Chapter 17

IDENTITY MANAGEMENT FOR E-GOVERNMENT SERVICES

Fabio Fioravanti[1] and Enrico Nardelli[2]

[1]*Department of Sciences, University of Chieti-Pescara, Italy (fioravanti@sci.unich.it);*
[2]*Department of Mathematics, University of Rome "Tor Vergata," Italy (nardelli@mat.uniroma2.it)*

CHAPTER OVERVIEW

Identity management systems play a critical role in the field of e-Government and e-Business, as they constitute the basic building blocks enabling secure and reliable access to online services. In this chapter, we highlight the main technical and organizational pitfalls of current approaches to identity management which are either based on a centralized architecture or require adoption of common (technological and organizational) standards. We believe that these limitations can only be overcome by designing a common infrastructure which provides applications with transparent access to identity management services, independently of the underlying identity technology. Moreover, we describe the bridging backbone, an interoperability architecture based on a federation of national infrastructures which follows a cooperation-based approach and is fully compatible with and respectful of organizational and technical choices of existing systems.

1. INTRODUCTION

Building secure and effective identity management systems is a critical factor for the successful deployment of e-Government and e-Business services. Indeed, accurate and reliable verification of the electronic identity (e-ID) of the citizen requesting the execution of an online transaction is a prerequisite for customized delivery of high-value e-Services, which have to rely on an environment which provides protection from identity theft and fraud.

An (e-Government) identity management system defines a framework of organizational and technical standards and procedures for creating, storing, validating and using electronic attributes associated with the identity of a physical person. Effective use of an identity management system can help reduce costs and improve quality of delivered services, stimulating the emergence of new integrated services and fostering a service-oriented IT economy. Moreover, preventing illegitimate use of identification and authentication credentials helps States in defending national security, combating illegal immigration, terrorism and other criminal activities.

There exists several technical solutions for identity management employing very different technologies and standards. Many of these solutions are effective in a homogeneous environment, but when interoperability among different identity management solutions is involved, even the most basic functionalities are not compatible.

However, in the real world economy, the key to success is in interoperability among different systems, not in a centralized approach, as exemplified by the failure of Microsoft's Passport initiative. Additionally, national sovereignty and organizational issues prevent the creation of a single authority for securing the authentication process in its entirety, preserving full autonomy and responsibility of national organizations for citizen authentication. Any centralized solution for addressing secure interoperability issues, although technically feasible and usable in strictly hierarchical environments (e.g. multinational companies), is doomed to fail as it does not satisfy this highly critical organizational constraint.

In order to overcome this limitation, significant standardization efforts for creating commonly agreed upon specifications of interoperable federated e-ID management systems have been made by the Liberty Alliance [10], a consortium of industrial partners including AOL, HP, IBM, Intel, Oracle, RSA and Sun.

However, we believe that these issues can only be overcome by tackling the difficult problem of bottom-up design of an interoperability framework which is based on existing national infrastructures and not by imposing yet another identity management architecture. Indeed, switching to a common

standard for e-ID interoperability would require radical changes in existing IT systems and infrastructures which are not acceptable in the short or medium term for several reasons. These include economic arguments (adopting a new technology always requires making large investments on new systems and losing investments on abandoned ones), technical arguments (unexpected difficulties can introduce delays and discontinuity of service provision) and organizational arguments (switching to a third party standard also means losing the possibility of choosing which technologies to use and customizing them according to organizational needs).

European member States have made considerable investments into their national infrastructures and a wide variety of electronic identity management systems have been developed in an independent and uncoordinated way. These systems, which have not been designed for interoperability, use different technologies for hardware tokens (smart-cards, magnetic cards, mobile phones, etc.), biometrics (fingerprint, facial, retinal) and digital signatures. Consequently, member States do not necessarily trust each other's certification service (or other security services) providers. While some bilateral agreements exist between member States, in some scenarios, some of them prohibit – many times, de facto – the usage of authentication, authorization or signature certificates coming from other member States. A further obstacle originates from the fact that different organizational schemes are in use in different States: for example, the responsibility for issuing national e-IDs and validating foreign e-IDs is assigned to a single organization (centralized management of validation) in some member States, and is distributed among different autonomous organizations, even from different public administrations (distributed management of validation) in other States. Moreover, differences in legislation on identification (e.g. use of unique identifiers), data protection and digital signatures, which often reflect socio-cultural differences, hinders deployment of interoperable e-ID management systems.

Therefore a key goal is to research, define and implement an identity management framework that is based on secure and interoperable verification and authentication of identities, thus making the underlying identity technology – be it based on smart-cards or other security devices or biometric attributes – transparent and invisible to the application.

We need to understand which new components are needed, where to allocate them, and how to split tasks between legacy and new components. No ready-made recipe exists for solving such hard interoperability problems of these highly heterogeneous and complex legacy systems.

We propose an interoperability architecture based on a federation of national *citizen e-Authentication infrastructures* (CEIs) following a cooperative approach for trustworthy e-ID verification, which can coexist with any organizational and technical solution used by legacy national CEIs.

The rules governing the federation establish roles and responsibilities of involved member States in managing authentication credentials and conditions for their delegation and relaying.

In our approach, security functions are based on a permanent infrastructure layer, since this is the only viable approach for guaranteeing efficiency of e-Service provision and effectiveness of security in open and intrinsically insecure environments like the Internet. Applications should not take care of the management of security functions, which are provided by an independent layer put on top of the layer providing communication services. Applications consider security functions as infrastructural services, analogous to what happens with communication services: details regarding communication protocols used for message delivery are completely transparent at the application level.

Our proposal to address techno-organizational problems in secure interoperability among CEIs is based on defining a permanent infrastructure layer, called *bridging backbone*, providing security services to interactions between national CEIs. Each CEI will continue to operate in the normal way under the national scenario, while it will cooperate with other CEIs under the inter-national scenarios, each working within its responsibility boundaries.

The framework's architecture has provisions for generating proof of evidence for transactions and for clear separation of responsibilities. The cooperative approach is also followed by similar e-Government projects which are currently being deployed in the United States [13], [8], [7].

2. STATUS OF NATIONAL ELECTRONIC IDENTITY IN EUROPE

In this section we report on some of the most prominent architectures, technologies and projects related to electronic identity management which have been developed in Europe. The information we provide is extracted from several sources including the CEN/ISSS WS e-Authentication [1], the European Union IDABC website [11], and presentations given by governmental representatives at meetings of the Porvoo group [9].

2.1 Austria

In 2004, the Austrian Government started issuing electronic cards within the ‘Bürgerkarte’ project which defines a set of functions and minimum requirements for secure identification and use of digital signatures in e-Government. The reference framework, which is based on open standards and interfaces, supports different ID tokens (e.g. smart-cards and SIM

cards). Citizen cards are issued by several private and public sector organizations (including mobile phone operators, banks, civil service, social insurance) and support online access to about one hundred e-Services (which will become 80% of total e-Services by the end of 2007). Cardholder verification mechanisms vary depending on the card issuer (global PIN, application-specific PINs, one time passwords) and usage of biometrics is not envisioned. Authentication and digital signature functions are performed by using two different on-card certificates, and rely on a PKI with three certification authorities: a public one which is managed by the Main Association of the Social Security Institutions, and two private authorities managed by A-Trust (banking) and A1 (cellular phones). Cards and certificates have a validity period which differs from issuer to issuer, with a maximum of five years for qualified certificates. The card is not mandatory and is not a valid official ID document.

E-Government applications using the citizen card for authentication include tax services, request of residence certificates and registered e-mail. However, many more are likely to be developed due to the distribution of MOA (Modules for Online Applications), a set of server-side modules made available by the government for developing applications using the citizen card for authentication and digital signatures.

As of May 1st, 2006, over 10 million e-IDs had been issued, with an expected number of 15 millions e-IDs by the end of 2007. The number of active public sector certificates is 3,200, but they are expected to reach 50,000 by the end of 2006.

The forthcoming e-Health insurance card system 'e-card', which should replace paper-based healthcare vouchers (40 million/year), will contain personal and social insurance data and will be ready to include digital signature functionalities. The e-card will be based on the infrastructure provided by the Health Information Network (Gesundheits Informations Netzwerks - GIN) which will connect 14,000 Austrian doctors, social security offices and healthcare service providers.

2.2 Belgium

The official launch of the Belgian personal electronic identity card project (BelPIC) took place in March 2003, involving 11 Belgian pilot municipalities in cooperation with the National Register and the certification authority Belgacom.

The basic functionalities of the system are identification, authentication and digital signature. The Belgian e-ID card is a smart-card with a chip storing cardholder's personal data (including date of birth, parenthood, civil status, current and past addresses, and military situation, if applicable) and certificates for authentication and digital signature. The card is issued by

municipalities, is valid for 5 years, and uses a PIN-based access method. Currently only the photograph is present on the card, but inclusion of other biometric data is envisioned in the long term. The card is also a valid international travel document for the European 'Schengen' countries.

The e-ID card can be used for reliable access to e-Services, e-portal functions, online tax declaration, certified e-mail, e-library services, home banking and other applications that are under construction, including social security, university student services, and access to buildings. Currently, Belgian e-ID cardholders can digitally sign Adobe PDF documents and there are plans to integrate Belgian e-ID technology into Microsoft MSN Messenger for online identification.

In April 2006 a report on technical, legal and deployment requirements for secure and privacy-preserving applications based on the Belgian e-ID card was published by adapID (advanced applications for electronic IDentity cards in Flanders), a project of the Flemish Government (IWT-Vlaanderen) focusing on e-Government, e-Health and trusted archiving applications, and investigating technologies for future enhanced generations of the e-ID card (to be deployed from 2009). In September 2004 the Federal Government started the full national roll-out. In 2005, 1,378,474 citizens had an e-ID card and 8,200,000 citizens were expected to have one by 2009. According to the latest schedule the nationwide distribution will be completed in 2010.

2.3 Estonia

In Estonia national e-ID cards are issued by a public-private partnership under the responsibility of the Citizenship and Migration Board. The card is contact-based, contains a file with personal and card data (including name, national ID code, date and place of birth, sex, card number and validity) and integrates two certificates, and associated private keys, for identification/authentication and non-repudiation purposes. The card is PIN-protected and contains a chip for storing ICAO-compliant facial image and fingerprint biometrics. Certificate validation services are made available by means of certificate revocation lists, an LDAP repository and an OCSP service.

The card is a valid official identity document, a European travel document and supports access to public and private e-Services including tax, migration, citizenship, and e-ticketing services.

The validity of the card is ten years, while digital certificates have a validity of three years. However, there is a proposal for assigning a validity period of five years to cards and certificates. It is worth noting that the Estonian public sector must accept digitally signed documents and process them in the same way as it does with paper signed documents. The card is

mandatory for all Estonian citizens and permanent resident foreigners over 15 years of age.

The deployment started in 2002 and, as of May 1st 2006, about 933,662 cards had been issued (over a population of 1,441,780), with an 18% yearly growth rate.

The Finnish Population Register Centre and the Estonian Certification Service Provider have signed a Memorandum of Understanding stating that they "will cooperate to make legally binding digital documents a reality within and between Finland and Estonia." Ongoing relationships with Belgium authorities also exist.

2.4 Finland

The Finnish e-ID card contains the Citizen Certificate, a government-guaranteed 'electronic identity' available to every individual resident in Finland, which is issued by the Population Register Centre (PRC) operating under the responsibility of the Ministry of Interior. The Citizen Certificate, which is based on open standards and secured by a public key infrastructure, can be used for user identification, authentication and confidentiality of the exchanged data, as well as information integrity and non-repudiation of message delivery. The card itself is issued by the police, has a validity of five years, is PIN-protected and contains no biometrics. Optionally, Finnish citizens can have health insurance data included in their electronic ID card.

Several services (over 50) are available to cardholders including social security services, tax services, health insurance, municipal application for employees and payment of meals. Since 2003, it is possible to carry out legally binding transactions using digital signatures.

From 1999 to 2005 about 78,000 chip-cards had been issued with an annual growth rate of 35,000 cards and an expected number of 135,000 cards by the end of 2007. The number of services using e-ID authentication is expected to reach 200 by the end of 2007, with a mid-term goal to provide 1,000 services and to have 35% of the citizens (about 1.8 million people) using the e-ID.

Since 2005, the PRC is storing Citizen Certificates in SIM cards, in cooperation with national telecom operators. This solution allows citizens using mobile devices to access services for address change notification and checking of existing personal details in the Population Information System. A number of additional m-government services are under preparation, including services offered by the Social Insurance Institution, the tax administration, and the Ministry of Labor. Due to the diffusion of mobile phones in Finland, this is expected to become the most inclusive channel for the delivery of electronic public services.

Finland is cooperating with Estonia in a cross-certification project which is developing on two levels: the legislation level and the technical level.

2.5 France

The creation of the French e-ID card was first announced in September 2003 with country-wide deployment scheduled for 2006. However its launch has been postponed until 2008 due to concerns raised by a number of institutions and civil rights associations regarding privacy, security, and use of biometric data in the INES project (Identité Nationale Electronique Sécurisée / National Electronic and Secured Identity), which had provisions for secured information processes for issuing e-ID cards and for a central database storing biometric identifiers.

The French e-ID card will be a multi-application smart-card containing cardholder personal data which will provide citizens with electronic signature facilities and will allow secure execution of both e-Government and e-commerce services and transactions. Integration of facial and fingerprint biometrics is envisioned. The e-ID card will be compliant with current international standards, like European Regulation 2252/2004 for travel documents and IASv2 for authentication and signature tools. French citizens are expected to be able to start using e-IDs from 2008. Differently from paper-based identity cards, electronic ID cards will not be mandatory.

In 2004, the French Government started the ADELE e-Government program for modernizing the state infrastructure, for simplifying administrative procedures with the central administration and for developing systems for security identification of citizens. The following services will be made available within the ADELE framework: a call centre service, a one-stop shop service for address change, tenders submission, personalized public services portal, civil registration certificates (birth, marriage, and death certificates), and applications for funding.

The Vitale card is an e-Health insurance card which is issued to all individuals above 16 years of age who are entitled to social security reimbursements. The Vitale card contains administrative and entitlement information and can be used for electronic transmission of reimbursement claims between healthcare professionals and social security institutions. In 2005, a French IT professional managed to create and use a fake e-Health insurance card. For this reason, the Vitale card project will undergo a major security upgrade starting in 2006.

In March 2003, the “Carte de Vie Quotidienne” (daily life card) project was launched, aiming at providing electronic access, and possibly payment functionalities, to local public services through a smart-card-based identification and authentication process.

In April 2006 the French Ministry of Interior announced the imminent introduction of e-Passports. French citizens living abroad will experiment with the use of e-Identification tools in e-Voting during elections on June 18th, 2006.

2.6 Germany

In Germany there exists a plan for switching from the paper-based national ID card, which is mandatory for citizens starting from 16 years of age, to a highly secure smart-card-based ID card which will serve as a travel document and as an authentication token for accessing e-Government (e.g. tax filing, employment and salary certificates) and e-Business applications (e.g. e-Banking, e-Commerce). The card will also include, as an optional add-on, functionalities for qualified signatures which, according to the German Signature Act, are equivalent to handwritten signatures. The card will have a validity of 10 years, will be able to incorporate facial and fingerprint biometric information according to European Union and ICAO specifications and will use contact-less RFID technology. Roll-out is scheduled for 2007.

Following the Council Regulation of the European Union on standards for security features and biometrics in passports and travel documents issued by member States (Council Regulation (EC) No 2252/2004), the German e-Passport, will introduce biometrics in two phases: during the first phase the facial image will be included, while two fingerprints will be added during the second phase (starting in March 2007).

The Digital Health Card contains administrative data, vital patient data, and electronic prescriptions and can optionally be used for qualified signatures. However, the electronic health card and the digital identity card will not be merged and use of the Digital Health Card will not be made mandatory for procedures not related to public health.

The Job card project, which is envisioned to start in 2007, will issue a card for online access to employment services and social benefits systems to economically active citizens.

The Federal Cabinet decision of 9 March 2005 on the e-card strategy for harmonization and consistent usage of smart-cards states that:

- digital signature interoperability should be ensured through adoption of accepted standards, authentication and encryption technologies,
- all German cards must permit inclusion of the qualified digital signature at time of issuance or at a later time, and
- all administrative procedures requiring a qualified signature must support the standards agreed on by the Signature Alliance, a public-private partnership to promote the use of digital signatures.

2.7 Hungary

The Hungarian Government has adopted a national strategy for smart-card usage. This strategy includes the definition of an interoperability framework for smart-card requirements, standards and interfaces and their applications to healthcare and e-ID cards.

The 2005 'act on the general rules of public administration and services' ensures that electronic procedures have the same legal value as paper-based ones. In addition, the Hungarian public administration will be obliged to make information and services available online.

2.8 Italy

The Italian national ID card project CIE (Carta d'Identità Elettronica / electronic identity card) was launched in 2001 and is aiming to replace the 40 million existing paper-based identity cards.

The first experimental phase ended in June 2003 with about 100,000 cards issued in 83 municipalities. The second experimental phase ended in 2004 with 2 million cards in production and 600,000 cards dispatched to 56 municipalities. Municipal authorities have been distributing 400,000 cards (December 2004) to citizens older than 15. From January 1st, 2007 all municipalities will issue e-ID cards to their citizens. The aim is to issue eight million cards a year for the next 5 years. Cards are manufactured and initialized by the Italian mint (Istituto Poligrafico e Zecca dello Stato), but cardholder's personal information is added by municipalities. The deployment of the infrastructure required to access registry and demographic services and validate data on the card data was completed in Q2 2004, reaching all of the 8,102 Italian municipalities, with 23 million data controls and alignments performed.

The card is a contact smart-card of 32 KB with an optical stripe on the same side of the card with a capacity of 1.8 MB. The card contains holder's personal data, including fiscal code, blood group and a fingerprint template which is embedded in the chip and in the optical stripe. The card carries one digital certificate which can be used for access to e-Services. The certificate itself contains no personal data, which, however, service providers can acquire from the Ministry of the Interior (CNSD-INA) via an online process. Fingerprint and certificate information are only stored in the chip, with no central or local database in accordance with Italian data protection legislation. Currently, the card is PIN-protected and does not support the digital signature for non-repudiation.

The card is a valid national identity document, an official travel document recognized by 32 European and North African countries, and allows an easy and efficient access to public services. Some operational

services at the local or national level using the CIE for authentication are: payment of waste collection tax (TARSU), children's school enrolment and school fees payment, city residence and street residence change, payment of fines, age check at cigarette machines, identification check at the polls, check of a citizen's fiscal position, and access to SIM (Mountain Information System). Furthermore, several services are under preparation, including: civil and criminal complaint filing and status control, payment of social charges for house servants, income tax return payment, enrolment to local sport centers, booking of hospital admissions, medical visits, medical tests, welfare requests filing (social support checks, scholarships, …), house local tax (ICI) variations and payment, economical support to disadvantaged people (elders, orphans, …).

In Italy there exists another project, named CNS (Carta Nazionale dei Servizi / National Services Card), which aims at becoming an access mechanism for all existing and future Italian e-Government services. The card is equipped with a microprocessor containing holder's personal data, including a personal ID number. As a result of an agreement with the Italian Bankers Association, the card is also being tested for online payments using an existing financial service called Bankpass Web.

The CNS card is not an official identity document and is meant to complement rather than duplicate the national electronic ID card CIE. Indeed, by decree of the Italian Council of Ministers in February 2004 it was laid down that all Italian citizens will be able to access all of the country's e-Government services using a single smart-card. The Decree of the President of the Republic n.117 of 2nd March 2004, containing "Regulations on the diffusion of the National Service Card," states in Art.2, Paragraph 3: At the time of issuing or renovating the national service card, the administration, by means of the telematic services made available through the National Index of Personal Data Registries (INA – Indice Nazionale delle Anagrafi) checks the validity of personal data and verifies the person is not already a holder of the electronic identity card (CIE). If the personal data are valid and if the applicant is not holding an electronic identity card the administration issues the national service card.

So it may be expected that in due time the CNS and CIE cards will merge and only the CIE will remain. Nevertheless, the Italian Government set a target to distribute 10 million CNS cards by Q1 2006. More generally, the new government coming out from the general elections of April 2006 might revise the entire Italian strategy in this area.

2.9 Poland

Poland has plans to introduce an electronic ID and is closely monitoring the solutions and progress in neighboring Hungary. By 2005 the Polish

Government plans to replace all old ID booklets with machine readable cards. Smart-cards might be introduced in the future. The Polish Computerization Act is an instrument for the modernization of the public administration which gives citizens and businesses the right to contact public authorities electronically and establishes the Plan for Information Society Development. Additionally, a framework for public sector IT systems was introduced mandating interoperability with other systems, technological neutrality and fulfillment of a set of minimum requirements.

2.10 Slovenia

The Slovenian e-ID project started in 2002, after the definition of the legislative framework and the establishment of the governmental certification authorities, which issue qualified digital certificates to governmental employees (SIGOV-CA, Slovenian Governmental Certification Authority) and to natural and legal persons (SIGEN-CA, Slovenian General Certification Authority).

The identity card contains a chip with holder's personal data and two digital certificates, one for holder authentication and one for digital signature. The card, which is not mandatory, is ready to contain biometric data, in compliance with the EU e-Passport regulation. Adoption of contact-less technology has also been considered.

The Slovenian national e-ID project is divided into three phases. The first phase, which is in progress, is a pilot project. The second phase will follow and will include the tender and the production of a national e-ID. In parallel to the two phases, a third phase, which is already in progress, is focusing on interoperability and e-Services with Slovenian banks and e-ID projects running in EU member States.

E-services considered in the third phase include services which are already available, such as tax return, access to data in state registers (Register of Civil Status, Permanent Population Register, and Vehicle Register), e-forms and e-invoices. In April 2006, the Slovenian Government adopted a Strategy for Electronic Commerce in Public Administration for 2006-2010 which provides for the launching of several additional governmental e-Services including one stop shop for business startup (2006), social transfers, land register and cadastre, e-archiving (2007-2008), with the goal of achieving interoperability with European member States by 2010.

Following recent EU regulations and US demands, Slovenia is introducing new biometric e-Passports which integrate a contact-less chip. Moreover, the health insurance card system, operational since 2000, issues cards both to patients (2 million) and to healthcare professionals (18,000) for identification and data storage. There is a plan to gradually upgrade this

system, so as to allow cardholders to use their card for online access to healthcare services.

2.11 Spain

In February 2004 the Spanish Council of Ministers approved the creation and distribution to Spanish citizens of electronic ID cards (DNI Electrónico) which provide secure identification and authentication and digital signature functions for a wide range of online transactions, ranging from e-Government services to e-Commerce and Internet banking.

In order to authenticate themselves or to sign electronically online, cardholders only need their PIN code, a card reader and specific software that will be downloadable from the Internet. The new electronic ID card is meant to become a universal digital signature instrument, valid for all types of transactions.

The electronic ID cards are smart-cards containing the following information stored in the chip: an electronic certificate for authentication purposes, a PIN-protected certified digital signature for signing electronic documents, facial image and fingerprint biometric data, cardholder photograph and handwritten signature in digitized form, in addition to data printed on the card (date of birth, place of residence, etc.).

Cards are manufactured by the Spanish Royal mint (FNMT) and contain several physical security features, enhanced by cryptographic methods and bi-dimensional bar codes. The e-ID cards and electronic certificates therein contained will be issued by the National Spanish Police Department of the Ministry of Interior. The validity of e-ID cards is either five or ten years, depending on the age of the cardholder, while certificates are valid for 30 months.

Services supporting user authentication based on e-ID cards include tax declaration and social security services. As already mentioned, the electronic ID card can also be used for digital signatures which, from a legal perspective, are equivalent to handwritten signatures.

The electronic ID card was officially launched in March 2006 with a high-profile media campaign. There are currently 29 million paper-based ID cardholders in Spain (the card is mandatory starting at 14 years of age), with approximately 6 million cards being renewed each year. It is envisioned to issue 5 million e-ID cards and 10 million certificates by the end of 2007.

According to the government, the Spanish e-ID card will be interoperable and technically compatible with the electronic cards being developed in Germany, France, Italy and the United Kingdom.

2.12 United Kingdom

On March 30th, 2006 the UK Parliament approved the Identity Cards Act after two years of Parliament debates and several readings. This is a major step in the ongoing political debate in the UK on the issue of national ID cards, but there was a strong opposition against introducing such a token on a compulsory basis.

Under this scheme, a National Identity Register will be established containing biometric data (fingerprints, face, irises), which can be accessed by public and private sector organizations to verify a person's identity, with her consent. From 2008 every citizen wanting to apply for or renew a passport will be issued an ID card and her personal data and biometric information will be stored on the National Identity Register database. Until 2010 UK citizens can choose not to be issued a card, but registration will become compulsory for all UK residents by 2013. It will not be compulsory to carry the e-ID card.

According to the government, the scheme will provide citizens with a simple and secure standard for proving their identity in everyday transactions with public and private services and help ensure UK national security. The card will hold basic personal data such as name, age, validity date, entitlement to work, and a unique identification number will appear on the face of the card. The card will feature a secure encrypted chip that will contain a unique personal biometric identifier and will have a 10-year validity period.

The responsibility for managing the National Identity Register and for issuing e-Passports and e-ID cards has been assigned to the Identity and Passport Service, an Executive Agency of the UK Home Office.

A pilot for e-Passports was launched in 2004 for testing recording, recognition and usage of facial, iris and fingerprint biometrics. The roll-out for the introduction of e-Passports should be completed in 2006/07.

3. A COOPERATIVE FEDERATED ARCHITECTURE FOR IDENTITY MANAGEMENT

The model adopted in our approach [15], which is inspired by the CEN's e-Authentication CWA [1], addresses interoperability problems at different architectural layers: the citizen device layer, the infrastructure layer and the application layer.

The physical environment where the device is operating while accessing the infrastructure constitutes the *citizen device layer*. The device can either

be a smart-card (as it is common in many member States) or any other device supporting strong authentication (like mobile phones with cryptographic capabilities). Accessing devices must be linkable to personal identity, if needed, but should also be detachable from it in cases where only role identification is performed or where a certain degree of anonymity has to be guaranteed.

The *infrastructure layer* encompasses communication networks and systems which can be found on the path from the physical interface with the citizen device to remote servers, including (i) a *user access point*, that is the local part of the infrastructure used by the citizen device for accessing the system, (ii) an *e-Service access point*, that is the remote part of the infrastructure interfacing with service providers, and (iii) *identity validation services*, supporting e-Authentication procedures.

The *application layer* is composed of the applications which deliver services to authenticated users.

In a federated architecture, organizations cooperating in order to achieve a common goal rely on information provided by other members of the federation. For this reason, it is of fundamental importance that members of the federation agree on the quality of protection they provide when issuing and managing e-IDs and rigorously define reciprocal responsibilities.

Indeed, components at any architectural layer (devices/systems/services) must have a correct understanding of mutual levels of trust during the interaction with other components. For example, an authentication mechanism based on username and password issued during a completely online process cannot share the same level of trust of as an authentication method based on counterfeit-resistant credentials issued after careful physical identification. The definition of various degrees of trust existing in each CEI and a clear mapping between trust levels in various CEIs is therefore needed.

Problems of high technical complexity derive from the need to manage the whole process in an efficient and effective manner while ensuring, at the same time, interoperability of geographically distributed IT-based systems, independently of technical solutions used by participating organizations, and fulfillment of privacy and security constraints in a democratic manner.

Security and performance are, indeed, the most critical functional capabilities of the interoperability architecture.

The first essential functionality is end-to-end security. This refers to the capability of ensuring traditional security requirements (from basic ones: confidentiality, integrity, authentication, authorization, to derived ones: auditing, non-repudiation, etc.) from the citizen accessing devices all the way down to the point providing the required service.

The second critical functionality is performance experienced by end-users. Due to the cooperative approach that has to be followed in designing

the overall interoperability architecture and to the size of federated systems of national CEIs that will result, each service invocation may require establishing and traversing several times geographically long and organizationally complex communication paths. For improved performance, only cross-border interactions, which are important for security and privacy purposes or for documenting interaction between CEIs, will be required to be secured. Moreover, a carefully designed architecture must be able to cache information at usage points and keep it fresh to avoid the well-known attacks based on exploiting stale security information. From a user perspective this is similar to single sign-on, which avoids the need to repeat the process of identification and authentication for a series of transactions.

3.1 Further Interoperability Issues

Interoperability between national electronic identity management systems must be provided at three different levels of functionalities, which are listed below in increasing order of complexity:

- identification and authentication: that is the process of associating a set of attributes or a personal identifier with a citizen (identification) and proving that such association is trustworthy (authentication);
- authorization: that is the process of deciding whether a user is allowed to perform a particular action;
- electronic signature: that is the process of establishing authenticity of data and identity of the signer mainly for the purpose of producing verifiable records of transactions.

Noteworthy semantic problems will have to be solved for enabling interoperability among privilege management systems which handle authorizations and access rights of citizens depending not only on their identity, but also on their role within an organization (e.g. doctor, policeman, CEO). Although this is an important research area to be investigated, role-based privilege management systems [2, 14] must be built on top of effective and reliable authentication systems, and must be kept separate from them.

Interoperability of electronic signatures is another important issue to be solved, which is orthogonal to interoperability of CEIs. In the EU, this is a difficult and very controversial point because some member States have developed very different interpretations of the EU directive containing recommendations for management of electronic signatures. Consequently, using electronic signatures as a basis for performing e-Authentication will lead to potentially never-ending legal and juridical disputes. Additional critical issues are interoperability of security policies, user profiles and certificate validation services.

An additional requirement of an interoperability architecture is support for the specification of privacy preferences, giving the citizen full control over collection, storage and use of personal information, along with support for anonymity schemes and a mechanism for protection against user profiling. An effective system should inform the user every time her electronic identity is used in a transaction and should allow almost immediate revocation by the holder.

3.2 Architectural Interfaces for Interoperability

From an architectural viewpoint it is also important to identify interfaces lying between different components. Indeed, in the case of interoperability of national CEIs, some of them are managed by different national systems, raising the need for establishing a secure and reliable dialog among them. A first interface is between the citizen device used for requesting access to the system and the physical device interacting with it at the user access point. A second interface is between the user access point and the service access point that is between the local terminal application and the access point to the requested service. A third interface, which is highly critical for services requiring user authentication, is between the validation service used to verify the authenticity of user credentials and a user or service access point. The fourth interface is between a service access point and an e-Service.

3.3 Interoperability Scenarios

Depending on whether the citizen device layer, the infrastructure layer and the application layer, are *on-us* (meaning national/domestic) or *not-on-us* (meaning foreign/alien), different scenarios derive, bringing technical and organizational interoperability problems of different dimensions and nature.

If we fix a value for one layer, then all possible interoperability scenarios are clearly identified. For example, the Italian access network (which means that the citizen device is physically in Italy) has to provide access in the five interoperability scenarios listed below:

1. Italian devices accessing Italian services,
2. Italian devices accessing foreign services,
3. foreign devices accessing Italian services, and
4. foreign devices accessing foreign services. This has two sub-cases:
   a. foreign devices accessing their national services, and
   b. foreign devices accessing services provided by a third foreign country.

As a further example of how this approach to modeling interoperability scenarios works, Table 17-1 shows the possible kinds of interoperability

scenarios obtained by choosing the citizen device belonging to the Italian domain.

Table 17-1. Interoperability scenarios

	Italian application	Foreign application	
Italian infrastructure	Italian CEIs	partial operability	
Foreign infrastructure	partial interoperability	same CEIs	partial interoperability
		different CEIs	full interoperability

A synthetic characterization of the different kinds of interoperability scenarios follows:

1. national CEIs: components in all three layers belong to the same domain,
2. partial CEIs interoperability: components in two layers belong to the same domain,
3. full CEIs interoperability: components in each layer belong to different domains.

An example scenario at the widest possible interoperability level is the following: an Estonian citizen wishes to make access to an Italian service while visiting Belgium. In this case, the first interface is physically in Belgium, the second interface spans the three countries, the third interface is physically in Estonia, and the fourth is in Italy.

3.4 The Bridging Backbone Approach

Provision of cross-border services to mobile citizens requires interoperability of national e-ID management systems at different layers. Initially, citizen credentials must be obtained from the citizen device and understood by the access network. Then, the citizen's request is first relayed to the competent CEI for authentication and subsequently to the CEIs which are competent for providing the requested services.

Efficient provision of end-to-end security requires a highly secure and efficient exchange layer among national CEIs, which facilitates quick exchange of all required information to properly authenticate accessing citizens. This exchange layer must be overlaid to and logically distinct from existing CEIs.

We propose an infrastructural solution to security and interoperability issues in provision of cross-border e-Services to mobile citizens: the *bridging backbone*. The bridging backbone provides security services (like confidentiality and integrity services, authentication, authorization and auditing) in an easy and transparent manner, independently from locally deployed network technology and topology. Security services are provided

at a layer lying between the application and communication layers, which is in charge of monitoring network connections and securing them according to the cooperation policies of the federation of involved infrastructures (see [5], [4], [6], [3] for details).

A mandatory requirement of the cooperation-based approach is the ability to document transactions that were carried out during interaction between national CEIs. Given the legal value attached to data being managed and exchanged in this process and the fact that many various kinds of mistakes can take place during the interaction, it is necessary to clearly and unequivocally understand who did what. The absence of a super-national organization that can supervise and direct the activity of national CEIs makes these certification functions a mandatory requirement. Moreover, as certification functions in a federation of national infrastructures play a back-office and subordinate role, they are fully acceptable by involved organizations, both from political and organizational viewpoints.

It is important to stress that in the real world of non-electronic services and whenever some kind of contractual responsibility is involved, security functions are always based, to various degrees, on some form of permanent infrastructure. For example, public utilities like power supply, water, and sewage are provided by municipalities to houses on the basis of the house ownership or rental. People interact with banks in buildings and offices clearly and permanently identifiable as bank settings (even ATMs are usually placed in trustable environments). Also e-Banking, the currently most widespread e-Service among the ones where trust is a fundamental aspect, is based on an initial setup phase where a security infrastructure is established: the customer goes physically to branch offices for signing the contract and receives codes and instructions for accessing the service on the Internet.

A further important point regarding security in interaction between institutions (as compared to interaction among people) is that organizations typically do not allow any inside member to unilaterally establish trust with external entities. The reality of institutional cooperation shows that inter-institutional trust is always based on bilateral agreement at the organizational level. The electronic counterpart of this convention is that there must be an infrastructure layer providing security functions, and security functions are provided with reference to and after an agreement is formally in place between the involved organizations.

4. CONCLUSIONS AND DISCUSSION

Our proposal considers an interoperability architecture based on a federation of national infrastructures and follows a cooperation-based

approach which is fully compatible with and respectful of organizational and technical choices of existing systems.

In our view security is not an add-on service but is an infrastructural service of inter-organizational communication. By providing applications with security services in a completely transparent, infrastructural way, issues related to security services and business logic are kept separate, thereby reducing the risks of introducing security flaws. This is in contrast with the standard approach, where security services are usually provided at different levels of the protocol stack.

The technological neutrality and the compatibility with legacy systems of our approach do not violate techno-organizational choices of involved organizations. Moreover, since interoperability is not based on country-to-country system interfaces deriving from bilateral agreements, this approach allows the designing and building of a scalable and efficient system. The bilateral agreements approach would be, in fact, viable and effective only when there are very few actors: as soon as the stakeholders are more than three or four its complexity becomes unmanageable.

We solve the organizational pitfall of a naive use of PKIs, where trust can be established unilaterally, by allowing cooperation between members of different organizations only on top of the bridging backbone layer, which is set up only after a bilateral agreement is formally in place at the organizational level.

Additionally, the bridging backbone enables the certification of successful e-Services interaction and composition, identification of culprits of unsuccessful service provision, and monitoring of the actual performance of service provision [5].

REFERENCES

1. CEN/ISSS Workshop on e-Authentication, 2005. http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/wseaut.asp
2. Gail-Joon Ahn. Specification and Classification of Role-based Authorization Policies. In Twelfth International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises June 09 - 11, 2003 Linz, Austria, 2003.
3. Franco Arcieri, Elettra Cappadozzi, Enrico Nardelli, and Maurizio Talamo. SIM: a Working Example of an E-government Service Infrastructure for Mountain Communities. In Workshop Electronic Government (DEXA-e-gov'01), associated to the 2001 Conference on Databases and Expert System Applications (DEXA'01), pages 407–411, Munich, Germany, September 2001. IEEE Computer Society Press.
4. Franco Arcieri, Mario Ciclosi, Fabio Fioravanti, Enrico Nardelli, and Maurizio Talamo. The Italian Electronic Identity Card: a short introduction. In The National Conference on Digital Government Research (dg.o2004), May 24-26, 2004, Seattle, Washington, USA.
5. Franco Arcieri, Fabio Fioravanti, Enrico Nardelli, and Maurizio Talamo. Inter-organizational E-Services Accounting Management. In 3rd IFIP conference on e-

Commerce, e-Business, and e-Government (I3E-03) Sao Paolo, Brasil. Kluwer Academic Publishers, September 2003.
6. Franco Arcieri, Fabio Fioravanti, Enrico Nardelli, and Maurizio Talamo. Reliable Peer-to-Peer Access for Italian Citizens to Digital Government Services on the Internet. In Roland Traunmüller, editor, Electronic Government: Third International Conference, (E-GOV'04), Zaragoza, Spain, August 30 – September 3, 2004, volume 3183 of Lecture Notes in Computer Science, pages 250–255. Springer-Verlag, 2004.
7. United States Federal PKI Operational Authority. Federal Public Key Infrastructure (FPKI) Architecture Technical Overview, 2005.
8. United States Federal PKI Policy Authority. X.509 Certificate Policy for the Federal Bridge Certification Authority, 2002.
9. The Porvoo Group website. http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/index_eng. Follow the link "Electronic Identity" and then the "Porvoo Group" one.
10. The Liberty Alliance project. http://www.projectliberty.org
11. The Interchange of Data Between Administrations (IDABC) program of the European Union. http://europa.eu.int/idabc/
12. The International Civil Aviation Organization (ICAO) website. http://www.icao.int
13. United States General Accounting Office. Planned e-Authentication Gateway Faces Formidable Development Challenges, 2003. Report to the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House of Representatives.
14. Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-Based Access Control Models. IEEE Computer, 29(2):38–47, 1996.
15. Franco Arcieri, Andrea Dimitri, Fabio Fioravanti, Enrico Nardelli, Katia Pallucca, Alberto Postiglione and Maurizio Talamo. An Infrastructural Approach to Secure Interoperability of Electronic IDs: The Bridging Backbone. In Maria Wimmer et al., editors, Electronic Government: Fourth International Conference, (E-GOV'05), Copenhagen, Denmark, August 22-26, 2005, volume 3591 of Lecture Notes in Computer Science, pages 291–299. Springer-Verlag, 2005.

SUGGESTED READINGS AND ONLINE RESOURCES

- The Porvoo Group website:
  http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/index_eng
  Follow the link, "Electronic Identity," and then "Porvoo Group." The Porvoo Group is an international cooperative network whose primary goal is to promote a trans-national, interoperable electronic identity, based on PKI technology (Public Key Infrastructure) and electronic ID cards, in order to help ensure secure public and private sector e-transactions in Europe. The Group also promotes the introduction of interoperable certificates and technical specifications, the mutual, cross-border acceptance of authentication mechanisms, as well as cross-border, online access to administrative services.

- IDABC (Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens):
  http://europa.eu.int/idabc
  IDABC is a European Union project for supporting use of ICT in the delivery of cross-border public sector services to citizens and enterprises in Europe and for improving efficiency and collaboration between European public administrations.
- CEN/ISSS Workshop Agreement on eAuthentication for smart-cards and e-Government applications:
  http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/wseaut.asp
  A CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN/ISSS).The outcome of the CEN/ISSS Workshop Agreement on eAuthentication is a set of requirements, recommendations and best practices for reliable pan-European interoperable e-ID within an e-Government issued and public-private partnership based multi-application card scheme.
- e-Government Unit of the Directorate General for Information Society of the European Commission: http://europa.eu.int/e-Government_research
  The mission of the e-Government Unit in the DG Information Society is to implement policy, good practice exchange and innovation through the eEurope action plan and the IST program.

QUESTIONS FOR DISCUSSION

1. What are the advantages and disadvantages of adopting a centralized approach to ID management with respect to a federated/cooperative approach?
2. What is the organizational, economic and legal impact of migrating to third party technologies for ID management in a trans-national scenario?
3. How does infrastructural security compare to application-level security?