

SYNERGY

The IDABC Quarterly

JULY 2005 – ISSUE

03

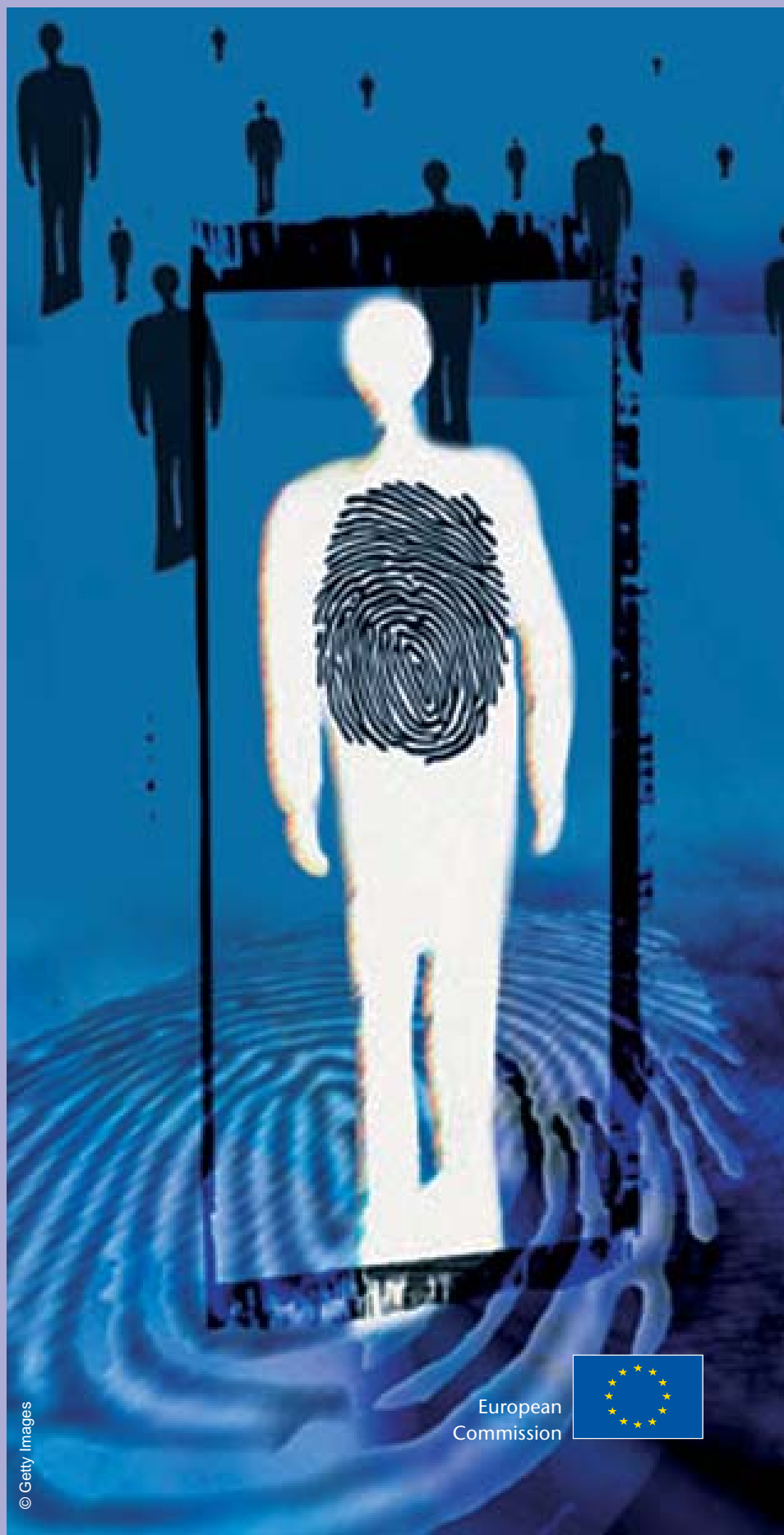
**TOWARDS
INTEROPERABLE eID:**
IDABC work programme
addresses key eID issues

**ELECTRONIC IDENTITY
IN PRACTICE:**
Case studies from
Austria and Estonia

THE EXPERT VIEW:
Interview with
information security and
cryptology specialist
Professor Bart Preneel

**A COHERENT
APPROACH TO eID:**
European level activities
in the field of eidentity

**PROMOTING
eGOVERNMENT
THROUGH FEDERATED
IDENTITY:**
The Liberty Alliance



© Getty Images





Dear Reader,

Electronic identity (eID) is a key topic within IDABC. An effective system of

electronic identities, enabling – across Europe – convenient and secure access to different applications, is fundamental for the development of cross-border eGovernment services.

This issue of SYNeRGY is therefore dedicated to electronic identity, describing actions that are part of the IDABC work programme as well as activities that are taking place elsewhere.

You will find details about IDABC's action on eID interoperability, along with information on a study on identity management in eGovernment sponsored by Modinis, a programme from the European Commission's Directorate-General for Information Society that supports the eEurope Action Plan by disseminating good practices, sponsoring analysis and strategic discussion and other measures.

The creation of effective, interoperable eID systems will need partnerships between different stakeholders, including administrations and the private sector.

This issue of SYNeRGY reviews the work done by organisations such as the Liberty Alliance and the Porvoo Group.

In the meantime, Member States are facing their own eID challenges. We therefore include two case studies – firstly, the Austrian eID scheme, which is distinguished by its potential for incorporating foreign eIDs; and secondly the Estonian scheme, which is distinguished by its widespread adoption and coverage.

We hope that this issue of SYNeRGY will be a useful reference point for the current state of play on eID in Europe and will stimulate further reflection on this topic. As always, we welcome your comments and feedback. Contact information for the IDABC Unit can be found on the IDABC website at <http://europa.eu.int/idabc>.

Future issues of SYNeRGY will examine other priority areas. Each time, we provide information and hope to provoke discussion, making SYNeRGY interesting reading for everyone working in the field.

Karel De Vriendt
IDABC Head of Unit

Publisher: European Commission, DG Enterprise and Industry, IDABC Unit

Editor in chief: Karel De Vriendt

Production: GOPA-Cartermill

ISSN: 1830-205X

Catalogue No: NB-AT-05-003-EN-C

The IDABC Unit thanks all those who contributed to this issue of SYNeRGY and welcomes comments and contributions at idabc@cec.eu.int

Further information, including subscription to this publication, is available at the following address:

<http://europa.eu.int/idabc>

SYNeRGY is published by the European Commission (Enterprise and Industry Directorate-General, IDABC Unit). The views expressed are purely those of the authors and may not in any circumstance be regarded as stating an official position of the European Commission. The unsigned articles have been prepared by a Commission external contractor. Neither the European Commission nor any person acting on its behalf is responsible for the use that may be made of the information in this publication.

© European Communities, 2005

Reproduction is authorised provided the source is acknowledged.

♻️ Printed on recycled paper

CONTENTS

TOWARDS INTEROPERABLE eIDS FOR EUROPEAN CITIZENS..... 3

Electronic identities are fundamental for secure access to and convenient use of eGovernment services in Europe. A number of actions being taken by the IDABC programme are driving the eID agenda forward.

IDENTITY MANAGEMENT ADVANCES ON MULTIPLE FRONTS..... 5

Work on eID at European level takes a number of forms, including research funded under the Framework Programmes for Research and Development, studies and surveys and good practice exchange.

eID CASE STUDY: AUSTRIA..... 6

Austria's electronic identity scheme has attracted interest from across Europe, in particular because it facilitates integration of foreign eIDs into Austrian eGovernment processes

eID IN ACTION: ESTONIA..... 8

Estonia's electronic identity card has been taken up widely across the country and is usable in multiple government and private sector applications.

FEDERATED eID 9

The Liberty Alliance is developing a federated identity standard based on open technology specifications with in-built privacy controls, and is attracting increasing interest from European administrations.

ENSURING PRIVACY 11

Electronic identity schemes must take full account of European privacy and data protection legislation.

INTERVIEW: PROFESSOR BART PRENEEL 12

Professor in the Computer Security and Industrial Cryptography research group at Belgium's Katholieke Universiteit Leuven, Bart Preneel is well placed to give an overview of the state of eID in Europe

THE PORVOO GROUP: PROMOTING eID INTEROPERABILITY..... 14

The Porvoo Group meets twice yearly to consider technical aspects of electronic identity and the current state of play. Most recently, the group met in Reykjavik, Iceland, at the end of May 2005.

Electronic identities are fundamental for secure access to and convenient use of eGovernment services in Europe. A number of Member States have introduced electronic ID (eID) schemes, whilst others are planning to do so. In order to prevent these developments from creating new digital barriers across borders, a set of minimum requirements and common standards must be agreed to enable European eID solutions to interoperate. These issues were discussed at the IDABC Launch Conference in February 2005 and are being further addressed through the new IDABC work programme.

Early activities in the eID field concentrated on **smart cards** as the medium to effectively manage identities. Smart cards are already widely used in telephony, banking, and, increasingly, in healthcare and public transport. They are **safe and tamper-resistant** and provide a secure environment for electronic transactions. They enable secure, fast and convenient access to both online and offline services, whilst generating user confidence by giving cardholders control over the personal information delivered through electronic networks.

However, electronic identities are not restricted to smart cards. eID is rather a concept that can potentially operate across different platforms with **mobile phone SIM cards** being of particular interest. Whatever media is used, eID schemes need to be able to authenticate users and to support a digital signature facility that can give consent in an eTransaction process. eID cards can incorporate advanced security features (such as biometric identifiers) for convenient proof of identity of a person. For governments, eID is therefore both a secure replacement for paper-based identity schemes and a reliable key to identify and authenticate users of e-enabled public services.

The early focus on smart cards

As work on electronic identity developed – chiefly around smart cards in the early stages – it became evident that coordination was needed to implement minimum requirements in order to avoid incompatible technologies. In December 1999 the European Commission launched the eEurope Smart Card (eESC) charter, bringing together experts from government and industry to address issues of interoperability and security with regard to the deployment of smart cards across Europe. In March 2003, eESC delivered the **OSCIE (Open Smart Card Infrastructure for Europe)**, a complete set of guidelines and technical specifications for the development of smart

card technology capabilities. Among other things, the OSCIE incorporates the Global Interoperability Framework (GIF), a common specification for smart card-based **IAS (Identification, Authentication, and electronic Signature services)** access mechanisms to eServices.

The OSCIE documents were forwarded to the European Committee for Standardisation - Information Society Standardisation System (**CEN/ISSS**) for transposition into **CEN workshop agreements (CWAs)**. CWAs are specifications



Work on eID is moving from smart cards to a wider range of solutions

reflecting a consensus among public and private sector organisations participating in a thematic workshop, which may take the form of best practice agreements, codes of conduct, technical guidelines or informative guidance. CWAs are not European standards but are sometimes considered as pre-standards, paving the ground for formal standardisation agreements between national delegations.

The CEN Workshop on eAuthentication for smart cards and eGovernment applications launched in September 2003, paved the way for establishment of an open IAS standard to support the rollout and adoption of eGovernment services. A CWA was agreed at its final meeting on 11 February 2005, comprising three parts: an architecture for a European interoperable eID system within a smart card infrastructure; a best practice manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services; and user requirements for a European interoperable smart card based eID system. Although smart cards were the main focus, it was also recognised that other non-card based solutions for carrying out qualified eServices are being developed. Work on mobile device technology is particularly important, as this medium potentially offers cost, security and functionality benefits over smart cards.

IDABC and eID

It is these eID standardisation efforts – as well as related activities such as EU-funded research projects (e.g. eEpoch, GUIDE and PRIME¹), and the independent activities of organisations such as the Porvoo Group and the Liberty Alliance (which are covered separately in this issue of SYNeRGY) – that IDABC now aims to build on, following the IDABC Launch Conference of February 2005.

The conference demonstrated that much progress has already been achieved on the technical side and in the use of open standards for eID, but that important organisational and legal issues still need to be tackled. In this respect, participants called for the IDABC programme to play an important role in helping understand and define minimum requirements and common standards for interoperable, European level eID solutions in order to enable the secure delivery of eGovernment services.

The IDABC work programme has now been developed to address these issues in three main respects:

- **eID interoperability:** this IDABC horizontal measure will bring together an expert group to analyse European eID and authentication interoperability requirements, and to propose a global eID interoperability approach based on existing technologies. This will seek to address the introduction of different eID systems in different Member States, thus helping avoid discrimination in terms of use of different eGovernment services by different Member State citizens and businesses. The deliverables will be a survey of Member State and candidate country eID schemes; a survey and description of the national technical solutions; a market survey of those technical solutions; and a proposal for an effective eID interoperability solution, including minimum interoperability requirements.
- **Certification services:** this action will continue the **PKI Services** operational horizontal action of the IDA II programme. A number of European Commission Directorates-General and EU agencies currently use the IDA PKI services for their specific applications. This action will enable continued operational delivery of user or server certificates, and will allow certification services to be updated, on the basis of a new specific standard IDABC certificate policy and dedicated certificate practise statement.
- **Mutual recognition of eSignatures for eGovernment applications:** this action will analyse the requirements in terms of interoperability of eSignatures for different eGovernment applications and services, as a first step in overcoming the lack of or incompleteness of mutual recognition of eSignatures between different Member States. The deliverables will be a reference list of eGovernment applications involving use of eSignatures; an assessment of national eSignature legal requirements by type of eGovernment application; a report on technical implementations and interfaces; a review of the legal and technical interoperability issues; and a proposal for a mutual information mechanism on the legal requirements for eSignatures.

⁽¹⁾ *Respectively, eEurope Smart Card Charter proof of concept and holistic solution; Government User IDentity for Europe and Privacy and Identity Management for Europe.*

A broad range of activities is underway at European level in the field of eidentity, complementing the actions of the IDABC programme. These other European level initiatives include technical research projects and other work aimed at addressing interoperability issues and ensuring a coherent approach to identity management.

Research projects

A number of projects supported by the IST priority in the European Commission's fifth and sixth Framework Programmes for Research and Development are continuing or are approaching conclusion.

One of these is **PRIME – Privacy and Identity Management for Europe**. PRIME is focused around research issues of digital identity management (IDM) and privacy in the information society. Its stated objectives are to develop the solutions that will enable individuals to manage their eidentities and to promote deployment of solutions that enhance privacy. The project was launched on 1 March 2004 with a four-year duration.

The project will work on a range of IDM solutions, with a view to developing a set of requirements for each covering technical, usability, legal, social and economic aspects. The consortium will also implement privacy-enhancing IDM prototypes and models, and will deliver a technical PRIME architecture and framework for privacy-enhancing IDM. A large consortium has been brought together for the project, with coordination carried out by IBM France. The project website is at <http://www.prime-project.eu.org>.

Running concurrently, the **GUIDE project** (Government User IDentity for Europe) aims specifically to set the issue of eID in the government institutional context. GUIDE will create a European conceptual framework for IDM by initiating development of an architecture for secure transactions between administrations, citizens and businesses, which will also take into account back office processes. The project also includes social, ethical and legal research aspects. Like PRIME, a substantial consortium has been built, coordinated by British Telecom. For more information, see <http://www.guide-project.org>.

A range of other research projects also address IDM, including:

- **BioSec** (Biometric Security): Europe-wide deployment of biometric technologies; see <http://www.biosec.org>
- **ECRYPT** (European Network of Excellence for Cryptology): facilitating European collaboration in cryptology and digital watermarking; see <http://www.ecrypt.eu.org>
- **eEPOCH**: demonstrating interoperable and secure smart card based digital identification systems, with a particular focus on interoperability; see <http://www.eepoch.net>
- **FIDIS** (Future of IDentity in the Information Society): exploring the relationship between identification and identity in a high-tech environment and considering the implications for the European Area of Freedom, Justice and Security; see <http://www.fidis.net>

eID in Modinis

Questions of IDM are also being explored though the European Commission Directorate-General for Information Society's Modinis programme, which is sponsoring a **study on identity management in eGovernment**. A consortium led by the Katholieke Universiteit Leuven in Belgium is conducting the study.

The objective is to work towards a coherent approach to IDM in eGovernment by assessing the policies supporting cross-border and cross-sector eGovernment services; by analysing initiatives and possible solutions at European level; by gathering information on ID technologies, market developments and technical requirements and by developing a methodology based on use of good practice in

IDM. One of the main goals of the study, which commenced on 1 January 2005, will be to outline a common terminology that can bridge the gap between the private sector and government in IDM. The project is being steered by an eGovernment Identity Management working group, and will contribute to addressing the advancement of IDM by taking into account legal and cultural differences as well as the EU data protection framework.

IDM advancement through good practice exchange

The work of the European Commission DG Information Society eGovernment Unit in bringing

together information on eGovernment research activities is also relevant in terms of IDM. A subgroup is working on eID issues, whilst the broad objective of the Unit is to promote good practice exchange as a tool of policy implementation. The **eGovernment research web portal** features a regular project of the month, as well as news, events and access to the eGovernment good practice framework, which is a tool for assessing, describing and transferring good practice.

The eGovernment research web portal can be found at:

http://www.europa.eu.int/information_society/activities/egovernment_research/index_en.htm

EID CASE STUDY: AUSTRIA

6

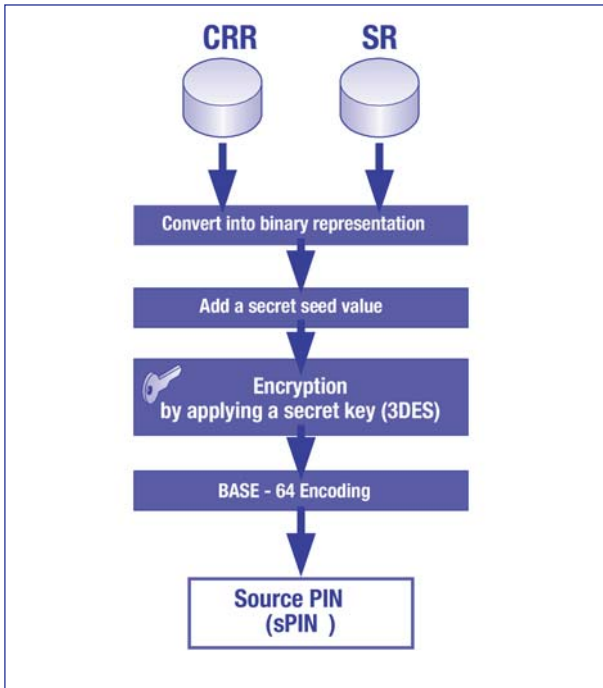
Austria's electronic identification scheme, which is based on a system of generating secure 'sector specific' digital certificates for different eGovernment applications, has attracted interest from across Europe. Under the Austrian system, it is also possible to incorporate to some extent foreign eIDs into Austrian eGovernment processes.

At the root of electronic identification in Austria is the source PIN (personal identification number). Every person in Austria is assigned a **unique source PIN**, which is generated from identification numbers held in Austria's base registers – the Central Residents' Register and, for foreigners living in Austria, the Supplementary Register. Whilst the identifiers held in the registers are publicly available, the source PIN is secret and under the sole control of the citizen. Neither governmental nor private organisations have the right to store source PINs.

The technical process for generating source PINs involves four steps: conversion of the identifier held in the Central Residents' or Supplementary Register into a binary representation; addition of a secret seed value; encryption achieved by application of a secret key; and finally BASE-64 encoding.

The source PIN can then be built into the **Austrian Citizen Card**, which is used for accessing eGovernment services and for electronic signatures. However, no identity card is required in Austria and the Citizen Card concept should rather be understood as a broader range of tools enabling administrative procedures to be carried out electronically rather than as a universal and uniform identity card. Because of the open, technologically neutral approach taken by Austria, a variety of entities can issue Citizen Cards. These include both public bodies (including Federal ministries and universities) and private bodies (certification authorities, banks) and can even involve other technologies such as mobile phone signatures.

The Citizen Card concept has been developed by the Austrian Secure Information Technology Centre



Source PIN generation

(A-SIT), an independent body acting as a partner to the Austrian government, with support from organisations such as the Austrian National Bank and the Technical University of Graz. A-SIT specialises in eSignatures and eAuthentication and has developed the Austrian source PIN based electronic identification model.

Spinning a web of ssPINs

For eGovernment application identification Austria uses **sector-specific PINs**, or ssPINs. These are derived from the source PIN held by the citizen whenever he or she uses his or her Citizen Card. Each different area of public administration has a specific alphanumeric code, known as the sector code. This is combined with the citizen's source PIN. A cryptographic one-way function (a Hash function, where the input can be of any length but the output is of a fixed length) is then applied to create the ssPIN.

This system offers a number of benefits. Firstly, there is no linking of identity across different eGovernment services, thus **protecting privacy**. Secondly, the system offers a high degree of security as each ssPIN is different and it is not possible to work back from the ssPIN and calculate the source PIN. Nor is it possible to calculate any other ssPIN from a given ssPIN.

In eGovernment applications therefore, the citizen is identified by the ssPIN, which will depend on the particular application being used. Authentication is

via electronic signature, which is also incorporated into the Citizen Card.

The Austrian system offers a further major benefit: it is possible to create what are known as **substitutional source PINs** from foreign eIDs, which can therefore be integrated into Austrian eGovernment services. By Austrian legislation, this can be done for certain eGovernment applications requiring a recurring identity – where a citizen registers for an application and that application continues to recognise the citizen based on a repetitive identifier.

A-SIT has developed a prototype web service that allows holders of Italian and Finnish eID cards to request a substitutional source PIN. These are created by applying keyed Hash functions to identifiers derived from Italian and Finnish eIDs. The result is then BASE-64 encoded to generate the substitutional source PIN. This can be used in certain Austrian eGovernment applications in a similar way to the source PIN held by Austrian citizens or residents. A-SIT is presently working on integration of Belgian eIDs into the same system.

The Austrian Government is now cooperating with other Member States and the services of the European Commission in preparing the ground for future work in this domain at pan-European level. The new **i2010 Programme** launched by Information Society Commissioner Viviane Reding at the beginning of June 2005 includes a proposed **Action Plan for eGovernment** that will include specific actions to enable eGovernment services across national boundaries using a common framework of mutually recognised national eIDs.

During the Austrian Presidency of the EU, starting in January 2006, there will be a major high-level eGovernment conference at which the issue of interoperability of European eGovernment services and the role of electronic identity in building trust in the growing 'European Information Space' will take centre stage.

Further information:

Thomas Rössler of A-SIT participated in the IDABC Launch Conference in Brussels in February 2005, and his presentation on the Austrian eID scheme can be found at: <http://europa.eu.int/idabc/servlets/Doc?id=19404> (PDF file). The A-SIT website is at: <http://www.a-sit.at/> (in German)

In terms of coverage of the population, Europe's most developed electronic ID card scheme is found in Estonia. By the end of May 2005 around 765,000 cards had been issued. In addition, 158,000 eID cards had been issued to foreigners. Estonia is one of Europe's smaller countries with 1.37 million inhabitants and it is in this context that achieving widespread coverage has been possible. Estonia is also distinguished by good ICT infrastructure and the Internet is accessible from 99 percent of the territory.

The Estonian Parliament took the decision to introduce an eID card in 2000, and the first cards were issued in January 2002. 130,000 were issued in the first year. **The Identity Documents Act** regulates the scheme and cards are mandatory.

The cards are issued in standard form and there are no optional features that holders can choose to have or not have. However, if citizens wish to suspend the electronic functions of their cards, they have the right to suspend the validity of their certificates. This also removes the holder's data from the public certificate directory – unique personal ID numbers are public information in Estonia.

8

The front of the card contains:

- Holder's signature and photo
- Holder's name
- Personal code (national ID code)
- Date of birth
- Gender
- Citizenship status
- Card number
- Card validity expiry date

The reverse of the card contains:

- Holder's place of birth
- Card issuing date
- Residence permit details (if applicable)
- Card and holder data in machine readable format (except for the photo and signature)

This information is not duplicated on the card chip, which contains two certificates and their associated private keys protected by PIN codes. The certificates contain only the holder's name and personal (national ID) code. The certificates are designed for authentication and for signing documents.

An interesting feature of the Estonian eID is that the authentication certificate also contains a **unique email address** allocated to the holder. This takes the format [firstname.lastname.NNNN@eesti.ee](#), where NNNN represents four random numbers. This address is intended as a lifetime address. It is not associated with a real email service but is rather a relay address forwarding mails to the holder's 'real' address. The holder can update his or her 'real' address details whenever necessary.

The email address is intended for government communications but can also be used privately or for dealings with companies. The addresses are publicly available through Estonia's National Registry of Certification Service Providers' certificate directory.

At the heart of the system is AS Sertifitseerimiskeskus (SK – 'certificate centre'), which maintains the electronic infrastructure necessary for issuing and using the card. Two major Estonian banks, Hansapank and Eesti Ühispank, in partnership with telecom companies Eesti Telefon and EMT, established SK, and it is at branches of the two banks that citizens can collect their cards. However, when requesting a card, the citizen applies to the Estonian Citizenship and Migration Board, which administers the scheme.

The Estonian electronic signature strategy does not limit the use of digital authentication. It can be used in any sector without restrictions. It can also be used for accessing healthcare and thus no separate health card is required in Estonia – only the ID card is needed when visiting a medical institution.

The basic software components used for authentication are publicly available to all developers.

FIM systems were initially developed in the private sector by companies such as American Express, Boeing, General Motors and Nokia. One example of a straightforward FIM system is banking ATM networks: banks use simple authentication at the point of transaction (bank cards and PIN codes) to allow customers to withdraw funds from their accounts even though they may not be using an ATM belonging to their home bank and may even be in another country. The banks that have agreed to trust one another make the necessary transfers of funds 'behind the scenes' once a customer has withdrawn money.

Moving FIM forward with the Liberty Alliance

Momentum behind more widespread adoption of FIM is now building up thanks to the Liberty Alliance, an international organisation with a membership of more than 150 companies, non-profit and government bodies. The Liberty Alliance project is dedicated to building a **federated identity standard** based on open technology specifications with in-built privacy controls. The standards are compliant with international regulations, including EU data protection legislation (see box), and Liberty Alliance issues Liberty Interoperable Certifications that validate implementations and are designed to drive take-up of the standards. The Liberty Alliance approach contrasts with more centralised, proprietary systems as pioneered by organisations such as Microsoft with its .Net Passport system. In late 2004, the Liberty Alliance added a number of new members, including IBM and Adobe, providing a major boost to its approach.

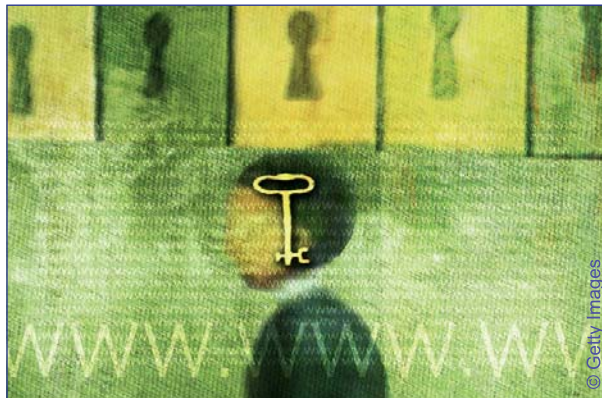
Liberty Alliance specifications describe the federated architecture and provide policy and security guidance, define transport bindings and usage profiles for abstract protocols, give detailed implementation guidelines and checklists, and list mandatory and optional features. For exchanging authentication

information within the circle of trust, Liberty Alliance has developed specifications based on **Security Assertion Markup Language (SAML)**. The Liberty Alliance is now readying itself to include SAML 2.0 in its interoperability testing programme. Development of SAML 2.0 has been overseen by OASIS, the Organisation for the Advancement of Structured Information Standards.

FIM – the potential for eGovernment

The potential benefits of FIM in terms of eGovernment services to citizens and businesses are underlined by the fact that several government organisations have become Liberty Alliance members. One sponsor member is the French government agency for the development of electronic administration (ADAE – Agence pour le Développement de l'Administration Électronique), which is set to develop its identity management architecture in accordance with Liberty Alliance specifications.

In order to develop the French administration's personalised portal, aimed at citizens and businesses, ADAE was tasked with finding a solution that would simplify access without concentrating identifiers in a central database. FIM was identified as a potential answer to this requirement, and ADAE joined the Liberty Alliance in mid - 2004.



Developed by the private sector, governments are now starting to apply FIM technology

From ADAE's point of view, FIM technology has many advantages for establishing standards of user identity management. These advantages go beyond the basic benefit of access simplification. For example, FIM can **reduce the investment in authentication systems** by each government department or level of administration. By its nature, FIM is also well-suited to federal organisations and so can be used to link national and local services, with the possibility in the future of expanding to include European services.

ADAE is also working on a proof of concept aimed at improving the user experience of federated identity.

A FIM infrastructure, compliant with Liberty Alliance standards and usable across the range of French public services, will be constructed in 2006. FIM in France will 'go live' in 2007, firstly on the French administration's personalised portal, and then for other services. ADAE is also studying the notion of Attribute Providers¹ linked to federated identity, as a way of simplifying user data management in eGovernment procedures.

⁽¹⁾ An Attribute Provider is defined in Liberty Alliance specifications as follows: The attribute provider (AP) provides Identity Personal Profile (ID-PP) information. Sometimes called an ID-PP provider, the AP is an ID-WSF (Identity web services).

For further information:

The Liberty Alliance: <http://www.projectliberty.org/>
OASIS (Organisation for the Advancement of Structured Information Standards):
<http://www.oasis-open.org>
ADAE (Agence pour le Développement de l'Administration Électronique):
<http://www.adae.gouv.fr>

ENSURING PRIVACY: DATA PROTECTION IN THE EU

Data protection enjoys a high priority in the EU. A recent paper by the Liberty Alliance¹ notes that the EU's approach to privacy and data protection has become an important international standard, and any federated or other electronic identity scheme must meet the rigorous legal requirements in this respect.

The two primary relevant Directives in the **data** protection and privacy field are the **Data Protection Directive** and the **Electronic Communications Privacy Directive**.

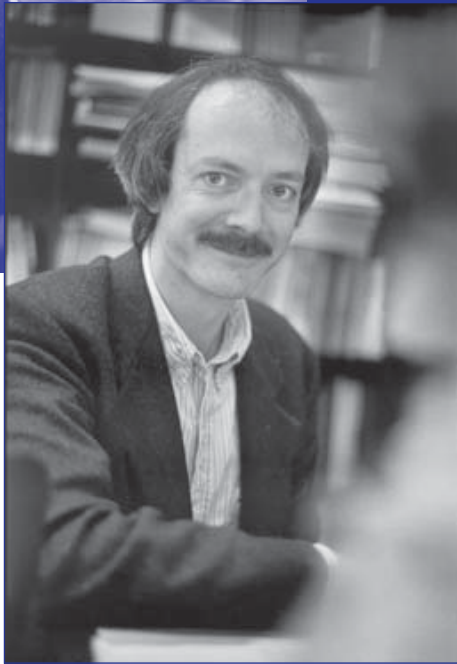
The first of these, agreed by the European Parliament and the Council in 1995, gives equal protection to the personal data of all EU citizens, though it only applies to areas within the EU's competence and thus does not cover public security, defence or criminal law enforcement. The Directive states that data can only be collected for specific and legitimate purposes; it must be relevant to the use it will be put to; it must be accurate and up-to-date and there must be reasonable access for checking and erasing incorrect data; data cannot be kept longer than necessary; and all data controllers must adhere to a supervisory regime.

The Directive also states that data can only be processed if the data subject unambiguously gives consent. More sensitive data (such as health data) is treated even more stringently.

The Electronic Communications Privacy Directive, adopted in 2002, updated earlier data privacy rules and adapted them to modern electronic communications, for example, by clarifying the position of email. It introduced new information and consent rules on entries in publicly available directories, along with an 'opt-in' regime for electronic communications used for marketing. It also introduced controls on cookies and other Internet tracking devices.

⁽¹⁾ *Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation, Liberty Alliance Project, February 2005.*

Further information about the data protection and privacy regime in the EU, including full details of the Directives, can be found at:
http://www.europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm



*Interview with **Bart Preneel**, Professor in the research group COSIC (COmputer Security and Industrial Cryptography) in the Electrical Engineering Department of the Katholieke Universiteit Leuven in Belgium.*

Professor Bart Preneel is a leading researcher into information security, with involvement in a number of European projects examining questions of electronic identity and privacy. He is presently leading a study on identity management in eGovernment under the European Commission's MODINIS programme.

WHAT IN YOUR VIEW ARE THE MAIN FACTORS DRIVING THE CURRENT DEVELOPMENT OF eID INITIATIVES IN EUROPE?

Several Member States, starting with Sweden and Finland, identified a need to move towards eID. A number of other countries also have quite advanced schemes. In Estonia there is very extensive coverage. Austria, Belgium, Italy and Spain have also made progress.

I was involved with writing the specifications in Belgium as early as 1999. The Belgian rollout started in 2004 and is now in full swing, but it will take until 2009 for the full rollout of 10 million cards.

The first goal of such a card is convenience for the citizen, and hopefully in the long term cost reduction for the government, though in the short term there are costs. For example now I need a card reader. However, if I have this, the benefits of the card become apparent. For example, I could look at the national register and see what is written about me and who asked for access to my files recently. I can ask for corrections to be made, all electronically. In the past you could also do it but it was more expensive and there were limits to how often you could do it. Now if you feel like it you could go every day and check.

This is one example, but the strength of the card is that there is a broad range of applications. Of course taxes and some other applications don't necessarily need very high security as embodied by a card. Governments need to look at an integrated approach.

The real benefits of eID will be felt only with private sector involvement. In banking for example, now they need a photocopy of my ID card; with an eID card everything can be done remotely.

WHAT ARE THE MAIN BARRIERS STANDING IN THE WAY OF THE INTRODUCTION OF eID?

There are of course several problems, such as infrastructure. A vast range of applications will become much easier once the infrastructure is established. There is a good case to be made for governments to invest in infrastructure so everybody benefits.

Another question is interoperability. I was surprised to learn that 10 percent of the population in Belgium, one million people, are special cases. Either they work abroad or they don't have Belgian nationality. It just shows why having an open, well-defined system with clear interfaces is important: more people want to work abroad, or collect their pensions abroad.

There are thus a number of administrative benefits from interoperability, but also for business.

But different systems are being developed in Europe. In Belgium every citizen gets one number, every administration uses this number, and all databases are linked through one central system.

But many other countries have multiple identities: for pensions, for social security, for healthcare and so on. This protects privacy but in terms of interoperability is a problem – how can these systems work together? In this respect it is certain that technical, organisational and legal issues are closely related and cannot be separated.

HOW WOULD YOU ADDRESS FEARS SOME CITIZENS HAVE ABOUT 'BIG BROTHER' AND THE RISK TO PRIVACY eID IS SEEN TO PRESENT?

Privacy is important. You have a certificate attached to your ID card, with your name and your key; it is a unique number so even if it's a random number, if you use it in every application people can theoretically link what has happened.

For many countries this is a big issue. In Germany, Austria, France and Portugal, for example, different government services are not allowed to link identities. The Austrians have a good solution to this problem whereby every application has its own number and the card computes the number for the application. It's a very neat solution.

There is also the question of what you need your eID to prove. One successful application in Belgium concerns municipal waste sites. In principle, citizens taking waste to the site only need to prove that they live in the city in question. They don't need to give any other information. So there is a question of eID being used in proportion to the need.

One answer to this may be the technology we are looking at in the PRIME project¹. We are building on IBM research, which allows this proportionate use, but

the technology is much more complex than what we have now. The mathematical eIDs in cards now date back to 1978; the engineering of them was done in the late 1990s and deployment is happening now. The eIDs developed by IBM are more sophisticated and my view is we should plan to implement those, because then eID will gain greater public acceptance.

WHAT IS YOUR PROGNOSIS FOR THE FUTURE DEVELOPMENT OF eID IN EUROPE?

We should try to identify the key issues and see what the advanced solutions are, and then we have the option of defining interfaces. It doesn't have to be too complex. As a Belgian citizen for example, if I go abroad and go to the city hall or a bank, I could just use my card online to go to a Belgian server to attest who I am. There would just need to be an agreement that one country will recognise the attestation from another.

Card solutions have big advantages but you already have one card in your GSM. In the future your card may identify you, but also your fingerprint and your GSM. We will have multiple devices for identification. It would be more secure and more robust so if you lose one you're still identifiable.

The most difficult point in this matter is to rollout things in a way that can be upgraded in the future. If you build technology well actually it protects you better than now. Now if you lose your wallet, you lose everything. If you have eID it actually protects your privacy much better – the card will be useless to anyone else.

⁽¹⁾ PRIME – privacy and identity management for Europe, a European RTD Integrated Project under the FP6/IST Programme. See <http://www.prime-project.eu.org/>

The importance of interoperability for electronic identities is becoming more central as European integration deepens. There are more opportunities than ever for cross-border living and working and it is vital that there are opportunities for debate on eID between governments and for exchange between the private and public sectors. At the same time, learning about good practice from outside Europe can deepen understanding of the eID challenges facing Europe. One forum for discussion and exchange of good practice in eID, helping to inform the European perspective, is the Porvoo Group.



© Getty Images

The Porvoo Group: a meeting place for discussion of eID technology and good practice

Established in the Finnish town of Porvoo, the Group was initially an initiative of the **eEurope Smart Card Charter**, a project launched in 1999 by the European Commission to examine interoperability and security questions in relation to smart cards, and the **Finnish Population Register Centre**, which continues to provide the permanent secretariat for the Porvoo Group. The aim of the Group is to be a pro-active European-level electronic identity interest group, and to provide relevant contributions to informed public debate about eID questions.

The Porvoo Group meets twice a year with the most recent meeting – known as **Porvoo 7** – taking place in Reykjavik, Iceland, on 26 and 27 May 2005. The seminar brought together government, private sector

and European Commission representatives and included presentations on the Icelandic eID and PKI experience; the US Government Smart Card Program and Personal Identity Verification card; the Japanese Resident Registration Card, which is being developed as an eGovernment authentication tool as there is no national identity card in Japan. The meeting also reviewed the state of play within the EU, with country updates from Austria, Belgium, Estonia, Finland, France, Germany, Italy, Sweden and the UK.

IDABC contributed to the meeting with a presentation on the status of the **IDABC Bridge/Gateway CA Pilot Project**. Technical aspects and current results of the project were also presented, including interoperability tests with the Belgian eID card.

Legal aspects, meanwhile, were not overlooked. Tapio Aaltonen of the Finnish Population Register Centre presented a report on **European cross-border legislative eID environment**. The European Commission is working on legal questions through several initiatives, such as a study on identity management in eGovernment being conducted under the Directorate-General for Information Society's Modinis programme¹, and Porvoo 7 adopted a suggestion to feed its report into the Commission relevant expert working groups.

The Porvoo Group meetings are proving increasingly popular for representatives of administrations. Porvoo 7 was attended by the Belgian and Spanish Ministries of the Interior, the Austrian Chief Information Office, Greece's Ministry of Employment and Social Protection, Hungary's Ministry of Informatics and Communications, the UK Office of the Deputy Prime Minister and a number of other ministries and departments from across Europe dealing with eID matters. Following each meeting, the Porvoo Group issues a communiqué, consisting of a summary of the issues discussed and the resolutions passed, concerning issues such as on-going Public Key Infrastructure (PKI) projects, standardisation, biometrics and relevant European level legislation.

This programme originated under the Dutch Presidency of the European Council in late 2004. It calls on the Council and European Commission to develop minimum security standards for eID cards including biometrics. In respect of these emerging developments, a plenary session at Porvoo 7 on the application of biometrics in eID noted that a number of countries plan to set up national biometric databases to support their ePassport schemes, and this will have an impact on the limiting of verification of biometrics to on-card matching. Actions relating to biometric passports will have a major impact on eID card schemes, and the Porvoo Group has resolved to discuss this developing issue further at its next meeting.

Prior to the Rejkjavik meeting, Porvoo 6 took place in November 2004 in Rome, where representatives from around 20 countries met. Resolutions arising from the meeting included a strong expression of support for positive horizontal co-operation in establishing and maintaining real interoperability between certification authorities, and for the inclusion of interoperability aspects in international standards in the smart card, certification infrastructure, and biometric domains. A resolution was also passed calling on major PC manufacturers to incorporate standardised features in smart card readers.

Another resolution concerned use of fingerprint biometrics in passports and eID cards. The Group noted that there was an immediate need for an international standard template for fingerprint minutiae. At Porvoo 7, the Group noted that in respect of biometrics, a number of important initiatives are currently underway or are due to deliver outcomes in the near future, in particular, the development of a new EU multi-annual programme called **The Hague Programme; strengthening freedom, security and justice in the European Union**.



⁽¹⁾ For more information on this, see the article 'Identity management advances on multiple fronts' on page 5 of this issue.

For more information:

The Porvoo Group:

<http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290>

The Hague Programme:

http://europa.eu.int/comm/justice_home/news/information_dossiers/the_hague_priorities/index_en.htm

