

Access

Finance

Mobile Communications

Public Sector

Public Telephony

Transport



White Paper

e-ID and the Information Society in Europe

September 2003



axalto

A Schlumberger company

How e-ID can contribute to prosperity

Virtual communities' role in economic growth in Europe

⇒ Virtual communities' role in economic growth in Europe

For the last 10 years, the European economy has been growing at a rate slower than that of the United States. According to recent research, this difference of about 2% is due both to Europe's slower population growth rate and its lower rate of employment. Further compounding this lag in growth is the lack of connectivity required to bind individuals or associations of individuals together in the interest of improving productivity.

One answer to this problem is the "virtual community," a community of individuals with common interests, or involved in shared actions connected via the Internet or other collaborative networks. The tie that binds these relationships is Information and Communication Technology (ICT), particularly the electronic identity (e-ID) that serves to legitimate the credentials of otherwise "virtual" individuals or entities. This white paper covers the elements required to build such virtual communities.

Although virtual communities cannot alter the population growth rate, they can contribute substantially to people's participation in productive activities. Production is then not only a reflection of the "formal economy," but also of the "informal economy," which is driven by a population whose largest segment (more than 50%) will soon reach 60 years and over. It is an economic necessity that people be able to produce, work, assist, help and entertain one another as much as possible, and with a minimum of logistical restrictions. Virtual communities hold the promise to support this essential flexibility.

There is no doubt that the most affluent could probably do without a virtual community, even those in retirement and/or living in rural areas. But with respect to major statistics and to the economy as a whole, virtual communities are a valuable tool for overcoming the challenges and many physical restrictions that exist and will arise in the near future. Virtual communities not only help make the formal economy more flexible, they are especially useful in supporting the informal economy. They do so by optimizing the use of available service capacities with the additional consideration of outside restrictions.

Virtual communities are capable of supporting both a minimum level of services in rural areas and modern conveniences in highly developed metropolitan areas. There is no fundamental reason why successful electronic citizen (e-Citizen) services as offered in sparsely populated regions, - such as in Scandinavia and Australia - could not be applied to the problems of urban living. Here the physical distance might not be the main issue, but logistical and social reach can make it challenging to fully realize economic potential. Virtual communities are the answer to surmounting the difficulties of connectivity suffered by economic and social entities. This is the context of this white paper, which aims to introduce the "building blocks" required to create virtual communities. In order, this paper covers the following topics:

- Electronic identity, the most basic tool for organizing individual, personal data in the information society
- Trust mechanisms for business and privacy in the information society
- Typical services for virtual communities
- Exploitation of services and business cases
- Building virtual communities
- Knowledge organization
- Up scaling and boosting learning curves

⇒ Strong electronic identity

Electronic identity (e-ID) allows a person or legal entity to be recognized and legitimated online. This identity is entirely digital and is neither as redundant nor as overlapping as real-life identity. In the 'real world people recognize each other through a variety of characteristics and situations. In formal situations, for instance, a person can prove his identity by presenting official documents such as travel papers, passports, identity cards, permits, official extracts of government records, etc.

Online communication and transactions necessitate efficient, unambiguous, widely accepted identity, however. Theoretically, this identity could be based on a code or digitized stable biometrics produced by the individual. This presupposes the deployment of a central database containing all data associated with each set of codes or biometrics. In Europe it is widely preferred that the identity data are stored on a "token" incorporating a microchip. The most common token today is the smart card, with visual data and security features built into the credit-card format plastic card and the corresponding identity data stored on the chip. The bearer holds this card in his possession until the time of use.

For online use, it is not efficient, nor relevant to make complete different tokens for the same function in different environments. Proving your identity on health care is the same as proving your identity for travel purposes, although we are acquainted to the use of different cards in these different environments. This is mainly because the identification function is integrated in the specific other applications of these

cards. All over this white paper it is argued that the e-ID-function should be treated with a clear 'line of demarcation' with respect to all other functions. Applying standards for the cards, the data and for card issuing makes more sense than creating and maintaining different e-ID card bases for a range of applications that, in fact, use 95% or more of the same e-ID data.

To make the e-ID card feasible for all types of services, it is, of course, important that the chip technology comply with international standards. Moreover, the data on the e-ID card should be well defined, at least at the pan-European level. This would cover details such as the person's name and date of birth.

It makes sense to make the eID function independent from the different ways to read the chip, via a "contact" interface (i.e. bank cards) or a "contactless" interface (i.e. access cards). The chip can also be concealed, as with mobile phones.

Microprocessor chips also provide the security required to protect identity- and transaction-related data. There is also enormous potential to use the standardized e-ID data stored on the card for many services and applications requiring identification. The EID capability is not only of interest for the citizens, but also for the providers of online services

⇒ Trust

Identification is often required online whenever transactions are involved. The following questions can arise:

- Is the person really whom he claims to be?
- Can I trust the company or body offering the product or service?
- Will my company really receive a bank payment when I agree to deliver?

Rather than differentiate cards with respect to their individual applications, it would be far more relevant and efficient online to adapt services to the required level of trust. Standardized e-ID is a starting point, but additional features must be incorporated. To create strong authentication of individuals' identity, the citizens' credentials must be

checked online. The same goes for the qualified electronic signatures, used in online forms. The international supported technology for this 'trust' mechanism is named PKI (Public Key Infrastructure), and comes with security features incorporated into the IT components involved.

Not all e-services require complete application of all trust mechanisms. Any e-Service provider will have to choose the level of trust required to deploy the technology in question:

1. Can an e-Service provider take for granted that the identification communicated by the smart card is authentic, focusing in this case only on securing IT components?
2. Should the e-Service provider require authentication of the card offline or online? The latter requires authentication of the cardholder's identity through a PIN code or biometric feature, which is then checked against data stored securely on the chip. The former involves digital certificates and verification of external data concerning card validity, etc.
3. Should there be a form that the cardholder must sign as a clear and non-repudiated expression of his or her will?

To be sure that the citizen and the e-service provider leverage all the benefits of this technology, the PKI embedding must be clearly set in a framework of layers:

1. The upper layer is the national and international legal framework based on European Union (EU) directives.
2. The middle layer contains the conditional processes for the virtual communities. The most important are
 - a. The secure issuing and verifying the validity of certificates stored on the e-ID card
 - b. The secure issuance of cards and personalization of these with data and certificates
3. The lower layer concerns the processes of the transaction partners, applying e-ID operationally for strong authentication and/or qualified electronic signatures.

In many cases these types of strong, qualified trust services are offered in addition to the basic e-ID, by another company than the e-ID card issuer. In some countries, the trust provider is qualified to be also the card issuer, and allowed to use the official ID-data.

The certificates to check the identity and the electronic signature are easy to apply to e-Services. By introducing interoperability agreements among virtual communities, e-Services can be granted permission to use trust services developed initially for the e-ID.

⇒ e-Services

Establishing the e-ID and trust services is not an objective in itself. These two functions are performed in relation with the e-Services used by the consumer. The real objective is defining the pre-eminent e-service most likely to make the exploitation of a card base, and the 'trust'-infrastructure profitable.

Most services are related to a contribution toward economic or social needs. The starting point should be target groups with great potential to use and take advantage of e-Services. Typically, service providers focus on direct business and the highest-spending consumer groups. Many initiatives are oriented toward business and/or municipal government. But the greatest potential exists in support services for groups with a use for individual support and counseling, or with a genuine need to simplify logistics. Generally speaking, these groups include on the one hand professionals and consultants, teachers, patients.

On the other hand also groups which are often not targeted, such as elderly people, young families with children, disabled persons, unemployed workers, people living in rural or sparsely populated areas. These groups can take advantage AND contribute to the exploitation of e-ID card base when offered adequately, for the use of e-services which are relevant for these groups.

It is very likely that the e-Services requiring e-ID will grow exponentially following a pairing of broad-band infrastructure with individual

communication capabilities. Many services are today categorized by objective. The following list is based on data from the city and region of Eindhoven (Netherlands), but it could be representative of just about any active city or region in Europe. It offers a general overview of service opportunities linked to combining services with e-ID, qualified electronic signature and/or payment:

- e-Government: city board documents; administrative forms; online community systems in newly developed areas; municipal government websites and e-Commerce; city archives
- Healthcare/Culture/Social welfare: social security services; healthcare documents; e-Museums; ticket sales for one-day sports and cultural events; public libraries; digital genealogy; environmental information; cultural event listings; information on official bodies; information for senior citizens and volunteers; interest circles
- Healthcare: data exchanges among hospitals, physicians, pharmacists, etc.; patient records; health monitoring alert systems; treatment coordination; administrative forms
- Education: e-Learning systems; courses from multiple schools and/or academies; school-home-links; Web cafes; translation services for foreign citizens
- Employment and jobs: regional company information; interactive applications; interactive career counseling; job vacancies (from private-sector and government sources)
- Business: business portals; digital maps for companies and industrial parks; start-up centers; regional subsidies; company support centers
- Smart living (private sector): e-Services from retailers, newspapers, auctions, travel agents, banks, insurance agents and "smart home" ICT home automation services for convenience, care taking and safety
- Sports
- Public transportation
- Miscellaneous: smart parking, kiosks, e-ID cards, student hotspots

⇒ Business case-building

In most cases one party develops the business case for the exploitation of a complete card scheme: the basic e-ID services (exploitation of the base of tokens and infrastructure), the trust services (exploitation of the digital certificates) and e-Services are closely interrelated.

The card is used to strengthen the brand name of the exploiting party.

In keeping with these definitions, the cost of an e-Service with qualified electronic signature has to cover the basic e-ID service, the trust service and the e-Service, but it is not necessary to have these services all in one hand. This could lead to a vicious circle.

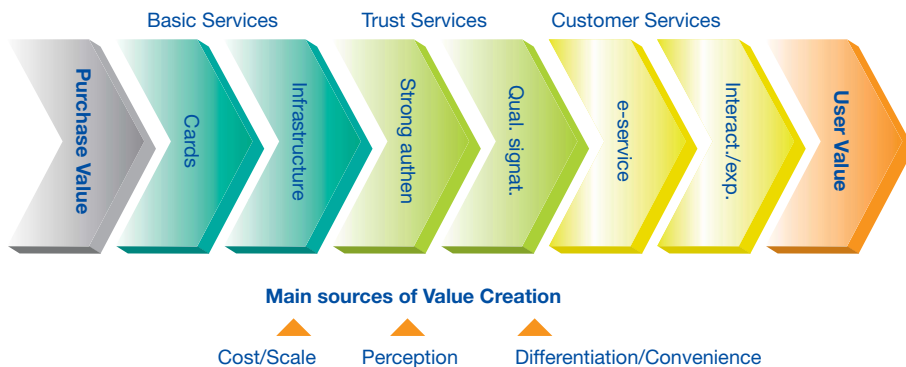
Investments in basic services could not be leveraged by profitable e-services. Services could not be developed without an existing card base. Simultaneous development is very tricky indeed.

Why?

Cards and infrastructure generally require a cost leadership strategy and/or large-scale production on the market; trust services for fail-safe protection require a perceived security strategy; and e-Services to satisfy the demands of the target group require a differentiation strategy. As a matter of course, this requires differentiation on the part of the suppliers, involved in the chain of 'value creation' for the citizens. No single enterprise could offer excellence in all three areas, as they require three distinctly different management styles and corporate cultures.

Another consideration is that the final e-service provider is the only one to be in the right position to develop the citizen's integration in virtual communities. They are, from a business perspective, the key drivers to upscale the card base, as the basis for the virtual community. Up scaling leads to cost reduction in the applied IT components in the basic services. Similarly, the higher the frequency of use, the lower the price per usage. In the case of multi-application or multi-service e-ID cards, the cost of the basic and trust services necessarily goes down as the number of cards issued and the frequency of usage of e-Services increase.

Value Chain



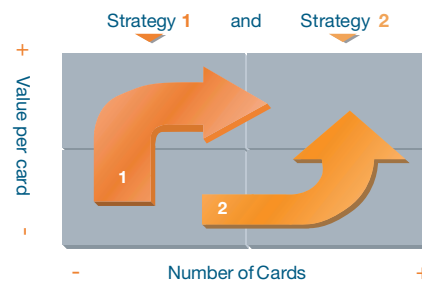
The key to business success can be summarized as an optimal reconciliation of a card base and infrastructure with e-Services. When it is assumed that the e-service providers are the best to develop the offer for the citizens, the basic services and e-services should be offered to him. The best contribution to of the basic services and trust services providers, to develop their case, is to offer e-service providers:

- High penetration of e-ID cards and trust services in their target areas
 - A competitive price for the basic and trust services related to e-services implemented.
- The first question to ask with respect to virtual communities is: how can profit per card be maximized? As each card represents a member of the virtual community, two strategies exist:
1. Building the virtual community by identifying and adding niches of consumers of high-level services that use the card frequently (i.e. physicians who sign prescriptions several times a day)
 2. Adding services to an existing card base within the community, and by doing so increasing the average frequency of use for the entire card base

The following diagram shows how these two strategies give a different way to maximize the total profit in a virtual community. Total revenue is calculated based upon the total number of cards and the average profit per card, minus costs.

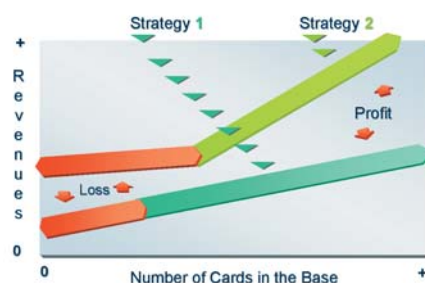
E-Services

Value per Card / Number of Cards



To illustrate the two strategies, the following diagram shows the trends of profit versus number of cards. In strategy two, investments tend to be higher and profits are delayed. Adding more e-services can substantially increase profits.

Profitability Trends



Policies and interoperability

With the creation of a virtual community, a single card would serve to prove a user's membership. All critical technical components used would be secure, and the card scheme operator would control the integrity of the card base, infrastructure and execution of critical roles through policies regarding:

- Roles to be implemented, with descriptions of goals, responsibilities, rights and obligations of the three main players: the card scheme operator, the e-Service provider and the cardholder.
- Trust policy (including the technical choices, how and when to deploy these choices) with statements related to the:
 - Issuing process for the e-ID card
 - Authentication of the cardholder (i.e. PIN codes and/or biometrics)
 - Association of the card with a front-office (PKI) database to verify certificate validity
 - Qualified electronic signature
 - Post-issuance additions and modification
- Technical policy with statements concerning multi-application standards and architecture for cards, terminals and infrastructure (including gateways/networks) and front-office systems
- e-Service policy, including compliance with regulations governing the acceptance and presentation of new services incorporating the core e-ID application into a card base, as well as financial policies for such use
- Business policy
- Interoperability policy, as discussed below

Knowledge organization

Virtual communities differ from industrial organizations in that:

- No physical meeting place or workplace exists. Access from anywhere, 24 hours a day, seven days a week, has replaced conventional business hours.
- Capabilities for instant, simultaneous processing catering to customer needs have supplanted step-by-step location-oriented operations overseen by specialists.

- Due to its early stage of development, IT with very short life cycles is generally deployed for ICT, but rapid implementations and adaptations and the roll-out of new services are nonetheless possible thanks to industry standards.

The traditional “pyramid” model with a small peak for mission and strategies and a broad base for operations is entirely irrelevant to a virtual community-based enterprise. Oriented toward exploiting knowledge, the modern enterprise will align with the concepts presented in this white paper through the establishment of four entities:

- A strategies and policies center
- An ICT technologies center, for building and maintaining the technical environment (terminal infrastructure and networks) of the virtual community
- A client support center, for building and maintaining individual relationships with members of the virtual community, especially cardholders (including during issuance)
- The business center, which is the entire set of all e-Services

There are no fixed views on the size of the entities. The strategies and policies center may in some cases be bigger than the others, and the relative sizes of all three could change temporarily to satisfy the evolving needs of the virtual community. Ideally, changes made by the different entities would be planned and carried out by steering committees through common projects.

With such type of organization, the virtual community can take the best of its business potential.

Knowledge Organization



⇒ Upscaling and boosting

The card scheme operator can boost both the growth of the virtual community and the use of services by:

- Acquiring new target groups and/or adding new services
- Arranging interoperability with the services of other communities, which stimulates growth in the card base and/or increased revenue through more frequent use of the cards and/or certificates

Growth of services offer

The strength of an e-Service with strong authentication and qualified electronic signature lies in:

- Availability of the service anytime, anywhere
- Simultaneously combining data from different sources
- Immediate and complete handling of administrative processes

The card scheme operator should look for opportunities where these strengths can pay off most. Examples include segments with users who must authenticate their identity frequently to access confidential and/or personalized data, or professionals who must validate official or legal documents with a qualified signature (i.e. doctors signing insurance documents or pharmacy prescriptions).

It is the responsibility of the card scheme operator to optimize the conditions in the virtual community most likely to further the development of e-Services. Once the card scheme operator has recognized the card base and infrastructure as a catalyst for development of e-Services, he can launch tools to boost growth in his community, such as smart labs, smart shops or smart factories. Such tools are helping e-Service providers to be the ultimate community booster.

The following incentives could be offered to potential e-Service providers to give birth to prototypes, pilot projects or small-scale start-ups:

- Hand on training and support for linking the e-Service application to the virtual community's e-ID, including the downloading

of applets

- Use of development tools and management systems (card management, invoicing, etc.)
- Test facilities for multi-application cards and interoperability (see below)
- Use of (a portion of) the card base, electronic signature certificates and the infrastructure at 'wholesale' rates (cost per identity registered for the e-Service; cost per certificate checked, cost per realized access of the e-Service, etc.)

Interoperability

The e-Service provider may offer his e-Service in more than one virtual community.

Interoperability is desirable, if not essential, to fulfilling the European information society's ambitions. Furthermore, the interoperability of e-ID could provide a pan-European access mechanism for all related e-Services. The operational architecture required to support truly flexible interoperability includes:

- Cards compatible with terminals all over Europe covered by the interoperability agreements of card scheme operators
- e-Services accessed independently from the card scheme operator that originally accepted and contracted the e-Service provider
- The PKI certificate check, or the qualified electronic signature, to be placed on any document of an accepted e-Service provider

To upscale the services offer, the card scheme operators will make interoperability agreements in which they mutually arrange:

- Mandatory identification data
- Operational architecture and technologies to be tested for interoperability
- Levels of trust, through assessment by both parties of critical processes like card and certificate issuing, post-issuance applet downloading, etc.
- Business issues, as presented here
- Legal issues, with respect to European directives, as well as to national laws (applicable responsibilities); codes of conduct for the protection of privacy; and the handling of complaints



The eEpoch project

A demonstration of e-ID's pan-European interoperability

⇒ Vision and objectives

European citizens require a secure and authenticated “digital identity” for certain services in the new information society, including many national and local government administration services and the private e-Commerce market. The eEpoch project aims to demonstrate the pan-European application's performance and the viability of open smart card infrastructures for electronic signatures with the provision of a European digital identity. It targets legally binding smart card-based services including e-Payment services, where relevant. eEpoch provides the necessary multi-application, cross-border environment required to validate the related deliverables of the eEurope Smart Card Charter initiative under real world conditions in several countries.

There will be seven pilot sites in six different countries. With active support from the national and local governments – a prerequisite for participation – each of the pilot sites is expected to provide the basis for extensive smart card roll-outs following the conclusion of each pilot project. While each site could accomplish this individually by applying smart card technology (using microprocessor chips capable of both storing personal data and creating a digital signature), the incompatibility currently suffered by ePurse and healthcare smart cards may very well afflict these developing communities in the absence of unifying standards and guidance.

User-focused, eEpoch is intended to improve transparency and provide access to all. Its long-term objective is to enable the European citizen using smart cards to benefit from

e-Government services in the physical world and over networks, anytime, anywhere and in complete privacy and security.

A key technical objective is the development of an implementation framework for smart cards in cooperation with the Japanese Government, which is participating in the definition of the eEpoch Framework specifications and the information exchange with the United States Federal Government. Both governments have already defined their version of a national common-access card and are well under way with their rollout plans.

⇒ Business and technical objectives

The specific business and technical objectives of eEpoch are to:

- Demonstrate the capability of smart card technology as a mainstream computing platform for trust
- Harmonize smart card-based infrastructures across sectors through implementation pilot programs, including Certification Authority (CA) interoperability systems and testing mechanisms/support
- Disseminate targeted information about implementations and the lessons learned among the user communities and all parties involved in the smart card business to encourage interoperable, compatible access mechanisms and infrastructures
- Ensure strong links to European and other standards efforts, basing deliverables on existing standards and contributing to standards organizations and possible maintenance where relevant

- Promote the widest availability and exchange of information on implementation frameworks and guidelines in order to encourage technical and other cooperation, both inside and outside Europe
- Establish and maintain strong communication links to equivalent initiatives in other regions (e.g. NICSS, Japan)

The main elements covered in the pilot project include:

- Specification of technical requirements for interoperable smart cards for electronic Identification, Authentication and Signature (IAS), the infrastructure and required services, in the aim of providing a clear picture of technically viable interoperable implementations and options
- Implementation of a Common European Digital Identity in support of e-Government services and the private e-Commerce market, and workable solutions for electronic signatures with a legal value (in compliance with requirements of both the “qualified electronic signatures” defined under Article 5.1 of the European Directive, and of the European Electronic Signature Standardization Initiative, or EESSI)
- Demonstration of interoperability for IAS in order to exploit e-Government services (government-to-government, government-to-business and government-to-citizen), such as:
 - Secure e-mail services
 - Access to government information (general and specific)
 - Transactions (i.e. form submission, permit application, transfer and settlement of funds)
 - Contracts and public procurement

⇒ How is eEpoch organized?

This two-year project (November 2002-October 2004) demonstrates pan-European interoperability of the smart card-based interoperable electronic identity, plus strong PKI-based authentication and qualified electronic signatures for e-Government services.

eEpoch is organized in four phases, each opening and ending with a conference:

- Preparation of the non-technical issues of interoperability in the pilot programs, followed by development of the technical specifications
- Implementation of the technical specifications for interoperability in each pilot program
- Testing and demonstration of interoperability in the pilot programs
- Evaluation and dissemination of results

The participating countries are France, Ireland, Israel, Italy, Spain and the United Kingdom.

Four work modules support the project:

- Knowledge research and the related knowledge portal (website)
- Dissemination
- Specification
- Operations support

eEpoch aims to coordinate its activities through:

- A white paper on e-ID and the Porvoo Group (coordination of European ministries of the interior with respect to e-ID, e-Authentication, electronic driver licenses, etc. every six months)
- Comité Européen de Normalisation (CEN)/Information Society Standardization System (ISSS) CEN Workshop Agreement on e-Authentication (in development), aimed at defining an informal standard and creating the implicit conditions for a European directive on e-ID and e-Authentication
- CEN ISSS Workshop agreement on qualified electronic signature (CEN ISSS CWA * “E sign” area K)
- Official activities concerning e-ID in the context of the CEN and the International Organization for Standardization (ISO)
- European Information Society Technologies (IST) Sixth Framework Program (FP6) concerning e-ID-related subjects

*European Committee for Standardization

⇒ Benefits

The end-user will experience the increased added value and ease-of-use of smart cards, which will lead to an improved market acceptance of smart card applications. Core capabilities for a pan-European Open Smart Card Infrastructure will be secured, and it is anticipated that this will provide the nucleus from which this infrastructure will grow, both in Europe and abroad (much like GSM networks). Public services in member states will be assisted to achieve their targeted percentages of government services online in the coming years.

Practical measures of success from eEpoch will include:

- Proven cross-border and cross-sector interoperability of pilot-scale IAS application systems
- The range of IAS-connected applications coordinated, as well as the completeness of practical guidelines produced
- Application of knowledge from European Economic and Social Committee (EECS) documents and related standardization processes
- Application of a common framework for smart card infrastructure (the Global Interoperability Framework, or GIF), leading indirectly to coordination with Japan and the United States
- Support mechanisms for national roll-outs of digital identification functionality
- A road map for holistic smart card e-ID environments and implementations

A long-term measure will be the influence of the applied architecture to business cases through:

- Large-scale production of cards and lowered manufacturing cost
- Elimination of unnecessary differentiation in trust-building certificate application
- Higher growth rates in the use of services that require government-supported identification, strong authentication and qualified signatures

eEpoch Projects at work

eEpoch pilot in France:

Issy les Moulineaux



Issy Les Moulineaux by night

City hall address: 62 rue du Général Leclerc, 92130 Issy-les-Moulineaux, France

André Santini, Mayor & Member of Parliament

Responsible for the eEpoch pilot: Mr. Eric Legale

Consulting company involved: Issy Media (Director Mr. Eric Legale)

Number of inhabitants: 55, 000

Characteristics of the city: southwest suburb of Paris.

The infrastructure

- The city of Issy is managing a number of public kiosks. The city wants to adapt these kiosks and provide access to cultural services (see later). This will not be operated in the first step, but later on.
- In the city museum, in the 'Mediatheque' and the 'Cube' cultural center: online networks are available, they will be accessed with the CVQ-card,
- PC readers for private access via the Internet. This requires a secure terminal application, to be emulated on the PC.

⇒ The electronic identity card

In France two cards will be introduced: CVQ (Daily Life card) under responsibility of the Ministry of "La Réforme de l'Etat" and the CEC (electronic Identity card) under the responsibility of the Ministry of Interior. The CEC card will use PKI for strong authentication and electronic signature and the first one should support PKI for this. The eEpoch Project will use the CVQ card, and start with a new JAVA-card base.

The identity data of the CVQ card used in the pilot, as well as the secure issuing process should be the same as for the CEC card. The CEC card will be standardized via AFNOR. It is accepted that this could have consequences that may follow from this CEC standard later. It is assumed that the chosen flexibility of JAVA-technology helps to control the consequences.

The trust mechanism for business and privacy Issy will follow the policy of using two certificates (one for strong authentication + optional for encryption and one for qualified signature)

An institute officially qualified, as Certificate Authority will do the certificate check.

The interoperability demonstration

The e-service offered by Issy, during the interoperability demonstration in 2004, allows citizens to access cultural services offered by the city (Médiathèque, le Cube, the city museum...). Announcements of cultural events are done on the Internet. The user clicks a form to order a ticket or a voucher. To avoid fraudulent orders, the users must authenticate themselves while filling in the form. In case of an electronic payment form (not yet decided), a qualified signature is required for non-repudiation.

This service will in principle be demonstrated from all cities involved, with all EID-cards and all certificates.

The implementation of services and the business cases

The implementation as foreseen now:

- For the CVQ Card, with two certificate for strong authentication and digital signature, no decision has been made concerning the way cardholders will get their cards (whether it will be sold or given to them)
- The future plan is to order an e-ticket via the CVQ that should give the user a discount on the normal ticket price. In the business case, Issy is planning that the e-service provider will have to take the discount for its own cost, and pay for the certificate checking process. The expected benefits are:
 - More revenues through additional ticket sales and less ticket handling costs.

Policies and interoperability

The city wants to use the ICT capabilities to offer services to the citizens. Issy wants to be one of the leading French pilots for CVQ and the CEC card. The use of the card should be offered primarily to service providers in social, educational and cultural bodies. Biometric authentication is not in the study scope. 'After-issuing-flexibility' is a key point in the technical policy. Interoperability to other cities will explicitly be promoted.

The knowledge organization

The city of Issy is considering the setting-up of "smart lab" to support the potential e-service providers, because the city wants to anticipate a very dynamic development of new services. The smart lab will be organized in cooperation with local / regional ICT-industry.

Up scaling and boosting learning curves

The first roll out strategy will be -via defining target groups- to issue cards in these groups and to offer dedicated services. As now, the city is considering Internet cafes for elder people, parents and employees of nurseries. The city is involving large companies in this roll out.

The second strategy is to assess the result services in other cities; issue cards in equivalent target groups in Issy, and makes an interoperability agreement. The first group to follow is "Telecities" in which Issy is also participating.

eEpoch pilot in Italy: Bologna



City hall address: Piazza Maggiore 6,
40100 Bologna

Responsible for the eEpoch project:
Fabrizio Boccola

Consulting company involved:
Engineering Spa

Number of inhabitants: 385,000

Characteristics: University city (oldest
University in Europe, founded in 1088),
with 100,000 students

The cardholder gets its personalized card, as part of a complete package including a card reader and PC software. The PC works like a local proxy with SSL connection.

In the past (till 1995) the city installed 40 terminals for its online services. They will be upgraded for smart card utilization.

The trust mechanism for business and privacy

In compliance with the Italian law, Bologna will issue two certificates, one for authentication and one for digital signature. Bologna does not consider biometric authentication. At this moment Bologna has a contract with BNL as CA, but in the future Bologna will work with more than one CA.

The Interoperability demonstration

Bologna is going to offer two services for the interoperability demonstration:

1. Foreign entrepreneurs starting a new business in Bologna can sign all the necessary electronic forms from their country with all cards that are interoperable in the eEpoch pilot.

⇒ The electronic identity card

The city of Bologna will use three types of card:

- CIE (Carta Identita Electronica) for the eEpoch interoperability demonstration. Thousands have been rolled out in Bologna. It is an official identity card. It contains basic personal data as well as an authentication certificate. The installed base, under national responsibility, is slowly growing.
- CNS (Carta Nazionale di Servizi), which is expected to roll out soon. This card contains the authentication certificate, while the digital signature is an option. The city is promoting the distribution of this card.
- CF (Carta Firma), containing a digital signature certificate, while the authentication certificate is an option. There are many of them, which are rolled out by acknowledged Certificate Authorities (CA) (most of them are dedicated branches of banks).

The Infrastructure

The infrastructure is completely Internet based, and communicates via a PC-browser with the cardholder.

Within the same application, the card will be used for authentication by an entrepreneur who wants to know the status of his/her request

2. Owners of grounds and houses in Bologna can handle their local tax forms from their country using the authentication and signature functions.

The implementation and business case

The citizen has to pay about 6 Euro for the CIE card. The national government and the municipality are responsible for the total budget.

The business policy for the CNS card is not yet determined. The municipality is responsible. Bologna has made available a start up budget. Talks will be opened with banks and university to specify the value of this card for their services, and build up a regular funding. The city itself will use the card for their online services via a service center. For this purpose Bologna has cooperation with 50 other Italian cities, to share investments and costs to develop e-gov services and to set-up a dedicated Service Center

Policies and interoperability

The city intends to develop its own service policy towards citizens via the CNS card. To extend the platform for local use as much as possible, the city will make the infrastructure interoperable for CIE and CF, using the two certificates for authentication and electronic signature. The city wants to offer services, which have high added value for relevant target groups in the city. Bologna is open for interoperability agreements with others on practical basis

The knowledge organization

The city and the university execute regular common consultations about strategies and policy. For the citizens the technical support is carried out by BNL, who offer the package for the Carta Firma. It is expected that BNL will also be contracted to make the call center available for the CNS card during the pilot. The municipal IT department is responsible for the technical support of the services. The city population register is the front office that issues the cards to the citizens.

Up scaling

The combined experiences in the eEpoch pilot will be used for decisions about upscaling. Technical and economical deployment plans are already underway, and will be refined based on the pilot outcomes.

eEpoch pilot in Italy: The INPS in Rome

INPS: Istituto Nazionale della Previdenza Sociale
Via Ciri il Grande, 21 - 00144 Roma (Italia)
Responsible for the eEpoch pilot:
Massimo Diana
INPS – Direzione Centrale Sistemi Informativi
Viale Civiltà del Lavoro, 46 - 00144 Roma (Italia)
E-mail: massimo.diana@inps.it
Number of clients: over 20,000,000
Number of clerks: over 30,000

INPS is the largest Italian public institution in the social insurance field. INPS has various institutional tasks, including the management of personal insurance contributions and positions, settlement, payment and management of pensions and other minor social benefits (unemployment benefits, salary integration, family financial support, disease and maternity allowances), to the most part of the categories of Italian workers.

INPS is the Italian national Institution which collect contributes (about 2 millions of registered enterprises) and provides pensions and other benefits to employed and self-employed workers (about 20 millions of benefits paid each month by telematics means).

INPS has HQ in Rome and local offices are located all over the Italian territory. Moreover INPS has many international co-operations with homologous Institutions. The geographic network (SNA and IP multiprotocol) provides connection to:

- About 600 LAN as many as the INPS offices located on the national territory.

- About 2,000 mobile users that act as vigilance inspectors.
- A large number of Italian Institutions qualified to access INPS data banks.
- Several Institutions in other European Member States for exchanging telematics information dealing with migrant workers in the context of TESS Program.
- All the Italian Banks for the payments of pensions and benefits.
- About 300 self-service kiosks located inside and outside the INPS premises (Post-Offices, Municipalities) dedicated to the distribution of social security services in integration with other Institutions.

Actually INPS is committed to distribute via Internet (see www.inps.it entry "servizi on-line") a large number of on-line services to both citizens and cooperating Institutions in Italy and abroad (i.e. cooperating Social Security Institutions in other countries or Italian Consulates in the world).

A dedicated large system is operating in INPS to welcome the request of connection trough internet, to identify the operator connected via user-id and password, to verify in the specific profile the authorization for operating and finally to start a VPN on-demand session with the client to establish a secure channel of communication.

The on-line services actually delivered by INPS over Internet include:

- Statement of personal contributory record;
- Provisional pension calculation;
- Pension claim status;
- Filling in and submission of e-forms (registration of some kinds of workers, income declarations, employers contribution declaration, claims for salary integration, claim for military service reunification, etc.)

Additional on-line services are likely to be delivered in the short-medium term. They require secure identification by means of PKI and smart cards. Such services include:

- Online multilingual services to foreign operators and citizens
- Payment of contributions (volunteers, home workers, etc) by credit card.

⇒ The electronic identity card

By the competent Authorities in Italy was introduced the national electronic identity card CIE (Carta Identità Elettronica). In anticipation of the mass roll out of this card, to facilitate the access to e-services provided by the e-government plan, a services card CNS (Carta Nazionale dei Servizi) has been introduced and distributed to a large number of citizens; the official identity data of this card (CNS) are the same as the national identity card.

A third type of card CF (Carta Firma) is set up in Italy by the Official Certification Authorities that are allowed to issue a card for qualified electronic signature. The eEpoch pilot of INPS will be based on the CNS card.

It is an ISO-7816 smart card, with fort INPS different entitlements for clients and for clerks.

The Infrastructure

The eEpoch pilot will use the operational Internet based infrastructure of INPS.

In such infrastructure, with the collaboration of partner FINSIEL, the new access technology via smart card will be integrated. The card will be distributed to the clients in a complete POSTECOM Kit for Window PC, containing: card with certificates on board, a (serial) card reader and software.

The trust mechanism for business and privacy INPS will accept and use the policy of two certificates: one for authentication and encryption and one for the qualified signature. For the pilot POSTECOM will be the Registration and Certification Authority and the card issuer as well.

The interoperability demonstration

The interoperability demonstration of INPS concerns the authenticated access of the INPS e-services also through the cards set up by Bologna Municipality. Moreover, it will be studied if it would be possible to use the smart cards of the other eEpoch pilots to access the INPS e-services. In this case it would be simulated that clerks, accredited by INPS in foreign countries, access the INPS database information.

The implementation of services and the business case

INPS follows strictly the 'lines of demarcation' model, separating (1) the implementation of the card, (2) the trust services and (3) the INPS e-services.

The issuing of cards is considered as the responsibility of the government, the trust service is the responsibility of the CA involved, and INPS is responsibility for the set up and delivery of services to its clients.

The POSTECOM Kit that today is sold for 100 Euro, it's a package complete with card, reader and software. About 500 similar packages will be free distributed to INPS clients and clerks in the eEpoch Rome pilot. In the future business case INPS will be one of the e-service providers using the CNS card. Profitable implementation of the card requires many services using the authentication/signature functions. INPS refers to Lombardia (Italian region with 9 millions of citizens), where the CNS card will be used for health care authentication and qualified signature and where FINSIEL is involved, too.

INPS will mainly invest in its online services for clients and clerks, and not in the development of the card and the trust services; the costs of the hardware and software infrastructure built by INPS to support the card use and the trust services are compensated by better services and their lower cost of delivery.

Policies and interoperability

INPS is a service provider that just wants to use the law based CNS/CIE/CF cards and trust services. This means that INPS accepts the national certificate policy and the national individual code (Codice Fiscale) to identify people. According to Italian law, no biometric is required for INPS, just PIN.

Due to the privacy Italian law, the vision is today that INPS, to allow other Institutions (national or foreign) the access to information of its Data Base, needs a formal Interoperability Agreement.

The knowledge organization

INPS has no other ambitions concerning the policy and card scheme strategies than as a service provider, who wants to get the best service for the price that he can afford.

The eEpoch Pilot Project it's for INPS the right opportunity to experiment on the field the use of smart cards as a key to access the on line services. To this aim INPS choose the collaboration of two qualified partners POSTECOM and FINSIEL to support the needed activities:

• POSTECOM as Registration, Certification Authority and card issuer;

• FINSIEL as provider of software services and assistance for the integration of the new card-based infrastructure.

The communication with the clients concerning the INPS services will be organized via the usual channels: INPS front offices, INPS call center, INPS web site, newspapers and so on.

Up scaling and boosting

INPS, in its role of services provider, will follow the government rolls out of the CNS/CIE/CF card.

eEpoch pilot in Spain: The Spanish police



■ Consulting company: Safelayer.

⇒ The electronic identity card

The political decision is taken that a national electronic identity card for strong authentication and electronic signature will be issued nationwide. DGP will have the role of card issuer, CA and “user” as well.

For the moment the smart card technology is based on ISO 7818, but it is not excluded that also JAVA technology is accepted, for reasons of post issuance flexibility. Constraints are oriented to costs and to security.

The Infrastructure

The infrastructure for the eEpoch pilot is defined, and deployed by the Spanish police. It consists of PC/SC card readers, and PKCS#11 based drivers, and OCSP network for certificate checks. Completely controlled by DGP. The technology is completely Internet oriented. The browsers to be provided should be based on PKCS#11. The infrastructure respects all requirements for the European qualified electronic signature. A biometric device (finger print) will be part of the authentication infrastructure. This will follow ICAO standards.

The trust mechanism for business and privacy DGP will act as the CA, and apply two certificates: one for authentication and encryption and one for the qualified signature. The police station is the front office for issuing the card. The population register supplies the ID-data.

The interoperability demonstration

The Spanish police will offer an “incident log” form via the Internet. The interoperability demonstration makes this form to be (qualified) signed with cards from those other eEpoch pilots with whom the Spanish police have made an interoperability agreement. It is studied to authenticate Spanish cards via foreign infrastructure, for Spanish citizens traveling abroad.

Business case

The EID card will replace the existing ID-card, which is generally used. The citizen has to pay for the card. The price today is about 6 euro. The price of the new smart card (substituting the old one) is not yet established. Any service provider to whom the citizen offers his/her card can use the public data of the card. It means not only that the ID data can be read, but also that the data can be authenticated via OCSP. The Spanish police are in this case one of the “users”. The price of this authentication service is not yet known.

Policies and interoperability

The new EID card will first of all be an ID-card, to be used at the Spanish territory. It is intended to use the EID card also as travel document. Two certificates will be applied, as well as a biometric file, according to ICAO standards.

The Spanish police is the one and only authority who could bring / change data in the chip. Service providers can use the public data, when the cardholder is presenting his/her card.

The interoperability concerns

- The use Spanish authentications and electronic signatures for foreign services.
- The use of foreign qualified signature under a Spanish document.

The knowledge organization

Policy and strategy concerning the card base is considered to be a political decision, executed by the ministry of interior.

The operational and technical support is completely assigned to the Spanish police.

The Spanish police have dedicated responsibilities for some semi public functions of the card.

All use of the public data by service providers is completely out of the responsibility of the EID organization. It is not yet decided if the service providers wanting to be able to authenticate the public EID data of the card should be “accredited”.

Up scaling

On the technical side, all is set to roll out five million cards per year, via the Spanish police.



About Schlumberger

Schlumberger Smart Cards & Terminals is the world's leading provider of microprocessor cards (Gartner 2003, Frost & Sullivan 2003) and a major supplier of card-related terminals and transaction software. Its 5,000 employees serve customers in more than 100 countries, with worldwide sales exceeding 2.6 billion smart cards to date.

Schlumberger continuously creates new generations of products for use in a variety of applications in the telecommunications, finance, retail, transport, entertainment, healthcare, personal identification, information technology and public sector markets.

Europe - Tel.: + 33 1 46 00 66 67

North America - Tel.: + 1 888 343 5773

South America - Tel.: + 55 11 34 44 76 00

Asia - Tel.: + 852 2956 3331

Japan - Tel.: + 81 3 3434 7300

* Mark of Axalto



axalto
A Schlumberger company