pre-existing one ?
No

- If so, briefly describe your experience from such pre-existing project.
--

- What are the targeted phases of deployment ?
April-September 10,000 cards for loyalty and authentication application

September 2000 cards for school pilots

September-December 6/8000 cards for toll bridge application

What significant problems did you encounter ?
Generally issues surrounded the changes in the service delivery rather than the technical issues. Technical issues were still prevalent.

- Has the project reached its goals ?
Yes but behind the original schedule

-What are the cost drivers in your projects ?
Hardware, software, human resources, both managerial and technical, wide geographical distribution of project partners

Is the cost of the usage of smart cards perceived as high ?
The cost of cards themselves is high and not just perception.

If that is the case, why did you decide to make that choice anyway ?
The project was tasked to establish what the benefits might be if there were any so it was clear that there were risks.

- Do you have breakdown elements to evaluate the cost of the project (unit cost of one smart card for setup/for usage, cost of management, cost of distribution …) ?
Yes we are working on a number of different models but they are commercial and in confidence

Transitions to come, under process or completed

- Which new standards or infrastructures are you considering for the near future and midterm ?
CEPS/a number of CEN standards, ITSO, Java (open platform)

- Do you consider migration of electronic signature to a scheme compliant with the art. 5.1 of the Directive (advanced signatures with Qualified Certificates) ?
We have made some tentative explorations in this direction. Our point of departure to data has been the UK Electronic Communications Act 2000.

- Which new services are considered in your existing application ?
Sorry I do not understand the question

- Do you consider re-using the same smart cards for additional applications ?
We are looking at adding a number of other applications to the scheme. These include ferries, the local football club, electronic voting etc.

- Can you accept relaxing the usage of the smartcards to less demanding requirements ?
Unsure of the question. Sorry!

Do you consider changing the topology of the organisation (from local to global, from centralised to decentralised …) ?
Yes but not specifically linked to the emerging smart card scheme.

- Which benefits are you expecting from that change ?

Process

- Please describe the smart card personalization & delivery process.
Application forms are collected from a number of different locations around the city this include both private and public areas. Completed application forms are taken with the associated documentation to a number of registration locations through out the city. These include all libraries and 9 of the 11 housing offices as well as a couple of central offices and the smartcities bureau itself. Applicants are expected to take a photo with them but in some offices we are able to take digital photos instead. Once the application form has been checked the individual retains his/her personal documents and the completed form is sent to the smartcities bureau for the card to be created.

Please describe the registration process.
See above

- What have been the training requirements for personalisation agents and Registration Authority agents ?
We have given staff specific training on how to accept an application for a SmartCities card. This has been backed up with comprehensive procedures. Most of the staff involved have previous experience in dealing with application forms and the registering of customers.

- Please describe your support efforts for the end user.
Telephone hotline, website Q & A, face to face customer enquiry desk

Please describe any documentation you might make available to the end user.
We provide a smart book, a brochure on the services and extensive information on website

- What has been the user reaction and feedback to your project ?
To date the feedback has been very positive. Some individuals have expressed concerns with the Big Brother issue but none of these have been cardholders.

- Were the organisation and responsibilities for the parties all taken into account at the beginning ? How ?
Sorry I am unsure of the question?

- Which new issues did you discover (during the project) ?
Sorry I am unsure of the question?

Do you have a published liability scheme ?
Te partners have their own public liability insurance schemes. The draft Certificate Policy includes a liability scheme.

- What are the commitments of each category of partners ?
Sorry I am unsure of the question?

Archival

- Are there any retention requirements for documents in this project ?
No

- Are there any time stamping requirements for this project ?
No

Suppliers

- In your project do you use a single or multiple suppliers for smart cards ?
Currently a single supplier

- In your project do you have a single or multiple suppliers for your PKI (if any) ?
Currently a single supplier

B. TECHNOLOGY USED IN THE PROJECTS

General

- What technologies have been considered in the project ?
PKI

Smart card- Java

J2ee

CRM

Https XML SSL Http

What were the arguments in favour/against a smart card ?
For: processing power, portability, ease of use, security

Against: cost of infrastructure (readers)

Smart card

What are the main features of the smart card ?
Do you mean the card face or the chip?

- Does your Smart Card support other applications or is it a single application card ?
See above

What are the cryptographic features of the smart card in your project ?
These include DES, T-DES, RSA and SHA-1. Microsoft Cryptographic Service Provider

What is the PKI related content of your smart card ?
Do you mean which application is relevant to PKI, if so, it will be used to authenticate citizens for secure electronic govt services using Web certs.

- If the smart card is used for electronic signing, what is the exact role of the card in the signing process ?
As part of the handshake between the authentication server and the smart card, the card will create a digital signature by producing a one-way hash from data generated randomly during the handshake and known only to the card and the server. This will be encrypted with the cardholder's private key and sent to the authentication server together with the cardholder's certificate containing his or her public key. The authentication server checks that the user's digital signature (the hash signed with the cardholder's private key) can be validated with the public key in the cardholder's certificate transmitted with the digital signature i.e. decrypted and the hash values compared.

What authentication mechanisms are used ?
As above & X509 v3 Digital Certificate

Are there any other form factors involved ?
No

- Is the smart card compliant with international security standards ?
Yes

- What were the criteria for choosing the smart card technology that was chosen in your project ? (durability, power, security, etc)
Led by Schlumberger.Sema, who is a leading card manufacturer.

What are the main features of the smart card readers ?
Card readers must be PC/SC compliant

Public Key Infrastructure

Do you manage the issuance of the certificates in house or do you outsource it ?
In House

Has interoperability with other PKIs been considered ? Particularly for e-Procurement.
Yes, but no actual work done yet

What are the user registration requirements for certificate registration ?
Same as Smartcard

What are the standards used in your project and for which specific purpose ?
X509v3 for certificates, LDAP for directory services, PKCS#10 and 7 for certificate request and return, also standards already listed

Client side software

Are the smart cards used in your project used with Secure Signature Creation Devices ?
Not on the client side

What are the software requirements on the client side ?
Microsoft Cryptographic Service Provider DLL, PC/SC Card Reader drivers

Briefly describe the general technology requirements of your project.
As described within this document

C. LEGAL ASPECTS OF THE PROJECTS

General

Could you describe the legal requirements that were considered in your project ?
Primarily this was liability, the DPA and the privacy issues

Digital signature

Does your project support electronic signatures in the meaning of Directive 99/93 on electronic signatures ?
N/A

What are your plans to roll out qualified certificates ?
None

Plans to roll into Secure Signature Creation Devices as specified in CEN-CWA 14167-172.
None

Has your PKI taken into account any accreditation schemes ? Have you planned or accomplished any accreditations ?
Will be looking to become T Scheme compliant at a later date

Have you planned or accomplished any audits of your project ?
Only internally

Do you make available an insurance policy for your project ? Please describe the risks covered and the liability caps.
Existing Southampton City Council public liability insurance

CP / CPS (Particularly for e-Procurement)

Could you describe the main features of your CP / CPS ?
Based around RFC 2527

- Do you make available any of the following such as a :

subscriber agreement		*Yes*
relying party agreement		*Yes*
consumer policy	-	*No*
privacy policy ?	-	*No*

Describe the approval procedures for your policies. Is there a designated Policy Board ?
Internal IS Board, Legal services

Do you foresee any dispute resolution mechanisms ?
Not at this stage. Existing SCC dispute resolution procedures will be used.

Have you undertaken ? Planned any cross certification with other CAs ?
None officially planned, however we do have aspirations in this area

Data protection, consumers and confidentiality

- What specific consumer protections do you apply in your project ?
Data protection procedures. Information on purposes for which personal data is collected is available on-line, by telephone and by written request. Information is anonymised prior to cross application / organisation analysis. Information is encrypted in data warehouse.

Terms and conditions of use give assurances on cardholder protection in so far as we agree not to load any applications on the card without the consent of the cardholder .

SCC has public liability insurance

- What are the major data protection warranties you offer ?
We are obliged by law to comply with the Data Protection Act. Warranties are not required.

- What remains confidential ? For how long ?
It is a requirement of the Data Protection Act that personal information is kept confidential from those not authorised to process it. Personal data must only be kept as long as is necessary for the purpose for which it is required so it's confidential for as long as it's kept.

The Certificate Policy defines the information that is considered confidential in respect of the PKI and the retention periods for this information.

END OF ANSWERS