Prepared for the eGovernment Unit

DG Information Society and Media

European Commission

Modinis Study on Identity Management in eGovernment

The Status of Identity Management in European eGovernment initiatives

28 February 2007

Table of contents

modinis*IDM* Member State- / Projects Overview

Out of MODINIS a project to identify good practice projects on eGovernment has been contracted by the European Commission. As one of three lots, the **modinis*IDM*** study will identify good practice projects on identity management and aim to build on expertise and initiatives in the EU Member States to progress towards a coherent approach in electronic identity management in eGovernment in the European Union.

This document is the first coordinated and public version of a national status report of the most significant IDM systems used throughout the 25 European Member States. While the report does not aim towards completeness – this would not be a realistic goal, since most Member States employ dozens or even hundreds of parallel IDM systems in their administrations, all with a different goal, scope and impact – but rather, the report would like to present the reader with an overview of the most predominant IDM systems in the Member States. Specifically, the report focuses on such IDM systems which potentially impact the whole of the Member State's population and/or business initiatives, and which are thus most likely to show potential for generalisation and/or cross border functionality.

A first version of the document was produced on 2 May 2006. This is the final iteration of the document. The most up to date versions of the national reports are available through the project website (https://www.cosic.esat.kuleuven.ac.be/modinis-idm). These profiles will be continuously updated as new information becomes available to the project team.

1.1 Document Scope

As stated above, the present report would like to present the reader with an overview of the most predominant IDM systems used in eGovernment applications in the Member States. Specifically, the report focuses on such IDM systems which potentially impact the whole of the Member State's population and/or business initiatives, and which are thus most likely to show potential for generalisation and/or cross border functionality.

The information in this report was collected through a variety of sources:

- Information that was directly known to the authors in their capacity of experts in the field of eGovernment IDM solutions;
- Information that is made commonly available through public administration web sites (i.e. eGovernment project sites);
- Information that is disseminated through specialised research web sites (including such projects as the GUIDE project, FIDIS, and PRIME);
- Information that is provided through the **modinis*IDM*** study team's network of experts, including through formal and informal interviews, and including the information collected through or as a result of the **modinis*IDM*** study workshops or related activities;
- Reports that have been submitted via the standardised questionnaire which has been disseminated at the **modinis*IDM*** study workshops or through the project website;
- Feedback received as a result from visitors to our website.

As a result of this approach, most of the reports have undergone a *de facto* expert review, as a result of the information being collected from an official source or through the intervention of a national expert. However, this is not the case for all country reports.

Therefore, activities have focussed on:

- Increasing the depth and detail of the reports;
- Ensuring that all reports have undergone adequate quality review, most notably through the intervention of the expert mailing list and through further dissemination of the present document as an RFC.

The result of this process is the present document and concludes the **modinis*IDM*** study.

1.2 Status of Identity Management in Member States

1.2.1 Introduction

1.2.1.1 Study planning

The Call for Tender document describes one of the **modinis*IDM*** study's core targets as follows:

> *Present the status of identity management in member states, issues, successes, failures and lessons learned, future plans;*

This information is to be the foundation of **modinis*IDM*** study's research activities, which entail three distinct phases:

- *Phase I: Information collection*

  The first phase consists of the identification of existing major European IDM systems, along with their scope, advantages, weaknesses, and lessons learned. This first phase resulted in the previous version of this report, which set the parameters for the two following phases, since the current status of eGovernment IDM solutions is the basic input on top of which a solution framework is to be constructed. As indicated above, the contents of the previous report were continuously updated through the **modinis*IDM*** study website, and the final outcome is summarised in this version, the second iteration of the report.

- *Phase II: Analysis of problems and barriers to IDM interoperability*

  A second phase, following the creation of the present overview of the status of IDM solutions in the Member States, was the identification of the problems and barriers to making these solutions interoperable. If phase I results in the description of the situation at the time of the **modinis*IDM*** study, then phase II will result in a definition of the difficulties to be resolved by the **modinis*IDM*** study's conceptual framework. The result of this second phase was a paper (D.3.9 and, in a final iteration, D.3.10) describing and analysing the barriers to interoperability.

  It should be noted that the lack of a suitable homogeneous, unambiguous and consistent terminology for discussing interoperability problems was the first problem identified by the **modinis*IDM*** study. This specific realisation resulted in the creation of the **modinis*IDM*** Terminology Paper, which has been presented through the **modinis*IDM*** study website.

- *Phase III: Proposal of a conceptual framework for European IDM interoperability*

  In the third and final phase, the **modinis*IDM*** study envisaged to present a conceptual framework, which would allow the existing solutions to exchange information, thus creating an interoperable pan-European IDM infrastructure. The proposal will keep into account the work already done by related initiatives both on a European and an international scale, in particular such initiatives as the Liberty Alliance and the Guide Project.

1.2.1.2 Information in the national profiles

The current paper represents the second iteration of the outcome of Phase I, and provides a full overview of the status of the most significant identity management systems in eGovernment applications across the Member States. The scope of the profiles can be delineated as follows:

- *Public sector IDM systems incorporating digital identities:*

  Firstly, the national profiles are limited to IDM systems (defined in the **modinis*IDM*** study terminology paper as "*the organisational and technical infrastructure used for the definition, designation and administration of identity attributes*") which have been set up by public administrations with a view of providing public services to a more or less broad section of the general public (without excluding legal entities). The services must thus be under public sector control, although this does not rule out the intervention of private sector parties for organising such services (i.e. through public/private partnerships or outsourcing initiatives).

  It should be noted that the examined IDM systems are limited to systems which work exclusively or in part with digital identities (defined in the **modinis*IDM*** study terminology paper as *"partial identities (i.e. a subset of one or more attributes of a specific entity) in an electronic form"*); traditional non-electronic IDM systems (such as paper registers (population, birth, land registers, immigration, tax, social security,…), paper identity documents (identity cards, passports, health cards, social security cards,…), paper licence documents (drivers licenses, public servant cards, fishing licenses, …) and so forth remain out of the scope of this document, except insofar as such documents are the direct or indirect precursors of present day solutions, in which case their existence may be indicated as valuable background information.

- *With a wide application or impact:*

  Only IDM systems with a potential impact on the whole of the Member State's population and/or business initiatives will be extensively examined. This excludes systems which are only in common use within a limited geographical reason, for internal administrations, or within specific niche sectors, unless such a limited service was identified as specifically relevant by a local expert. The most important reason for this is two-fold:

  - Most Member State use many hundreds of IDM systems, when one takes into account purely administrative systems (e.g. building access management) and local services (e.g. municipal staff administration). Such services are typically not susceptible to generalisation, nor are they particularly relevant for the purposes of the **modinis*IDM*** study.

  - Furthermore, the **modinis*IDM*** study is concerned with services which show some promise or potential for cross-border interoperability, i.e. services for which the integration of/cooperation with foreign IDM systems offers a certain added value. For this reason, only IDM systems with a generic or at least sufficiently broad service scope are significant for the **modinis*IDM*** study, and only such IDM systems are described below.

- *General description and assessment:*

  The profile for each country will provide the following information:
  - A brief description of the most significant IDM systems, both existing and planned systems;
  - An overview of the scope and history of these systems, including a description of its technical and organisational characteristics, the applications (both existing and

planned) which are accessible through the IDM system; and references to public sources, when available;
- An assessment of the solution, including its strengths, weaknesses, and lessons learned throughout the deployment, implementation and functioning;
- The expected evolution of the systems, including any new systems to be introduced which could replace existing solutions.

1.3 National reports

1.3.1 Austria

1.3.1.1 General status and most significant systems

The Austrian IDM approach "Konzept Bürgerkarte" covers various eID tokens both issued by the public sector and the private sector. The idea followed allows the citizens the choice on which eID token to activate. In this technology neutral approach several public sector and private sector smart cards initiatives have currently taken up the concept, as well as a mobile service provider that allows to use any cell phone capable of receiving SMS to act as a citizen card.
The major rollouts are:

- Health insurance card - roll out started in May 2005 and was completed in November 2005, approx. 9 Mio cards have been issued to date
- Bank cards – each bank card issued since March 2005
- A1 signature – a service launched in 2004 to activate mobile phones as citizen card
- Public Service Cards of several federal ministries

Further initiatives include the membership card of the Austrian Computer Society (first smart card rolled out as citizen card in 2003; meanwhile discontinued), civil servant's service cards, or student service cards rolled out by some universities.

A History, Scope and Goals

The Austrian citizen card initiative has been launched in a Cabinet Council in November 2000 with the intention to employ smart card technology to facilitate access to public services. The government decided to enhance the health insurance card to be issued to each citizen by electronic signatures. However, already in early stages of the project the intention has been declared to remain open to the market, i.e. to remain open for other smartcards or other technologies.
To define the requirements a white paper "Weißbuch Bürgerkarte" has been prepared in 2001. This white paper defined the requirements on an eID and IDM system on a general level and from the government's perspective.
As a follow-up, technical standards have been developed that consist of a technology neutral XML-based interface "Security Layer" and a set of minimum requirements that a technology needs to fulfil in order to constitute an "Austrian citizen card". To illustrate how technology-neutrality has been approached, these minimum requirements inter alia include the need of being capable of generating or verifying electronic signatures, but e.g. no mandatory cryptographic algorithms are specified, thus allowing for RSA, DSA, or ECDSA. Common signature formats are defined (such as cryptographic message syntax or XML dsig).
A further requirement is that two key-pairs are given – one as a supplement of the handwritten signature (qualified signature or administrative signature, see below) and another one for other digital signatures or to encrypt data.
The legal basis has been established in March 2004 with the Austrian E-Government Act. The IDM concept is based on a so-called identity link. This is an electronic attestation that establishes a link between personal identification numbers and electronic signatures as a separate signed data structure. Moreover, the data protection principles that need to be followed have been laid down. Aside identification of the citizens using the citizen card, rules for electronic representation and acting as proxy have been defined.
A general principle followed by the citizen card issuers is that citizen card implementations are ready to be activated as citizen card, but in the end it is the citizens' choice to actually activate the electronic signature (apply for a digital certificate) and to activate an identity link.
The concept has been followed by both the public sector and the private sector. By mid 2006, the major rollouts are:

- Public sector
- Health insurance card "e-card": Smart card system to replace health care certificate complemented by electronic signatures (secure signature creation device SSCD as defined in Directive 1999/93/EC). Its rollout to each citizen started in May 2005 at a rate of 70.000 cards/day. Rollout has been completed since November 2005.

- Public service card of the Federal Ministry of Interior and the Federal Ministry of Finance (SSCD smart card system launched 2004/2005).
- Student Service Cards of some universities (smart cards with qualified signatures)
- Private Sector
- Mobile phone service "A1 Signatur": Started in March 2004. The mobile service phone provider A1 offers a service where the identity link and the electronic signature's private keys of the citizen are stored in a security server that are activated by the citizen via username/password and an one-time code send via SMS to the citizen's mobile phone.
- Bank cards "Maestro/Bankomatkarte": Each bank account card (ATM Card) rolled out since March 2005 is capable of qualified signatures (is an SSCD) and can be activated as citizen card.
- A-Sign Premium: The private sector qualified certificate CA A-Trust issues the product A-Sign Premium as citizen card.
- Membership card of the Austrian Computer Society "OCG Karte": The OCG started to issue their membership smart cards as citizen cards in 2003. The service has ceased in 2005 with the massive rollouts of e-card and Bankomatkarte.

The software required with the citizen's PC to implement the technology-neutral interface "Security Layer" has been procured by the government as a general license and is made available for free. The general license supports all the smart card systems described above. In addition, further EU Member State eIDs are being integrated.
To complement the citizens' eID infrastructure at the server side the Austrian government has procured so-called "Modules for Online Applications" (MOAs). The MOAs are basic modules that are made available free of charge. MOAs implement the processes required at the server side for identification, signature verification, signature creation, or electronic delivery.

B Technology

The citizen card concept is based on an open Web-based interface (Security Layer) that represents an abstraction of the citizen card environment (e.g. the smart card, or the card reader and drivers). High-level XML-based commands are used to e.g. create an electronic signature or to start the IDM process using the identity link. This de-couples the eGovernment application (e.g. a Web-Service) from the actual technology used for the citizen card.
The major technologies used are:

- Health insurance card e-card: A smart card using elliptic curve cryptography (ECC), 192 bit NIST GF(p) curve, Giesecke & Devrient StarCOS chip operating system.
- Bank Cards: A smart card using ECC, 192 bit NIST GF(p) curve on an Austriacard ACOS chip operating system.
- A-Sign Premium: Various smart cards using 1024 Bit RSA, Siemens CardOS or Giesecke & Devrient StarCOS, and for 192 bit ECC the Austriacard ACOS (bank card) chip operating system.
- A1 mobile phone signature: Server-based hardware security module.

The IDM approach is based on sector-specific personal identification numbers (ssPINs) that are cryptographically linked to the electronic signature. A three tier approach is used:

- In the first tier, unique identification numbers (base identification number) of national registries identify the natural or legal person. The registries are the Central Register of Residents for natural persons, the Register of Company Names and the Central Register of Associations for legal persons, a Supplementary Register for natural and legal persons not covered by the registers mentioned before (e.g. foreigners), respectively.
- The second tier is the identity link which is only stored at the citizen card. The identity link holds a unique number (source personal identification number – sourcePIN) that – for natural person – is cryptographically derived from the base identification numbers of the first tier and the public keys stored in the digital certificates. The identity link is signed by a public authority (sourcePIN Register Authority). This signature attests that a person approaching the public authority using her/his sourcePIN (identification function) and subsequently signing using her/his electronic signature (authentication) is the very person whose identification credentials have been derived from public registries.
- The third tier is the concept sector-specific personal identification numbers (ssPINs). The IDM processes may not store sourcePINs for data protection reasons. By using cryptographic hash-functions, ssPINs are derived from the sourcePINs so that a citizen is

uniquely identified within a certain sector of state activity (e.g. tax, health, social security, etc.), but linking between ssPINs of a citizen in different sectors is inhibited, except for cases where the citizen allows such cross-relations by providing her/his citizen card (the sourcePIN), or where legally admitted the data protection authority creates the cross-relation via the first tier registers.

In addition to the public keys and the sourcePIN, the identity link stores the name and date of births as these data are frequently used in official processes.

The PKI providing the certificates for the electronic signatures can be both private or public sector borne. The CA contracts as service provider for the sourcePIN Register Authority that is signing the identity link. The identity link is generated during the registration process at the CA or afterwards. The following CAs are currently established or announced:

- Private sector
- A-Trust, e.g. issues certificates for bank cards
- A1 signature issuing certificates for the mobile phone signature
- Public sector
- The health insurance system issues certificates for the health insurance card e-card since November 2005

The validity period for certificates depends on the CA. For qualified certificates, the Signature Order allows for a five year validity period. However, e.g. bank cards are physically replaced in a three year period that determines the validity.

The Austrian E-Government Act has a transitional provision until end of 2007 that for the citizen card function so-called administrative signatures shall be treated the same way as qualified signatures, i.e. signatures following article 5.1. of Directive 1999/93/EC. This allows for citizen cards that are not based on SSCDs or on qualified certificates (i.e. as defined in Annex I-III of 1999/93/EC). Currently, the situation is as follows:

- Qualified signatures (SSCD and qualified certificates): Bank cards, A-Sign premium, student service cards, and civil servant service cards of ministries
- Administrative signatures using an SSCD (but no qualified certificate): e-card with certificate of the health insurance systems (the system is however open for CAs to issue qualified certificates)
- Administrative signatures (no SSCD, no qualified certificate): A1 mobile phone signature

The eID system is open to the private sector. E.g. some banks follow the concept in their Internet banking applications. If the ssPIN IDM model is used, additional data protection provisions apply. Specifically, generating the private sector ssPIN (pssPIN) is done in such a way that the unique identifiers are created uniquely for each private sector entity so that two companies cannot cross-relate their customer's identifiers (ssPINs).

Provisions for access for non-Austrians are being made. The Belgian eID BELPIC, the Estonian eID, the Italian and the Finish e-ID are already integrated into the software procured as general licence by the government. The concept followed is to add the foreign citizens – if not anyhow registered in the Central Register of Residents – to the Supplementary Register and to create a "substitute sourcePIN" from an identifier in the foreign eID. This substitute sourcePIN is the basis for the identity link the IDM system is based on.

C Applications

Several applications on the national, regional, and local level can be used, such as:

- tax applications online
- application for register of convictions certificates
- application for electronic residence certificates
- electronic delivery of notifications (also substituting registered postal mail)
- VPN solutions such as access to ELAK (government's electronic dossiers)
- various applications of cities, municipalities

Information sources:

- http://www.buergerkarte.at (citizen card information in German and English)
- http://www.cio.gv.at (federal ICT strategies, mainly German)
- http://www.help.gv.at (federal portal, in several languages)
- http://www.egiz.gv.at (e-government innovation center)

1.3.1.2 Existing issues

The Austrian approach raises a few issues, which can be summarised as follows:

- Future interoperability standards: Adoption of future interoperability standards seems difficult, if these go into too much technical detail. Massive rollouts in various technologies make it hard to argue to replace such investments. However, integration of implementations of such standards is rather easy, as the integration of the Belgian or Estonian eID has shown.
- The Signature Order that had been enacted in 2000 settled requirements for card readers and viewers. This impeded broad coverage with card readers. An amended Signature Order of 2005 removed the certification requirements of the signature environment except for the SSCD. Moreover, for a limited amount and period, parts of the card reader costs are sponsored by banks and the government.

1.3.1.3 Analysis: successes, failures and lessons learned

The lessons learned from the Austrian eID-project can be summarized as:

- Openness for various technical approaches allows for an eID market and various solutions that give the citizens a choice.
- Both the private sector (e.g. banks) and the public sector (e.g. health insurance system) can roll out eID tokens.
- Availability of server-side modules (e.g. the MOAs in the Austrian system) to facilitate integration of the IDM concepts is as essential as the citizen's eID tokens. In particular at the local level, availability free of charge stimulates take up.
- Coordination between the national, regional, and local level is an important aspect in order to understand the various needs.

1.3.1.4 Expected future developments

Even though 100 % coverage of at least one eID token per capita have been reached in 2005, further citizen cards are expected (most of the citizens even possess several tokens that can be activated as citizen card, e.g., bank card, health insurance card, mobile phone). E.g. further universities that offer smart cards as student IDs or further public authorities that roll out service cards.

1.3.2 Belgium

1.3.2.1 General status and most significant systems

The most significant IDM eGovernment project in Belgium is the introduction of the Belgian Personal Identity Card (BELPIC), an electronic identity card that should facilitate access to eGovernment services for all Belgian citizens, as well as offering a variety of other services. Detailed information is available through the official Belgian eID website (http://eid.belgium.be; available in Dutch, English and French); we will summarise the key characteristics below.

A History, Scope and Goals

The Belgian Council of Ministers decided in July 2001 to introduce an electronic identity, to be issued to every Belgian citizen over the age of 12. It was decided that the card should have the dimensions of a bank card, and should contain a photo, the national registry number and a set of other identification data. The data should be printed on the card as well as integrated electronically on a chip (with the exception of the holder's address, which should only be stored electronically, but not printed on the card, because of its changeable nature).
The chip should also contain two electronic key sets, allowing the authentication of the citizen and the use of a qualified electronic signature. This should improve government efficiency, since the electronic authentication would allow the government to retrieve the electronic information about the holder that it already has, thus reducing unnecessary form filling (the so called "authentic source" principle: there should be only one authentic source for each piece of information, to be reused by all applications) and data redundancy. The keys should also allow the citizen to authenticate himself in private sector transactions and to conclude legally binding electronic contracts.

The eID-card is being deployed since the second half of 2003, and at the time of writing more than a million card have been issued (for up to date statistics, visit http://godot.be/eidgraphs). Rollout is envisaged to be completed around the beginning of 2008.
Along with this rollout, the organisation of public services is also undergoing reform to ensure efficient and secure exchange of information, and to increase the number of services available to eID card holders. This is particularly important as Belgium is a federal state, and the separate administrations will need to provide services which use the eID without compromising their autonomy in their fields of competence. To this end, the federal government concluded a cooperation agreement in March 2001 with the regions and communities, emphasising also the necessity of collaborating with the provinces and municipalities. As a consequence, citizens will be able to use their eID card as an authentication mechanism for the electronic services at each of these levels.

B Technology

The eID is based on PKI technology, and incorporates two certificates: one for authentication, and one for electronic signatures. Each private key is dependent on the use of a PIN-code. Each card is issued at the level of the municipalities (which function in this regard as registration authorities), and has a validity of 5 years. The cards are produced, initialised and personalised by private company ZETES (http://www.zetes.com), which also provides the Belgian social security card (SIS-card). The certificates are managed by Belgacom (majority shareholder: Belgian State), which functions as certification authority.
As mentioned above, certain personal data (such as the first and last name, national registry number, gender, place and date of birth, photo and nationality) is stored on the card. No biometric data is involved or currently planned. This information cannot be updated, so when an element changes the card itself needs to be replaced. Any other information must be retrieved using databases and information networks currently in place or to be added; no additional data regarding the holder will be stored on the card. This increases the security and reliability of data, and allows more strict access controls since the validity of all access requests can be checked against an authorisations database.
Identification of the citizen is based on his national registry number. Use of this number is strictly monitored, and subject to prior approval by a sectoral committee within the National Data Protection Commission (http//www.privacy.fgov.be). This same number is also used within the Crossroads Bank for Social Security (http://ksz-bcss.fgov.be) to exchange administrative information about the citizens between administrations. Similarly, companies and organisations are also assigned a unique identification number to be used in conjunction with the so-called Crossroads Bank for Enterprises (which also incorporates the central trade registry and the national registry of legal persons)
The eID card also has the capability to contain programmes which can be run within the card processor chip, e.g. for generating key pairs and using the private keys. Expansion of the eID's functionality is presently being investigated; see below.

C Applications

Presently the number of available applications is limited, but increasing. In the long run the eID card will allow the user:

- to access the records kept by the local authorities about you (see https://www.mondossier.rrn.fgov.be for a practical application: consulting the data the National registry's has regarding you)
- to request administrative documents (e.g. birth certificates) on-line
- file taxes electronically. See www.taxonweb.be for a practical application regarding income tax declaration)
- to electronically file statements or complete administrative transactions (social services, banks, post, insurance…)
- to get in touch with his municipal authority. Several municipalities are already equipped with electronic windows that enable the citizen to make requests by filling in electronic forms. The advantages of using an eID card (electronic identification and signature) will make contacts with local authorities easier, quicker and more efficient.
- to get in touch with the regional and federal services on the Internet. The website of the Federal Public Service FEDICT (http://www.fedict.be) or the federal portal

(http://www.belgium.be) enable the citizen to contact all other Federal Public Services and to find the information he needs to know. He can also consult:

- the Walloon portal at http://www.wallonie.be/
- the Flemish portal at http://www.vlaanderen.be/
- the Brussels portal at http://www.bruxelles.irisnet.be/
- the German-speaking portal at http://www.dglive.be/
- the portal of the French Community at http://www.cfwb.be/
- to make secure commercial transactions on the internet (on-line selling and buying)
- to affix an electronic signature to documents with the same legal value as a handwritten signature
- to use a variety of applications which will be put at the citizen's disposal in the future by the State as well as by the private sector (bookings, registrations, payments, orders, to terminate contracts as well as many other things, in complete security. Company badges, electronic payment cards, on-line VAT declarations… represent other examples of possible applications).

(Main source: http://eid.belgium.be)
Additional possible applications are currently being investigated as a part of the ADAPID-project (ADvanced APplications for the IDentity card – https://www.cosic.esat.kuleuven.be/adapid/), which will focus on eGovernment, eHealth and Trusted Archival Services.

1.3.2.2 Existing issues

The Belgian approach presents a number of issues, which can be briefly summarised as follows:

- Accessibility to non-nationals: the Belgian system is largely built for Belgian nationals. For persons who are not registered in the national registry or in the so called waiting registry (e.g. asylum seekers), a secondary registry known as the "Bis-registry" is planned. All government databases have been or are currently being redesigned for this purpose.
- Additional features can be built into the eID system, but are thus far largely unavailable. The RAPID project mentioned above is looking into this. None the less, additional information systems (such as the social security card (SIS-card) and driver's licence still coexist with the eID-card. While integration of these cards into the eID is envisaged, no solid timetable exists at this time
- The suitability of the eID for cross-border interoperability needs to be examined. Belgian interoperability efforts have mostly focused on national A2A transactions between the different administration levels (federal, regional, community, municipality,…)
- While the rollout of eID cards is proceeding smoothly, the lack of applications and the relative rarity of card readers results in a limited use of the cards electronic features in practice. However, promotion activities are being undertaken to alleviate this problem.
- The functionality for mandates/proxies can be emulated through the creation of separate mandate databases (as is being done for e.g. online tax declarations), it remains to be seen whether this will prove sufficient. The system seems to be working in a satisfactory manner with regards to tax declarations.
- A number of smaller practical and organisational issues have presented themselves. E.g., as described above, address information is incorporated electronically, but not visually on the chip. This implies that e.g. the police can only verify a citizen's claimed address if they have the required reader. Since the distribution of such readers was delayed, local governments have resorted to issuing a separate document stating the card holder's address along with the eID card. While this is a temporary solution that has already been solved in many places, it was none the less considered an inconvenience by many citizens who thought it an inherent flaw of the eID card's design.
- Due to its strongly centralised character, privacy management is legally quite complex. While centralisation also allows the implementation of strong control mechanisms, the Belgian system only allows access to personal data by third parties upon approval by a sectoral committee of the National Data Protection Commission. While this approach has worked thus far, its scalability remains to be seen when the rollout of new applications increases.

1.3.2.3 Analysis: successes, failures and lessons learned

The following stand-out as the lessons to be learned from the Belgian eID-project:

- Roll-out has been fairly smooth and very cost-effective when compared to solutions abroad. This is mainly attributed to the choice of a single certification authority, thus maximising the economics of scale and countering to a certain degree the risk of a digital divide. This risk is also reduced because the Belgian approach focuses on reforming the administration's back office as a whole, so that benefits are not limited to users of electronic services. Traditional (non-electronic) channels also remain available, in principle at the same costs as the electronic version.
- The extensibility of the system can be questioned because of the limited number of available applications. While additional applications are in the works, there is thus far no "killer application" that clearly demonstrates the usefulness of Belgium's IDM choices to the public.
- The Belgian IDM system is technologically limited, in the sense that a smart card has been chosen as the medium of choice, and that the inclusion of any other technology might prove to be very difficult.
- The centralised privacy protection system described above (depending on centralised clearance of personal data use) is currently functioning as planned, but its scalability has not yet been tested.
- Potentially the greatest success element is the rollout of an IDM system within a (complicated) federal state, that is functioning on a federal/regional/community/municipality level.

1.3.2.4 Expected future developments

See the RAPID-project mentioned above for newer applications. The current principal question is when the rollout of additional applications that would increase the eID card's usefulness can be expected, and if and when other identification mechanisms (such as the SIS-card and driver's licence) can be integrated into the eID card within a reasonable timeframe.

1.3.3 Cyprus

1.3.3.1 General status and most significant systems

Cyprus identifies persons – legal and natural persons – by using the following identifiers:

- Natural Persons: a single identification number exists; but in some application sectors – social security, national health system, passports, electoral cards – separate ID-numbers are in use; other application specific identifiers, such as the tax number or the driving license number, are derived from the single identification number.
- Legal Persons: single identification numbers are used; VAT and taxation numbers are linked to the single identification number.

Single identifiers in order to uniquely identify natural persons exist; they are managed in the database of the Cyprus Civil Registration System which is managed by the Civil Registry Department under the authority of the Ministry of Interior. A single identification number is assigned to every person who is born in Cyprus, is a foreign worker in the Cyprus' labour market pension fund or has to deal with tax affaires. The single identification number is usually used as primary key in almost every governmental IT system.
There is no specific legal framework in place to regulate the usage of these single identification numbers. For identification purposes the single identification number (number of the identity card) is usually taken by both, public authorities and private organisations.
Cyprus links the following attributes of a natural person to a person's single identifier (beyond others):

- name, first name(s), sex, date of birth, place of birth, address
- former names, parent names, nationality, marital status, religion
- photograph
- legal right to stay in the country

Other application specific identifiers that are derived from the single identification number are:

- social insurance number
- driver license number
- military number

- electoral booklet number
- refugee booklet number

1.3.3.2 Expected future developments

Cyprus plans to introduce electronic identities – in form of smart cards – to be mainly used for services of the public administration, but Cyprus intends to bring up an e-ID solution in cooperation with other EU Member States.
Currently, no concrete e-ID project is planned.

1.3.4 Czech Republic

1.3.4.1 General status and most significant systems

In the Czech Republic, identities are managed based on personal identification numbers. Every citizen has got a unique personal identification number which has been issued by the Ministry of Interior. These identifiers base on the citizen's date of birth plus a special number making the resulting personal identification number unique.
The personal identification number together with other significant data of a citizen, such as her name, surname, maiden name, date and place of birth, sex and nationality, are held in central and regional registers.
The Czech Republic has created a draft law of Data Sharing between Administrative Bodies (Návrh zákona o sdílení dat při výkonu veřejné moci) for interdepartmental review in July 2005. The main intention of this law is to set common rules for data sharing between public authorities, to provide a more effective administrative system and to eliminate the administrative burden from citizen site. Therefore, the law also foresees a closer incorporation of the three main registers, in particular the Central Register of Residents, the Register of Companies and the Register of Land and Addresses. After interdepartmental review the law will be promoted to the Czech government. The law may become effective in the year 2007.
Each resident of Czech Republic is required to possess a conventional identity card. Electronic identity tokens for all citizens are not yet in place.

1.3.4.2 Existing issues

A Identification Numbers of the Czech Ministry of Labor and Social Affairs:

Within the Czech Ministry of Labor and Social Affairs special identification numbers for client identification are used. Those identification numbers can be also included in qualified certificates and are required for the eTax service (see below) as well. It expects that this new system of identification numbers is going to replace the current system of unique identification numbers

B eTax (service for electronic tax returns):

The eTax service – a service for electronic tax returns for individuals – is available since the year 2003. To access this service, users have to use a qualified certificate which has to contain her unique identification number issued by the Czech Ministry of Labor and Social Affairs (see above).

C IZIP project – IT utilization in the health system:

IZIP - internet access to patient healthcare information – is a system for interchanging of healthcare information, i.e. a patient's (client's) medical file, for healthcare professionals. A patient who is registered with IZIP can empower her doctors or other healthcare workers to access her medical files through IZIP. To access the system, identification credentials and a password are used. Additionally electronic certificates from selected certificate service providers can be used to access IZIP.
IZIP's general partner is VZP, the largest healthcare insurance company in the Czech Republic, which covers about 70% of the Czech population (due to the high coverage rate, this system may become relevant for eGovernment as well). The IZIP project is under consideration of the Ministry of Health; a ministerial employee of the Ministry of Health is permanent board member of IZIP. Currently, IZIP holds 840.539 registered users and 7.892 registered healthcare workers (status by 20.01.2006).

D Qualified certification authorities

Three qualified certification authorities are in place in the Czech Republic by the year 2005:

- First Certification Authority, Inc. (I. CA)
- Czech Post
- eIdentity A.S.

All of them issue qualified personal certificates based on the Czech act on Electronic Signatures (Act NR 227/2000 Vol.).

E Chip cards in state organizations

The Czech Ministry of Labor and Social Affairs is currently the only state organization using chip cards in significant numbers. Since 2002, 6000 contact-based and 4000 contact-less cards have been issued. The contact-based cards can be used for creating electronic signatures as well. The ministerial e-IDs are mainly used for accessing the ministry's information system and to track employee's comings and goings.
Additionally, the ministerial e-ID provides control over disbursement of billions of crowns through social payments every month. In order to track who approved what payment to whom, applications are signed electronically by using the chip cards.
Another usage is the exchange of confidential information within the ministry using encrypted electronic correspondence (as the chip cards are capable of cryptographic functionalities used for electronic signatures and encryption).
For the future, a governmental project is planned to provide so-called "professional" chip cards for public administrative staff. The Ministry of Informatics is leading the project implementing a unified system of cards throughout the government and state administration offices. The project aims to equip 100,000 state administration workers and 50,000 regional administration officers with chip cards.

1.3.4.3 Analysis: successes, failures and lessons learned

The current system of unique personal identifiers for citizens is more or less similar to the current IDM system in Slovakia. A replacement of the current system is not envisioned.
Mentionable e-ID approaches can be found within the bodies of the public administration. For instance, the Czech Ministry of Labor and Social Affairs issues e-IDs to their ministerial employees. These e-IDs are not only used for identification purposes in everyday business, but also to electronically sign applications for disbursement of social payments (to track who approved what payment to whom).

1.3.4.4 Expected future developments

The Czech Republic has created a draft law of Data Sharing between Administrative Bodies. This law should ease the electronic communication between organisations of the public administration. This law may become effective in July 2007.

1.3.5 Denmark

1.3.5.1 General status and most significant systems

Denmark does not offer electronic ID cards or electronic identities and has shown no intention to do so. However the Danish government has taken an alternative approach and since 2003 it issues "free digital signatures" to its citizens as a means for user authentication. It allows a citizen to make use of online public services in a secure way.
The issuance of digital signatures is part of the eGovernment project that was started in 2001. Since then several steps have been taken to promote the transition of public services to eGovernment. One of the most recent actions was to make the online use of certain public services compulsory for all citizens.
For more information on the eGovernment project in Denmark see http://www.e.gov.dk/english/egovernment/index.html.

A History, Scope and Goals

The Danish Government has initiated a project in 2001 to coordinate the transition to eGovernment in Denmark, although public authorities themselves remain responsible for adopting eGovernment. The eGovernment project involved the central, local and regional government, and was initially meant to last for three years but has been extended in 2003 to the end of 2006.
As part of the project the government decided to initiate a modernisation of the Danish legislation. In January 2002 ministries were instructed to examine their legislation, to identify obstacles for digital communication and to point out if amendmends to legislation was needed to overcome the identified legal obstacles. For more information see http://e.gov.dk/english/results/2002/the_removal_of_legal_requirements/index.html .
In February 2004 a first public sector egovernment strategy was formulated that evaluated the results of the egovernment project and described a vision and signpost for egovernment. These should help to increase the quality of egovernment services and push the administrations further to digitalization. A second egovernment strategy is expected in the spring of 2006.
Two authorities that play an important role in the egovernment project are the Ministry of Finance and the Ministry of Science, Technology and innovation. Besides the Board and the Steering Committee of the project there is also a Digital Task Force that is responsible for the successful execution of the egovernment project.
One of the most important results concerning egovernment identity management was the decision taken in 2003 to issue free digital certificates to citizens. Scince February 2003 the Danish government provides digital signatures to its citizens, enterprises and public organisations and in this way it hopes to remove some of the impediments that keep public authorities from providing electronic services to citizens. These digital signatures allow for secure electronic identification towards administrations. The concept is commonly referred to as the "public digital signature". Denmark does not offer electronic ID cards but has taken an approach quite different from many other member states. Technically speaking this approach is not different from other eID projects where, e.g., smart cards containing digital certificates are issued to the citizens. However conceptually and legally the difference is that the Danish government doesn't issue electronic identities. It only offers free digital signatures to the citizens and promotes them as an official means for user authentication in the public sector.
This decision has further been supported and preceeded by other initiatives of the egovernment project. In 2002 the government declared that scince the 1st of September 2003, called the first eDay, government authorities have the right to demand that communication with other authorities happens electronically. However this does not include letters or documents with personally identifiable information about citizens. This communication, involving sensitive data, can only occur between authorities that use digital signatures. This restriction was set aside on the 1st of February 2005 which was the second eDay for Denmark. From that day on all the public administrations are able to use digital sigantures and secure e-mail. As a result all citizens have to right to communicate electronically and in a secure way with government bodies.
Soon after the government started issueing digital signature it was decided in November 2003 to provide the citizens digital access to their personal data and cases as part of the modernization of the administration. The goal of this decision was to increase the openness and transparency of the administration, to induce further cost savings and to propagate the use of digital signatures.
Information on the digital signatures issued by the Danish government is available on http://www.digitalsignatur.dk/ . (Danish only)

B Technology

The Ministry of Science, Innovation and Technology has signed a contract with Tele-Danmark Communications (TDC), the largest telecommunication company in Denmark.
The digital signatures are software based and can be used by citizens from their home computer. The citizen reveives a digital certificate and some software that can be used to create a digital signature.
The signatures are based on X.509 digital certificates and the signatures are created with the RSA signature algorithm and the MD5 or SHA-1 hashing algorithm.

C Applications

- The first application that could be used in combination with the digital signatures were the

online tax services of the Customs and Tax Administration (ToldSkat). Citizen could choose to use a PIN or a digital signature to submit their tax declaration online.
- Functionality for encryption is also available.
- One of the first application where public and private partners cooperate, was the agreement concluded in 2004 between TDC and SkandiaBanken, a Danish bank, who decided to use digital signatures in their banking transactions. The Customs and Tax Adminstration took part in this agreement.
- TDC stated in June 2005 on its website that "At the moment, the signature gives access to 88 services on the Internet and 382 organizations have already introduced solutions where the signature provides improved security when using email."

1.3.5.2 Existing issues

- Scince April 2006 some public services are only available by electronic means thus citizens are obliged to use them online. Millions of transactions, including financial transactions, that were paper based in the past will now be executed electronically. However there is a risk that a small part of the population will be excluded. It is expected that this decision will result in huge savings in the public sector.
- One of the goals was to allow all vendors to become certified certification authorities that issue digital signatures. It is not known whether there are any other companies than TDC that offer these services.

1.3.5.3 Analysis: successes, failures and lessons learned

- Denmark is one of the smaller member states, five million inhabitants, and therefore a complete roll-out is easier to achieve.
- The Danish government focusses heavily on digital signatures. These have to be linked to the signatory and in this way might provide, in some sense, an electronic identity.
- One of the major advantages is that the use of software based solutions does not impose any additional costs for the citizens as opposed to electronic ID cards which may also be perceived as intrusive. As more authorities are using digital signatures this may result in more electronic communication, less paperwork and thus again cost savings.
- It is not clear why the Danish government has decided not to issue or create electronic identities for its citizens. The steps that were taken to issue the digital signatures are very similar to the eID initiatives in other member states, for example, a nation-wide public key infrastructure has been set up.
- It is not known whether there are initiatives to promote interoperability with electronic signatures from other member states.
- From this initiative we learn that it is not easy to provide an infrastructure first and to ensure at the same time that it will have successful applications. One could try to think of applications before setting up the infrastructure but it is commonly believed that it works better the other way round.

1.3.5.4 Expected future developments

No plans have been mentioned to work on an electronic equivalent of identity cards and it is not clear if there are going to be any further developments on the public digital signature.

1.3.5.5 References

http://e.gov.dk/english/egovernment/index.html
http://www.digitalsignatur.dk/
http://danmark.dk/

1.3.6 Estonia

1.3.6.1 General status and most significant systems

The Estonian system is eID card based like in many other Member States, including Belgium and Finland. Estonia issues eID cards to all its residents, including Estonian citizens and aliens residing within the country.

The eID is a multifunctional card: it is a regular identity document, it functions as an electronic identity and it can be used to generate digital signatures.

A History, Scope and Goals

In 1997 the first steps were taken to develop an electronic ID card. In 2000 the digital signature act has been approved by the parliament. This act regulates the work of Certification Service Providers (CSPs) which have to be in the National Certificate Service Provider Registry. Identity documents in Estonia are regulated by the Documents Act.
The ID card is mandatory for Estonian residents. Alien residents living in Estonia with a resident permit valid for at least one year must possess an Estonian ID card. Visual verification of the identity of the citizen happens when the user applies for the card. The first cards have been issued in January 2002.
The authentication certificate contains an e-mail address of the form Forname.Surname@eesti.ee. This not a real e-mail account but merely a forwarding service offered by the government.

B Technology

The eID card contains a personal data file and two X.509 certificates, one for authentication and one for signing. Associated with the certificates are two private keys which are protected by two different PIN codes. The certificates are suspended if the card is lost and verifiers should query the certificate database. Estonian laws require certificate suspension. Services available for certificate validation are Certificate Revocation Lists (CRLs), an LDAP repository and an OCSP responder.
The present card is fabricated by a Swiss company and is like most common electronic ID cards. It is a pocket size card with a chip, it has several protection features like a hologram and digital certificates are on the chip. The Estonian eID roll-out is know to be one of the most successful in Europe.

C Applications

There are already many applications for the Estonian eID card. Estonian citizens can use it to buy e-tickets for public transport. It can be used for drivers permit verification. Citizen can use it to read their information in the population register. It can be used to digitally sign documents or to check one's telephone bill. The card can also be used for health insurance and banking purposes.
The main purpose of the card is to authenticate its owner. Authorisation is done externally. One application where the card is used for authentication is the e-Citizen portal. Unfortunately the portal allows the citizen to choose the authentication mechanism and as internet banking started in 1995, citizens tend to login to their bank and then go to the portal. Many people (65%) declared their tax online but not through the eID card. They did it with bank codes, so authentication is not the killer application. Also the card can be used for secure e-mail. The idea was to give a lifetime e-mail address to the citizens so the authentication certificate contains an e-mail address.
The creation of digital signatures is another feature supported by the eID card. In Estonia the public sector is legally obliged to accept digitally signed documents. There is a notion of free flowing digitally signed documents and the quantity of applications is innumerable. To support digital signatures and documents a uniform platform called DigiDoc has been developed. It is based on the Technical Specification TS 101 903 from ETSI also called XAdES. It allows long-term validation of documents.
A final application worth mentioning is Internet voting. As the infrastructure was in place, it was desired to use it. The eID card was the enabling tool. I-voting was based on an envelope scheme. The citizen makes a choice and the choice is then encrypted with the public key of the whole system. Many international observers were present when it happened in 2005.

1.3.6.2 Existing issues

Like in many cases the take-up of egovernment service applications based on the eID card was very slow.
There are some privacy concerns about the i-voting and the buying of public transport ticket with the eID card. The transport company knows the identity of the person who bought the ticket. The success of these applications is highly dependant on the trust users have in the system. Of course one can always travel anonymously by buying a paper ticket.

The e-mail address provided by the government looks like the perfect communication channel. However it works voluntarily, the citizen has to login to the citizen portal and register the address. Not everyone does this.

1.3.6.3 Analysis: successes, failures and lessons learned

The conclusion of the Estonian eID initiative is that people misinterpret the I in PKI, public key infrastructure. The infrastructure doesn't provide for anything but it is the use of the infrastructure that does something. It is like investing in roads. Developing the application first and then deliver the cards is wrong. One has to provide the infrastructure first and then the applications.
Estonia has a PKI penetration of more than 67%. The reason for its major success is that Estonia is a small country. It only has 1.35 million citizens and citizens younger then 15 years do not need an ID card. Today more than 900 000 cards have been issued so almost everyone has one. Although the ID card project is a success it took 5 years instead of the originally expected 14 months due to legislative and political issues. Another challenge was to promote the use of the card and to make people getting used to it.
From this we learn that one should not underestimate the efforts needed to setup the infrastructure for such an initiative. Also we see that it is possible to change the eID card to a multiapplication card (public transport tickets). Technically this is not a big problem, this is more of a legal challenge.

1.3.6.4 Expected future developments

It is expected that further work will be done to integrate the digidoc system in the public sector.

1.3.6.5 References

http://www.id.ee/
http://www.id.ee/file.php?id=122
http://www.cybertrust.com/media/case_studies/cybertrust_cs_easton.pdf

1.3.7 Finland

1.3.7.1 General status and most significant systems

The Finnish system is based on the concept of a Citizen Certificate serving as the citizen's electronic identity, which can also be used for encryption or signing purposes. The Citizen Certificate contains the first and last name of the citizen, and a unique electronic user ID. This is a unique identifier, different from the personal identification number which was issued at birth, that doesn't reveal any information about the citizen (like his gender or date of birth). The electronic user ID is called an electronic client identifier (SATU). It consists of a series of numbers and a check digit, and never changes.
An electronic client identifier is created automatically in the Population Information System for every Finnish citizen and for aliens residing permanently in Finland. The Citizen Certificate can be used as a means for strong authentication, for the creation of a legally binding electronic signature and for the encryption of e-mails and documents. The service responsible for the citizen certificate and the eID card is the Finnish Population Register Centre (PRC or VRK - http://www.vaestorekisterikeskus.fi). The Population Register Centre develops and maintains the Population Information System, certificate services, the guardianship register and the Public Sector Directory Service, and provides assistance for organising elections.

A History, Scope and Goals

B The Introduction of an electronic identity

The electronic identity started with the rollout of the first electronic ID cards in December 1999 together with the setup of the necessary infrastructures. Soon a number of e-ID card enables services were created. In April 2002 the citizen portal http://suomi.fi was launched grouping all kinds of public services available to Finnish citizens. Since 2004 the eID can be used to access municipal services.

In May 2003 Finland entered into a cooperation agreement with Estonia for the purpose of cross-certification promoting international interoperability (OpenXAdES project - http://www.openxades.org). The eID card is multifunctional document that can serve as a valid travel document in the EU, Norway, Switzerland and San Marino, and that be used for social security services. The card is issued by the police.
By the end of 2005 Citizen Certificates have been issued to 96,100 people.

C Mobile citizen identification

Because of a slow uptake of the eID card, the Population Register Centre launched a mobile electronic identification scheme. A Citizen certificate is then included in the SIM card of a mobile device, allowing the citizens to identify themselves through their mobile phone or via a computer. In addition a Citizen Ceritificate can also be attached to certain bank cards. So a citizen can have multiple valid Citizen Certificates at the same time.

D Making eGovernment Services more attractive

In an attempt to promote the eID card, it has been decided that since June 2004 Finnish citizens can choose whether they want their health insurance data to be on the eID card or not. If so then the citizen no longer needs a health insurance card.
Furthermore the government has initiated a new online identification system in April 2004 to make eGovernment services more accessible. Citizens can now use identification codes received from Finnish banks. Because of the slow uptake of the eID card, which was supposed to be a universal authentication mechanism, the government decided that the identification system used for Internet banking is reliable enough for certain services.

E Technology

The eID card is a typical smart card containing personal information about the citizen and its citizen certificate. Optionally it also includes health insurance data. Before being able to use the card for identification or for the creation of an electronic signature it has to be unlocked with a PIN code. There are two PIN codes, namely one for authentication and one for signing.
The Finnish Citizen Certificate is actually a set of two certificates, one for authentication and encryption and one for creating an electronic signature. The latter is a qualified certificate. The certificates are issued by the PRC being the only Certification Service Provider in Finland at this moment.
Mobile Identification is supported as the Citizen Certificate might be included in the SIM card of a mobile phone. There is also an Online Identification System using existing identification codes from Finnish banks.

F Applications

G Change of Address Service

One of the most recent applications is the address change notification online service, a service offered by the Finnish post in cooperation ith the Population Register Centre that allows a citizen to submit a single address change notification online, without having to inform several institutions or organisations one by one. Citizens have to confirm their identity by using a Finland Post username, Finnish Internet Bank access codes or the Population Register Centre ID card with a chip!
"The new address will be automatically relayed from the population information system to several authorities, including congregations, the vehicle administration, the Social Insurance Institution, the tax administration and the Finnish Defence Forces. In addition, many pension institutions, banks, insurance companies, organisations, publishing houses and other companies receive information about new addresses directly from the population information system."
source:
http://www.vaestorekisterikeskus.fi/vrk/home.nsf/maindocuments/a092a36e225eadfec2256c93003bae20?opendocument

H Electronic Birth Registration

All births are recorded electronically by the maternity hospitals so the child gets an identity code in less than a day. This improves the child's data handling in the hospitals and other issues.
source: http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=44510

I Online Crime Reporting

In March 2003 an online crime reporting service was launched. Citizens can report minor property offences and damages to the police via the internet portal. The services is not very interactive (yet), it is basically a form downloading service. The compiled forms still have to be delivered personally to a police department.

J Nordisk eTax

Nordisk eTax is a portal for citizens from the nordic countries, i.e. Finland, Sweden, Norway, Denmark and Iceland, that have incomes or assests in an other nordic country then the country where they reside. The portal provides information about tax obligations for private individuals.

K Non-disclosure of personal information

"Everyone has a right to forbid the disclosure of his or her personal information by the population registration system for purposes such as direct advertising, direct marketing, distance sales, market surveys, opinion polls, disclosure of address, genealogical research or membership rolls. Such disclosure can be forbidden by phone, by completing a special form or via an informal letter addressed to Local Register Office or to Population Register Centre. The disclosure can also be forbidden with the help of a chip ID card at Population Register Centre´s "Check Your Registered Data!" service."
source:
http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/7510ED645BBF937AC2256CCB00232C4D

1.3.7.2 Existing issues

A Divergent ID-verification systems in municipal authentication systems

"Helsinki, 15 December, 2005 — In Finland, Fujitsu Services has been selected as the supplier of an electronic authentication system for the Finnish public administration. The system will provide people with a web authentication and payment system, which will be the first nation-wide shared service initiative involving the state and municipalities in Finland. The service will enable integrated authentication and web payments in all government electronic access services in the system. Authentication can take place by using web banking ID, the resident authentication card of the Population Register Centre, or user ID. The first authentication services in the municipal sector will be launched in the first half of 2006."
source: http://www.e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=45214

B Access to the Internet – A Matter of Equality

http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=38402

C No Backup for Encryption Keys

Although the eID card has encryption features (the authentication certficate is said to be also an encryption certificate) there seams to be no support for backup of the encryption keys. The private keys of the cardholder are inside the chip of the card and cannot be extracted from it. Also if the eID card expires the cardholder receives new encryption keys which implies that he or she has to reencrypt his data with the new keys.

1.3.7.3 Analysis: successes, failures and lessons learned

1.3.7.4 Expected future developments

Electronic voting will be tested in 2007 for the Parliamentary elections in three cities and should be available in the whole of Finland in 2009.
source: http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=46243
http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=43175

1.3.7.5 References

A Population Register Centre

Information about electronic identity is contained on three different web sites of the Population Register Centre. The main site, http://www.vaestorekisterikeskus.fi , discusses the topic on a general level. The FINEID.FI site, http://www.fineid.fi, concentrates on the technical perspective, and the etu-club site, http://www.etu-klubi.fi, addresses the holders of electronic ID cards.

B Citizen portal

Suomi.fi, http://suomi.fi , is the portal for public sector services in Finland.

1.3.8 France

1.3.8.1 General status and most significant systems

The Agency for the Development of Electronic Administration (ADAE) plays a central role in French ICT policy and eGovernment organisation. This agency has a leading position in any eGovernment related initiative.
From an IDM perspective, France has traditionally relied on a (paper) ID card, which is issued to all citizens and the detention of which is mandatory. A number of initiatives have been introduced in recent years to modernise these cards.

- the electronic health insurance ID card, Vitale, was introduced as early as 1998. The card is currently being revised for modernisation, and the new updated cards will be rolled out in 2006, in parallel with the eID card.
- so-called Daily Life Cards (Carte de la Vie Quotidienne) were introduced in 2003. It concerns an entire category of cards whose common elements are that they are locally delivered and intended solely for the identification and authentication of users for services within the applicable region (which can conceivably span departments or be limited to a specific municipality).
- plans for an eID card by the name of CNIE (Carte Nationale d'Identité Electronique) were first announced in 2003, as a part of the INES programme (Identification Nationale Electronique Sécurisée). The roll-out phase is expected in to begin in 2006, although the card is somewhat controversial for its use of biometric characteristics, incorporating a digital picture and fingerprint scans.

A History, Scope and Goals

France has a long history in ICT related legislation, including through the establishment in 1978 of the national data protection commission, CNIL (Commission Nationale de l'informatique et des Libertés; http://www.cnil.fr), the introduction and widespread use of the Minitel network in 1984 (http://www.minitel.com/), and the creation in 2003 of the Agency for the Development of Electronic Administration (ADAE, http://www.adae.gouv.fr/), which functions as a general coordinator of national ICT policy and the development of eGovernment services. ADAE functions under the authority of the Prime Minister.
The 'Vitale' electronic health insurance card was introduced in 1998, and is currently being redesigned to reinforce the security of health insurance operations and reduce fraud. The next-generation cards will include a photograph of the holder in order to fight fraudulent use. The current version is used approximately 200.000 times per day by health care professionals (source: http://www.adae.gouv.fr/rubrique.php3?id_rubrique=76).
The smart card is distributed to all persons registered with the social security and entitled to health insurance. Its chip contains only administrative and entitlement information about the holder and the insured person. Together with the electronic card for health professionals, it

enables reimbursement claims to be transmitted electronically between health professionals and social security institutions over a secure closed network.
In 2000, the e-government service portal Service-Public.fr was launched, providing a single and convenient access point to public services online. A second portal that focuses more on localised services, http://www.servicepubliclocal.net/, was established in 2002.
In that same year the French government also published the first version of the French e-government interoperability framework (Cadre Commun d'Interoperabilité, http://www.adae.gouv.fr/rubrique.php3?id_rubrique=41). This framework examines the need for increased interoperability between information systems across the public sector and makes a number of recommendations in order to reach this goal. The framework was last updated in September 2003.
The "Daily Life Card" project was launched in 2003. Daily Life Cards are smart cards which are locally delivered and administered. Their scope is linked to the provision of services within a specific region only, and thus also to a limited service set. Their main advantage is the high degree of flexibility, allowing public administrations to provide the exact services which are locally required. The cards can be used for identification, authentication and even payment of services to a variety of public services, regardless of the actual service provider (local authorities, central government, or private companies delivering public services). Pilot projects are currently underway, supported by ADAE.
In 2004, the French government launched the ADELE e-government strategic plan and action plan. Spanning the period between 2004-2007, it provides a detailed framework for future e-government developments. It's main goals are:

- to simplify administrative procedures in order to make life easier for citizens, businesses and local authorities;
- to guarantee data security and confidentiality through the use of secure user identification systems and the possibility for citizens to control the use of their personal data by public bodies; and
- to contribute to the modernisation of public administration.

Finally, plans for an eID card by the name of CNIE (Carte Nationale d'Identité Electronique) were first announced in 2003 by the French Ministry of the Interior, as a part of the INES programme (Identification Nationale Electronique Sécurisée). The INES programme aims to:

- Harmonise and simplify the procedures for requesting passports and national ID cards, and to improve the security of these procedures;
- Improve the management of these documents using new applications;
- Deliver highly secure documents in compliance with international demands;
- Offer citizens the means to prove their identity through the internet and to sign documents electronically, in order to encourage the development of electronic administration.

The roll-out phase of the CNIE is expected in to begin in 2006, although the card is somewhat controversial for its use of biometric characteristics, incorporating a digital picture and fingerprint scans. The public debate regarding the introduction of the CNIE was kicked off in 2004 through the Internet Forum (http://www.foruminternet.org/carte_identite/), resulting in a critical report requesting that the scheme would be revised in order to address privacy and security issues.

B Technology

The next-generation Vitale cards, to be introduced in 2006, will include a photograph of the holder in order to fight fraudulent use. They will have a built-in crypto-processor featuring cryptographic mechanisms based on public keys, which will considerably reinforce the security of operations such as electronic authentication and signatures. The chip will have a capacity of 32 KB - eight times more than the 4 KB memory of the current cards - which will allow for storing a greater quantity of information. The cards will comply with the new IAS (Identification, Authentication and Signature) standards, thereby meeting the new requirements of the health and welfare field.
There are currently no plans to merge Vitale and the planned eID card, CNIE.
The CNIE, also to be introduced in 2006, will not be visually very different from the current ID card, incorporating mostly the same information: basic card holder identification (name, first name, address, ...), signature, and card number. However, the electronic information is somewhat more extensive.
The digital information stored on the card's chip is subdivided into multiple blocks, which use different encryption methods. Currently, the following blocks are planned:

- an Identity Block: the same card holder's information as above, with the noteworthy addition of a digital photo and two digital fingerprints. Due to its sensitive nature, this data will be most strongly encrypted, and only accessible to authorised officials.
- an Authentication Block, which only contains an anonymous card authentication mechanism. This will allow officials to check the authenticity of the card, without necessarily processing personal data.
- a Certified Identification Block, which allows the holder to identify him/herself using a PIN-code. This could conceivably allow access to any number of applications, including e.g. electronic banking services.
- an eSignature Block, allowing the user to sign documents electronically
- a Personal Portfolio Block, allowing the user to store any information that he/she would like to carry around and be able to re-use in other systems.

Accessing data in the Identity Block can be done without contact (although it does require certain data printed on the card), whereas other information requires the use of a reader.

C Applications

Information sources:

- http://www.service-public.fr/ (federal portal, in French)
- http://www.sesam-vitale.fr/index.asp (federal portal, in French; only basic information in English)
- http://www.adae.gouv.fr/ (federal portal, in French; only basic information in English)
- http://www.foruminternet.org/carte_identite/ (federal portal, in French; only basic information in English)

1.3.8.2 Existing issues

The French approach raises a few issues, which can be summarised as follows:

- Multiple cards have already been issued, and it remains to be seen if there is an actual need for several ID cards per person, and whether or not the French population will in time embrace this variety.
- Certain specific characteristics of the CNIE (notably contactless accessibility of data and the inclusion of biometrics such as fingerprints
- Certain parties have forwarded the criticism that the INES programme has unduly linked the issues regarding passports and national ID cards. While these documents clearly show some similarity, their different scope, purpose and application would suggest that they are sufficiently different to merit separate treatment. A perception exists that the design of the CNIE has largely and unnecessarily been influenced by requirements imposed on the passport.

1.3.8.3 Analysis: successes, failures and lessons learned

Both the INES and Vitale cards are still in the roll-out phase. However, some preliminary conclusions can already be formulated, summarized as follows:

- The controversy and continued debate surrounding certain key characteristics (most notably the use of biometrics and contactless access technology) of the CNIE suggests that the general population is not yet convinced of the design of this card. Whether this doubt is a result of genuine design flaws or a lack of sufficient knowledge of the technology used is open to debate, but the current status of the debate suggests an insufficient consensus.
- The French government consciously chose to keep the general eID card separated from the Vitale card for data protection reasons, i.e. to avoid health data being included on the eID card. This decision is generally supported as a privacy enhancing policy.
- The introduction of Daily Life Cards allows local administrations to provide the services required by their constituency, and thus closes any possible gap between national administrations and local needs. However, there is also the risk of creating an excess of ID cards and of implementing localised services in an excessively diverse manner, thus confusing card holders.

1.3.8.4 Expected future developments

Both the INES and Vitale cards are still in the roll-out phase, and 2006 is likely to be a breakthrough year for both.

1.3.9 Germany

1.3.9.1 General status and most significant systems

Germany identifies natural and legal persons by different, sector/application specific identifiers, for example :

- Natural Persons: pension insurance number, health insurance number, tax number (as of 2007)
- Legal Persons: ID for the social security system, ID for the tax system (as of 2007)

Public authorities are only allowed to share identifiers if the person has explicitly agreed to do so, on the basis of a special law or under certain circumstances. The tax number of a natural person must not be used by other authorities.
Germany has adopted the European Directive on Electronic Signatures in the year 2001 through the German Electronic Signature Act. In addition to the Electronic Signature Act an ordinance on electronic signatures came into force laying down the minimum standards and requirements for both, the certification authorities and signature creation devices. Electronic signatures in Germany are considered equal to handwritten signatures.

1.3.9.2 Existing issues

In 2001, driven by the German State Printing House (Bundesdruckerei), a pilot-project was initiated to evaluate the possibility of having smart-card based electronic identities within public administrations (German Office Identity Card).
In this pilot, a smart-card has been developed providing the following functionalities:

- creation of electronic signatures according to the German Signature Act (qualified signatures)
- signing/encryption of e-mails
- user-authentication (SSL/TLS client authentication; usable for Kerberos and login to MS-Windows/Domains)
- identification of employees for time recording

The pilot project has been carried out for seven month and ended in May 2002. Beside a final report no concrete further actions were taken. Another mentionable e-ID initiative is the German health card project which should end in an nationwide rollout by 2007. The health card is designed to be the key element of German health applications. It holds personal information of the cardholder and provides cryptographic functionalities. The health card can be optionally equipped with a qualified certificate and thus can be used to create qualified signatures according to the German Signature Act.
The e-health card holds the following personal data (obligatory):

- given name
- last name
- date of birth
- personal identification number of the cardholder
- sex
- country, city and city-code

Storing of further data is possible; on request of the cardholder, a set of emergency data can be stored on the card as well.

1.3.9.3 Analysis: successes, failures and lessons learned

During the 'German Office Identity Card' pilot project a lot of difficulties could be faced. Most of the lessons learned out of this project relate to the design and implementation of smart cards and smart card based applications. It was found, that especially the usability of smart cards should be in the center of interest of a succeeding project. For example, the unification of names of PIN-Codes or the introduction of PUKs (Personal Unlock Keys for unlocking of locked smart card functionalities) are considered to be important.

1.3.9.4 Expected future developments

A Electronic Identity Card

The Ministry for Internal Affairs announced in the year 2004 a new generation of identity cards which also base on smart cards. Similar to the upcoming European passports, also the new generation of ID-cards holds biometric data of the cardholder (two fingerprints and a face image). Optionally the cardholder can activate the function of creating electronic signature by requesting for a qualified certificate. Thus, the conventional ID-card becomes an e-ID to be used in online-transactions as well.
The personal data stored on the card are protected by secret PIN codes. So the cardholder is under to control of her personal information and unattended reading of personal data is prevented. The final specification of the ID-card as well as the information how electronic identities will be managed (by the use of which identifier) is not yet available. From the technical point of view, Germany intends to provide only a wireless interface (RFID) for the new ID-card generation, similar to the new European passports. In the event the signature functionality cannot be realised through the wireless interface a contact-based interface is planned to be provided as well. Following an announcement of the German government from end of 2005, it is planned to rollout the new ID-cards in the year 2007.

B Job Card

The German Job Card is not a real, physical card; Job Card is an application that can be used with any (existing) smart card which is capable of creating qualified electronic signatures according to the German Signature Act. Or more precisely, a Job Card can be requested by using any qualified signature creation device. Through Job Card, administrative tasks in the area of employee-employer-relations and social security applications should be eased. Since fall 2003, the Job Card application has been set-up through a pilot project; it is planned to introduce Job Card nationwide in the year 2006.

C E-Card Strategy

In 2005, the German Federal Government started an initiative called 'E-Card Strategy'. This strategy aims to force a consistent usage of smart cards within e-Government, e-Business and legal relations. It is planned that the resulting common strategic framework is going to supersede or supplement existing smart card applications in Germany, such as the health card, the new ID-card, the Job-Card etc. Therefore, the e-card strategy concentrates on the following issues and requirements:

- smart card functions – such as signature creation, authentication and encryption – of all rolled out smart cards should be interoperable
- all rolled out smart cards have to provide the option to upload/activate/create a qualified certificate and thus should be usable for creating qualified electronic signatures according to the German Signature Act
- all applications of the public administration which require qualified signatures have to accept all smart cards following the requirements provided by the E-Card Strategy
- signature creation devices, smart cards, qualified certificates and the whole public key infrastructure should be provided by private enterprises

1.3.10 Greece

1.3.10.1 General status and most significant systems

In Greece, major identifiers for citizens have been the ID card number and the Fiscal Registration Number. The Ministry of Interior has been leading Syzafxis, a project that aims at the deployment of PKI based identities to designated civil servant, devices etc.
The Ministry of Interior also has plans for a national eGovernment portal that would simplify access to eGovernment services. In 2006 biometric passports started being issued by the Ministry of Public Order. However there are currently no initiatives regarding the deployment of electronic identities.

The European Signature Directive has been adopted through the Greek Presidential Decree 150/2001 on Digital Signatures.

1.3.10.2 Existing Issues

A Conventional Identity Cards

Regarding Identity Cards, identities are managed by municipalities or other relevant prefectures. They are also responsible for issuing conventional identity cards. With respect to identity cards, the following data are stored:

- photograph
- surname and first name
- father's full name
- mother's full name
- date of birth and place of birth
- municipality of registration and corresponding municipal roll serial number
- municipality of registry of males (when applicable)
- status of military service
- blood type
- electoral subdivision

Whereas the use of the following personal attributes has become prohibited by the Greek Data Protection Authority:

- religion (not obligatory but only following request)
- spouse's full name

1.3.10.3 Expected future developments

The Greek government has indicated eGovernment to be a priority. Thus, the introduction of an electronic identity scheme is expected at some point in the near future.

1.3.11 Hungary

1.3.11.1 General status and most significant systems

Hungary's main eID system revolves around the so called Client Gate (http://www.magyarorszag.hu/ugyfelkapu), which is available from the Government Portal (www.magyarorszag.hu). Through this portal, citizens can authenticate themselves using a username/password system, and access a number of common eGovernment services. The credentials for this system are issued by local public authorities, after the identity of a requesting party has been verified based on the central citizen registry.
A PKI system with the same legal value has also been put in place, but is not yet in common use. This system's authentication features could be integrated into the Client Gate in the future.
While no plans for the introduction of an eID card presently exist (despite the fact that a compulsory traditional eID card has been in use for decades), the Hungarian National Health Authority will start issuing eHealth cards in 2007. It is possible that the functionality of this card would be extended at some point to also cover general e-government authentication purposes.

1.3.11.2 History and Background

The Administration Procedure Act, which is the most fundamental element in the legal background of e-government in Hungary, came into force on 1 November 2005. This act states that public authorities must provide their services electronically to citizens/businesses in addition to the traditional paper based form. As a result, electronic service provision in public administration became compulsory since 1 November 2005 in Hungary. However, to ensure continuity of services, public authorities have the possibility to postpone the introduction of electronic service provision throug the legal tools at their disposal for a given period of time.
The act also states that authentication/identification in e-government applications can happen in 2 ways: either by PKI based authentication, or by a username/password system through the so called Client Gate, a portal which is part of the Central System. There is no hierarchy between the username-password and the PKI based authentication systems, which means that they are considered to have the same legal value.

In both cases the identification following the authentication is based on a set of natural identifiers (name, place and date of birth, mother's name) and sectoral identifiers.
When a citizen doesn't hold a valid PKI certificate, he is obliged to use the Client Gate (http://www.magyarorszag.hu/ugyfelkapu) which is available from the Government Portal (www.magyarorszag.hu) and is part of the Central System (the methodology of identification used in the Client Gate is described below, as Case I).
When a citizen/business holds a valid PKI certificate, it can directly address the authority with a digitally signed document. In this case the identification/authentication is PKI based (as described below, as Case II).
The Client Gate (operational from the 1st of April 2005) is a single-sign-on system where authentication at this time is based on username-password. The Client Gate improves the accessibility of public services by providing a single point of access for the citizens. It is worth noting that this role of the Client Gate does not depend on the manner of authentication used when accessing the system, which means that in the future PKI based authentication in the system is also possible.
Providing their services through the Client Gate is equally advantageous for the public authorities, because in this case they don't have to solve all the questions connected to the implementation of a authentication/identification system by themselves (for example registration of the users occurs centrally).
Obtaining username-password to the Client Gate is free of charge and can be done in any of the more than 200 document offices countrywide. Before receiving the username-password a picture ID based identification is carried out on the spot, and a data comparison is made with the records of the central citizen register.
Since PKI usage in Hungary is very low at this time, in practice almost every available e-government service (including services planned to roll out in the close future) is provided through the Client Gate. Thus, it can be said that the Client Gate is the Central Identification Gateway of Hungary.
Since username-password based identification is not sufficiently secure and since mobile phone penetration in Hungary is at more than 90 percent, there is a plan to complement the Client Gate with SMS based OTP (one-time-password), which in practice is almost as secure as PKI based authentication.
The number of registered users of the Client Gate is 350.000 in early October 2006. The increase of the number of registrations is driven by 2 factors: firstly, more and more services are available which increases the system's appeal to citizens. Secondly, businesses have been required to submit certain types of tax declarations electronically through the Client Gate since May 2006. The circle of those obliged to do tax declarations in electronic form through the Client Gate will increase in the future.
There is currently no plan to issue a national eID card, despite the fact that plastic ID cards have been in use in Hungary for many years and that having an ID card has been compulsory for decades. However, the National Health Authority will start issuing eHealth cards in 2007. Since every Hungarian and foreign citizen will hold this card in the future there is a plan to extend the functionality of this card to include general e-government purposes. This project is still in a very early stage, however, and even the basic principles have not been decided yet.

1.3.11.3 Existing issues

A Enforcement of e-Government regulations of the new act on administration processes and services – Case 1: Authentication by password

The user must register before using the central government gateway. During registration the central population register is used to verify the requesting party's identity, and a new entry with the person's e-mail address will be added to the registration database. The person receives a password which must be changed before using any services. To enter the central gateway, the name, surname, e-mail address and password are used. The central gateway passes the control to the authority forwarding only the name, surname, e-mail address and a transition code. The authority performs its own identification procedure, and passes back the personal data with the transition code to the central gateway for authentication purpose.
This identification system bases on identification numbers and includes personal data as well:

- This ID system makes use of identification numbers and personal data.

- Identification numbers base on application specific registers; they are unique within the ID system.
- The identifier used remains the same throughout a persons lifetime, although some personal data may change (e.g. name,…).
- The following personal data are used:
- Name(s)
- Surname(s)
- Place of Birth
- Date of Birth
- Parent names
- This identification system is driven by centralised authorities, municipalities/cities and application specific authorities.
- The basis for the centralised register is the central residents register.
- This ID system is not obligatory; it is limited to e-government (all e-government services).
- This ID system is open to foreigners if they are residents.
- Specific data protection mechanisms are in place: the central (government) gateway forwards only the person's name, surname, e-mail address and a certain transition code to the authority.

B Legal issues:

- Act CXL of 2004 on administration processes lays down specific regulations regarding electronic authentication. Therein are two methods of electronic authentication defined: 1. password, 2. digital certificate. This section describes the e-ID system using the first method (username/password).
- For a constitute proof of identity, the following information is used: name, surname, place of birth, date of birth, mother's name
- A legal framework defining a concept for role management and mandates is not yet in place. However, a Government Decree is in preparation, that will regulate the electronic management of mandates.
- There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).
- The regulative framework provides a multi-tiered identification system. This ID system makes use of username/passwords to authenticate/identify persons. The next section (see 0) describes an analogous system using electronic signatures.

C Technical Issues:

- This ID system base on usernames/passwords; Persons are authenticated by passwords (PIN).
- The user credentials issued are valid for max. 60 months.

D IT-Security Aspects:

- Neither digital signatures nor a public key infrastructure (PKI) is used.

1.3.11.4 Enforcement of e-Government regulations of the new act on administration processes and services – Case 2: Authentication by digital certificate

The person enters the public authority's system using a digital certificate. After identification the authority sends the personal data to the provider of the certificate for authentication purpose. This identification system bases on identification numbers and includes personal data as well:

- This ID system makes use of identification numbers and personal data.
- Identification numbers base on application specific registers; they are unique within the ID system.
- The identifier used remains the same throughout a persons lifetime, although some personal data may change (e.g. name, surname).
- The following personal data are used:
- Name(s)
- Surname(s)
- Place of Birth

- Date of Birth
- Parent names
- This identification system is driven by municipalities/cities and application specific authorities.
- This ID system is not obligatory; it is limited to e-government (all e-government services).
- This ID system is open to foreigners if they are residents.
- Specific data protection mechanisms are in place: during authentication the transfer of personal data is restricted.

A Legal issues:

- Act CXL of 2004 on administration processes lays down specific regulations regarding electronic authentication. Therein are two methods of electronic authentication defined: 1. password, 2. digital certificate. This section describes the e-ID system using the latter method (digital certificate)).
- For a constitute proof of identity, the following information is used: name, surname, place of birth, date of birth, mother's name
- A legal framework defining a concept for role management and mandates is not yet in place. However, a Government Decree is in preparation, that will regulate the electronic management of mandates.
- There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).
- The regulative framework provides a multi-tiered identification system. This ID system makes use of username/passwords to authenticate/identify persons. The previous section describes an analogous system using usernames/password.

B Technical Issues:

- This e-ID system makes use of private sector smartcards – issued by different certification providers.
- The validity of an issued token varies; it depends on the certification provider of the provider.
- Persons are authenticated by using electronic signatures; in consequence by a special authentication procedure between of the authority and the certification provider

The following interoperability initiatives have been considered:

- EESSI standards

C IT-Security Aspects:

- A public key infrastructure (PKI) is used.
- Certificates can be issued by any – governmental or private sector – certification authorities (CAs).
- Certificates are non-qualified; registration process required; no pseudonyms.
- Certificates do not contain unique identifiers (identification number).

Information kindly provided by M. Zoltán Molnár and M. Zsolt Sikolya

1.3.12 Ireland

1.3.12.1 General status and most significant systems

The Irish Government's electronic identity management structure is currently built around two core concepts: the Personal Public Service Number (PPSN) and the Public Services Broker (PSB). The PPSN is a unique identifier which is now mandatorily assigned to every Irish child at birth, as a part of the application for child benefits. Historically, the number replaces the Revenue and Social Insurance (RSI) number, which was only used for taxation and social security purposes. This number was converted to the PPSN by the Social Welfare Act of 1998, which also contains the necessary data protection provisions.
As a consequence, any Irishman who previously held an RSI number also has a PPSN number. Thus, most people in Ireland automatically have a PPSN, including any foreigners residing in Ireland and applying for social benefits. Although initially mainly used for taxation and social

security, this number is envisaged to become the foundation of the provision of electronic eGovernment services in Ireland.
The PPSN is also the basis for the so-called Public Service Identity (PSI), introduced by the Social Welfare Act of 2002. The PSI also consists of the surname, forename, date of birth, place of birth, sex, all former surnames (if any), all former surnames (if any) of the mother, address, nationality, date of death in the case of a deceased person, and any other information as may be prescribed by the Minister (for Social & Family Affairs).
The PSB functions as an electronic broker/helper/assistant for any new electronic public service. It provides an interface between beneficiary and public service, both on a technical and organizational level. As such, its mission is to improve service delivery through traditional means (in person and over the phone) as well as through a self-service electronic channel (through the Reachservices portal). The PSB is also responsible for providing identification/authentication services for online public services. The PSB is being developed by Reach (www.reach.ie), a central authorization that was founded by the Irish government in 1999 and that is ultimately responsible for the development of the underlying architecture, including the provision of technical guidelines and standardization work.
Roll-out of services has recently begun, most notably through the automated application and granting of child benefits to newborn children, which has the added benefit of a gradual roll-out to all Irish citizens. Other applications are currently under development.
Thus, the Irish IDM policy is currently centralized. Furthermore, information which is currently stored in decentralized databases will gradually be transferred to a new "Public Services Database", containing the data required for all eGovernment services. This database will be managed by the PSB, and will only be accessible through the services of the PSB, thus easing privacy concerns.

A History, Scope and Goals

As early as 1998, legislation was proposed to introduce the PPSN and to permit the exchange of data between public administrations in compliance with the applicable data protection framework. Following the publication of the governments first Action Plan on implementing the Information Society in Ireland, Reach itself was founded by the Government in 2000 and received a mandate to develop the PSB briefly thereafter.
In 2003, Reach developed the so-called Inter-Agency Messaging Service (IAMS) to permit the exchange of information between public administrations. IAMS is to be integrated into the PSB. By the end of 2003, the first application was rolled out by the name of "eEnabling Life Event Data". The project "aims at creating a national database of all life events - such as births, deaths, and marriages", to be made available at any registrar's office, and automatically allocates a PPSN to any newborn as part of the birth registration process.
The final enaction of the required legal framework wasn't completed until February 2004, mostly because of problems in delineating the exact scope of the project, and because of privacy concerns, including those forwarded by the Irish Data Protection Commissioner (http://www.dataprivacy.ie/).
As outlined above, the initial fields of application are child registration, social benefits and taxation, but the PSB will eventually be the foundation of most eService provision initiatives in Ireland. It will provide a government-wide middleware layer and supporting interoperability infrastructure.
In June 2004 the Irish Government established an expert group to introduce a standard framework for Public Service Cards (PSC), making use of the PPSN. This PSC – which is still under development - could become the central building tool for electronic identification and authentication purposes, as it is intended to identify any individual using a public service. As such, it will bundle the functions of a medical card, social services card, etc..
An enhanced version of the Irish e-government portal reachservices went live in May 2005, making use of the first phase of the Public Services Broker (PSB) system. The deployment of the PSB represents an important milestone for the development of Ireland's e-government infrastructure and the integration and improvement of its electronic service delivery. In this first phase, the PSB includes a single identification and authentication process and a single electronic payment facility. The Personal Public Service (PPS) numbers database is use for authenticating users.
Source: http://www.reach.ie/

B Technology

The Irish system is based on a centralised database, managed through the PSB. It is the Reach agency which develops the applicable technical standards, and requires that any communication passing through the PSB adheres to these standards, such as the IAMS. Whenever possible, the standardization work is based on available ISO standards.
The PSB will offer common services to the customer and to public service agencies. Information will not only be made available through electronic networks, but also through traditional channels such as telephone and even face to face communication.
From an IDM perspective, the PBS' chief responsibility is to allow customers (both citizens and enterprises) to demonstrate their identity in self-service, face-to-face or telephone transactions, including a secure method of filing electronic applications. Frequently used personal data can be stored centrally to improve the efficiency of service provision. However, this will require the user's explicit permission.
Specific technical details are still sketchy at this time. While the Broker is said to function only within a secure privacy framework, this remains to be verified as more details become available.

C Applications

Currently, the most significant rollout is the aforementioned "eEnabling Life Event Data" initiative, which "aims at creating a national database of all life events - such as births, deaths, and marriages". Through the project, a PPSN is automatically assigned to any newborn as part of the birth registration process.
According to current plans, further "services will be grouped around typical episodes or events in the life of a customer or a business. This will provide convenient single access points to commonly required groups of services which currently require visits to several different agencies. Examples of typical events include:

- Birth of a baby
- Entering employment for the first time
- Starting school
- Becoming unemployed
- Moving house
- Starting a business
- Taking on new employees
- Death of a family member

Each episode will have the "intelligence" or capability to suggest the topics or services that may be of most interest or relevance to the customer. The customer will be able to build personal profiles during the transaction to allow the system to suggest or offer the most relevant services. The customer can help this process by supplying additional information to the system or by giving his or her permission to use personal information already stored by the system." (source: http://www.reach.ie/)

1.3.12.2 Existing issues

The analysis of the situation in Ireland shows that electronic authentication is still evolving rapidly, and that this report will likely need to be amended and updated frequently. The ModinisIDMproject intends to further elaborate on the following aspects:

- Privacy issues resulting from the use of unique numbers based on single centralised registers. A privacy framework has been provided by the Social Welfare Act of 1998.
- The PPSN is in principle communicated to the parents after a claim for child benefits is registered. Thus, the PPSN is not uniquely known to the rightful holder.
- Personal data will eventually be stored in a centralised personal data vault. In principle this will be done on a voluntary basis. Despite the voluntary character, this appears to be one of the most far-reaching centralization schemes of the Union. As such, it is worth observing how this will be implemented, and what the reaction of the general public will be.
- The PPSN is not strictly speaking obligatory, as adults only have it if they also had an RSI (tax and social security) number. The impact of this element on the roll-out of public services remains to be seen, although it will obviously not be possible to exclusively offer services through the PPSN.

- The system is limited to e-government: Citizen-to-Government domain (C2G) and Business-to-Government domain (B2G). C2C and C2B relationships are entirely unaffected.
- The roll-of a Public Service Card (PSC) using the PPSN is also planned, which will bundle the functions of a medical card, social services card, etc. The implementation of this card is not yet entirely fixed, and public acceptance remains to be seen.

1.3.12.3 Analysis: successes, failures and lessons learned

The following elements stand out as lessons to be learned from the deployment of the Irish e-ID solutions thus far:

- The PPSN system is open to foreigners who reside in Ireland and apply for social benefits, which excludes certain categories of foreigners (such as (some) expats, tourists, most types of refugees)
- The PPSN is obligatory, although roll-out is gradual by only forcing the issuance to newborns which are being registered for child benefits. This immediately creates a positive link between the identification system and the user, by pointing out a clear example of a benefit. Child benefits seem like a good starting point for the deployment of any eGovernment identity management system.
- Similarly, the project also revealed that is impossible to unilaterally impose a standard without first ensuring that there is a conviction in the field that the new system will work and be an improvement for customers and people in the field alike.
- The legal and organisational framework was a long time in the making. This was mainly caused by tight programme management principles: first delineate the scope in detail; then ensure that there is an appropriate legal framework. "Patchwork solutions" tend to cause discomfort and disputes about the legitimacy of the entire system, and can threaten an entire project.
- Applicable standards are centrally developed and imposed through the PSB. Whenever possible standards adhere closely to available ISO standards, which could facilitate interoperability projects.
- However, one of the reasons that this system could be raised with relative ease and with relative lack of opposition is that (by international standards) it is not technically or organisationally complex. Thus far, it mainly consists of connecting existing databases which were already largely centralised. The solution adopted may not apply easily to decentralised and divergent systems.
- Usage of the PPSN is strictly limited to legally mandated public organisations and persons (see the 'Personal Public Service Number - Code of Practice' - Appendix 2). Thus, expansion of its use to the private sector is excluded in principle.

1.3.12.4 Expected future developments

As indicated above, the PPSN will likely be integrated into the Public Service Card. It remains to be investigated:

- How this will be implemented, and how the public at large will react to this;
- In general: how the public will respond to the concept of a centralized data vault;
- Which services will be added to the existing framework.

1.3.13 Italy

1.3.13.1 General status and most significant systems

The Italian Electronic Identity Card ("Carta d'identitá elettronica" - CIE) is a hybrid card that covers two functions. It will replace the traditional identity card, and will also be an instrument for authentication and identification in e-Government processes. The Italian eID is not solely intended for e-Government environments, but can also be used as a health insurance card, fidelity card or fiscal document.
To accelerate the distribution of an instrument for online identification, the CNS ("Carta Nazionale dei Servizi") initiative has been started by the CNIPA ("National IT Center for the Public Administration"), as the rollout of the CIE for each citizen will last several years. The CNS has the same smart card characteristics as the CIE, but allows issuing to all persons living in Italy. The

CNS will be issued to citizens in certain pilot regions and is expected to be operational by the end of the year 2006.

A History, Scope and Goals

The history of the CIE goes back to 1998, where l'AIPA (the former CNIPA) conducted a survey for potential technologies of the CIE. The Ministry of the Interior went for a smart card with an optical strip.
On 19th of July 2000 the Ministerial Decree No. 116 took the initiative for the CIE by defining its technical and security requirements. The stage for the technical and security framework for a first test phase has been set and within the scope of this phase, CIEs should be rolled out to 100.000 citizens in 83 municipalities.
In November 2000 the first test phase was started to evaluate critical points of the project. More precisely, the implementation of the IT structure and the card emission process were evaluated. In March 2001 the first CIE was issued during the "IT Global Forum" in Naples.
In June 2003 the first test phase ended and in November 2003 the second and consolidation phase started. The goal was to gain experience with the rollout of many (about 2.000.000) CIEs. The number of total participating municipalities decreased to 56 and the CIE was issued to all people older than 15 years.
The third and final phase was started in 2005 and has the goal to rollout CIEs to all Italian citizens older than 15 years. In the next 5 years (2005-2009) all 40 million paper based identity cards will be replaced by the Electronic Identity Card.
The CIE fulfils three main tasks. It will replace the paper based identity card for a simplification in traditional governmental processes. Moreover, it will be an international travelling document according to ICAO and ISO. Last but not least it enables the use of e-Government applications. In order to identify a physical person, a fingerprint template is stored on the chip as well. According to the Italian law, the templates are not stored in a central database. As the smart card allows the storage of additional data, the CIE can be used in other sectors (even private sectors) as well. For instance, the blood type can optionally be stored on the card.
In order to meet the juridical, administrative and technical requirements, the following organisational structures and technical components have been introduced:

- CNSD (National Center of Demographic Services): this organisation is a sub-organisation of the Ministry of the Interior and provides several services that allow the identification of registered citizens.

The main CNSD services are:

- INA (National Index of Registry Offices): this service is a national registry referring to the personal data of all registered citizens. Public authorities can query, validate and update such data. For each entry the INA holds a pointer to the local authority of the citizen in case more detailed information is needed. The INA can be used by all interested authorities for querying and validating a citizen's personal data. The INA is also used in the issuing process of the CIE for validating the citizen's personal data.

The registry must be kept up-to-date. All municipalities are therefore responsible for updating the INA by communicating a change of residence, immigrations, emigrations, births and deaths.

- SAIA (Access and Interconnection System for Identification Data): a network system, that can be used by municipalities to interchange and communicate a citizen's personal data.
- AIRE (Registry Office for Italians living abroad): it is the pendant to the INA and holds the data of Italians living abroad.
- Civil state: a registry holding the civil status of all Italians
- Secure Information Structure: the "Backbone" is a network that enables a secure and certified communication structure between Public Authorities. Municipalities can transparently access the CNSD services in a secure way without having to care about security issues. The organizational and technical autonomy of the municipalities remains untouched by accessing the network using so called Trusted Anchor Point.
- SSCE (Emission Circuit Security System): this IT structure is used for the rollout of the CIE and primarily act as Public Key Infrastructure. It handles the data exchange and validation of personal data for card emissions as well as the revocation checking of CIE certificates in governmental processes.

The Italian Electronic Identity Card (CIE) can only be issued to Italians living in Italy. To enable the use of e-Government services for other people, the PSE ("Permission for Electronic

Accommodation") initiative has been started. The PSE is a hybrid card, has similar characteristics of the CIE and is compatible in regard to the used microprocessor (smart card). The legal basis for the PSE was established by the decree of 03/08/2004 defining the organisational and technical framework. At the moment the PSE project is in a first experimental phase and after finalization it will be issued to non-Italians (EU citizens as well as non-EU citizens).
The experimental phase for the CIE for Italians living abroad is in progress and can already be used for some services in the application range of e-Voting.

B Technology

The key technology of the CIE is a smart card with a cryptographic coprocessor capable of at least the RSA algorithm with a minimal key length of 1024 bit. The smart card has a memory that varies between 2 and 32 kB but can be extended to 64 kB. The file system of the smart card is well specified and contains in addition to the card id and certificate file some dedicated files for national or of local e-Government services.
The certificate on the smart card is issued by the SSCE and has a validity of 5 years in order to comply with the validity period of a paper based identity card. All certificates (X.509 v3) are issued by the SSCE, which implements the PKI infrastructure and acts as both Registration and Certification Authority.
The IDM approach is based on the unique national identifier (the "Codice Fiscale" – Fiscal Code) embedded within the certificate as part of the commonName attribute. The Codice Fiscale is a unique string assigned to each Italian after birth. Each CIE has a unique card id assigned by the IPZS. In addition to the Codice Fiscale the card id and a hash value over the citizen's personal data are also part of the commonName. By means of this two attributes the citizen can be identified securely in e-Government services using the SSLv3 protocol. The citizen authenticates himself by entering the PIN code of the smart card. The identification is done using the Codice Fiscale and querying the INA for personal data or by checking the hash value of the citizen's personal data.
E-Government services based on the CIE can be distinguished in several categories:

- Standard services do not need to modify or update data stored on the CIE.
- Qualified services can modify or update data stored on the CIE.
- Local services are provided and hosted by municipalities. If a local service is qualified, the municipality must define a dedicated file structure.
- National services are provided by the Public Administration. If a national service is qualified, a predefined file structure by the SSCE must be used.

C Applications

The national portal http://www.italia.gov.it enables the citizen to contact and access services of national and local authorities.
The portal http://www.impresa.gov.it is an initiative trying to bring companies and the Public Administration together.
Several applications on the national and local level can be used:

- Age verification for the use of cigarette machines
- Identification of citizens in electoral districts
- Reports of offences to the police (civil and penal)
- Several public charges
- Pre-booking for ward rounds
- Notification of residence change

1.3.13.2 Existing issues

The analysis of the situation in Italy resulted in a clear view on the technological aspects. The ModinisIDM project intends to further elaborate on the following aspects:

- International interoperability: The card relies on accepted standards (e.g. X.509 certificates or ISO 7816-3, -4, -5, -8, -9). Still technological deviations might exist and it is to be seen how the relation to standards such as developed by EESSI, Smartcard Charter TB1 or alike is.
- Integration of foreign eIDs into the Italian system. E.g. can usage of Codici Fiscale and INA queries be complemented by foreign eID systems or is PSE the preferred way.
- Keeping INA as a core part of the Italian IDM system up to date

- Overview of further services, such as sectoral services (health, etc.)

1.3.13.3 Analysis: successes, failures and lessons learned

ANCI has collected experiences and has developed recommendations for the communes. In the first project phases the following problems have been encountered:

- Connectivity to SSCE
- Lack of documentation
- Personnel in communes is not sufficiently trained, causing problems with the use of the technology.

1.3.13.4 Expected future developments

Interviews to get an overview of planned services still to be done.

1.3.14 Latvia

1.3.14.1 General status and most significant systems

The Latvian government planned to start issuing electronic ID cards in May 2004, like its neighbours Estonia and Lituania already do. The project has been suspended in October 2004 and restarted by the new government later that year. Scince then no cards have been issued yet. An infrastructure for electronic signatures is not yet in place. However the necessary legislation has passed.

A History, Scope and Goals

"In October 2004 the previous Latvian government decided to put on hold its electronic identity card project until precise EU requirements for travel and identification documents are known. The new Latvia government, installed in December 2004, decided earlier this year to re-start work on identification cards. A group comprising the Secretariat, the Ministries of Interior, Justice, Transport and Finance, is in charge of working out a strategy for the future support of electronic signatures." (source: http://europa.eu.int/idabc/en/document/4218/589)
"Legislation defining the legal status and conditions of use of electronic signatures (Electronic Documents Law) was passed by the Latvian Parliament in October 2002 and came into force on 1 January 2003. However, the development of electronic signatures has until now been impeded by the fact that no certification service provider has yet been approved. Lattelekom and Latvia Post, as well as the State Information Network Agency (VITA), have stated their intention to become certification service providers, but the Secretariat needed the government delegation to start negotiations." (source: http://europa.eu.int/idabc/en/document/4218/589)

B Technology

The eID card would be a typical pokcet size eID card with information of the owner on the front and a reserved area on the back so that it could be used as a travel document. Plans were made to include biometrical data, like fingerprints, of the citizen on the card.

C Applications

An e-government portal (http://www.eparvalde.lv) provides information to citizens.
In March 2006, the Ministry of Foreign Affairs, Normans Penke, launched a new internet portal (http://www.latviesi.com) for Latvian citizens living or working abroad. The portal contains information about Latvian organisations and communities abroad.

1.3.14.2 Existing issues

No identity cards have been issued although government plans to do so.

1.3.14.3 Expected future developments

It is expected that the necessary infrastructure to support electronic signature will be in place very soon, i.e. by July 2006.

1.3.15 Lithuania

1.3.15.1 General status and most significant systems

Although Lituania planned to develop and electronic ID card, no card has been issued yet. It was intended to serve as identification mechanism containing personal data and information about medical records and social insurance. Apparently the Lithuanian government has focussed more on the elaboration of an egovernment infrastructure in the back-office.

A History, Scope and Goals

"A relatively well-developed legal framework is in place to support the development of e-government, including the Law on Legal Protection of Personal Data (1996) and the Law on Electronic Signature (2000). In April 2002, the Ministry of Economy also approved regulations regarding some information society services, in particular electronic commerce." (src: http://europa.eu.int/idabc/en/document/1436/590)
The electronic signature infrastructure has been used to support the exchange of eletronic documents in the public sector. (http://www.ivpk.lt/en_main-aktual.php?cat=40&gr=1&sub=5&n=13)
In 2003 an electronic gateway to the government on the internet was set up. It serves as a portal to redirect citizens and businesses to the appropriate website of public administrations. (http://www.ivpk.lt/en_main-aktual.php?cat=40&gr=1&sub=5&n=11)
Ministry of Finance launched an electronic tax decleration service in 2004 and it has scince then become increasingly popular. Legal and natural persons can enter their tax related data in an electronic form which automatically validates the data. One of the positive side-effects is that tax overpayments get refunded quicker.
In 2003 a framework for qualified certificates was proposed. (http://www.ivpk.lt/en_main-aktual.php?cat=40&gr=1&sub=5&n=6)

1.3.15.2 Expected future developments

It is expected that in the future the Lithuanian government will refocus on the development of an electronic identity card.

1.3.15.3 References

http://www.ivpk.lt/
http://www.lrv.lt/main_en.php?cat=0

1.3.16 Luxembourg

1.3.16.1 General status and most significant systems

Luxembourg issues an identity card to its citizens, and also issues a unique identifier to both citizens and legal persons established in Luxembourg. However, despite ambitious eGovernment plans, no electronic IDM projects have reached a significant stage thus far.

A History, Scope and Goals

Since the enactment of the Law of 30 March 1979 regarding the numerical identification of natural and legal persons, Luxembourg has issued unique identifiers to its citizens and enterprises established within its borders. Certain core identification data regarding these persons is also stored in centralised registries. Additionally, the citizens of Luxembourg are obliged to carry traditional ID cards. Despite these favorable factors, no electronic IDM solution has yet been deployed.
None the less, the Luxembourg public administration has an ambitious eGovernment strategy in place, consisting mainly of the eLuxembourg Action Plan. A first version of this plan was presented in February 2001, and subsequently updated in June 2005. The strategy emphasises transparency and efficiency in public administration, citizen inclusion and participation, increased competitiveness, and encouraging the development of technical knowledge and know-how in Luxembourg.

While the action plan formulates a number of targets, electronic IDM does not appear to be a key priority at this time. The most notable initiatives include the implementation of an e-health portal in two phases (2005 and 2006), a cultural portal (2006), a sports portal (2006), and a centralised citizen service portal (2006).
Details on the surrounding infrastructural initiatives; such as the "Public Service Framework" initiative, interdepartmental workflow management and identity management projects, are currently scarce.
Details regarding Luxembourg's eGovernance strategies can be found at http://www.eluxembourg.lu/.

B Technology

No IDM technology/system is in common use thus far.

C Applications

No IDM technology/system is in common use thus far. While public administrations do typically offer information on-line, possibilities for on-line interactivity are limited.

1.3.16.2 Existing issues

No IDM technology/system is in common use thus far.

1.3.16.3 Analysis: successes, failures and lessons learned

No IDM technology/system is in common use thus far.

1.3.16.4 Expected future developments

The Luxembourg government is examining identity management possibilities, but details are currently scarce.

1.3.17 Malta

1.3.17.1 General status and most significant systems

Malta issues traditional ID card to its citizens. No public sector e-ID cards exist at this time, although there are plans to roll out an eID card by 2008.
By contrast, the Maltese government does issue electronic identities (e-IDs) in the form of certificates to its citizens, which can be used for a variety of eGovernment services.
The Maltese government also emphasises the development of m-Government services.
For a general overview of Maltese eGovernment policy, see http://www.gov.mt/egovernment.asp?p=106&l=1 and http://www.emalta.gov.mt/

A History, Scope and Goals

The Maltese government has been shaping its eGovernment programme through multi-year strategic plans and white papers, starting from 1998.
The first significant results of these policies were released in 2003, including:

- the online certificate portal, which allows Maltese citizens to electronically order civil status certificates (specifically birth, marriage and death certificates; see http://www.certifikati.gov.mt.
- the deployment of MAGNET, a government-wide Intranet (MAlta Government NETwork). All public officials can use this network to exchange electronic information. This network was partially replaced by MAGNET II in July 2005. MAGNET II mostly increased bandwidth, availability and security. The network also supports VoIP telephony.
- the Maltese government was also one of the first to begin deploying "m-government" or mobile government services. This programme offers access to a limited set of services through mobile phones, networked PDAs or other mobile devices. These services include the reception of: * Notifications via SMS of court deferrals * Notifications via SMS for license-renewal to the holders of licenses * Notification of exams results * Notification for Direct Credit Payments from the Department of Social Security (Source: http://www.miti.gov.mt/site/page.aspx?pageid=344; see also

http://www.mobile.gov.mt/)
- an on-line crime reporting website was also launched in 2003, focussing on smaller crimes and information exchange. Users of the portal receive a reference number and a password that enable them to keep track of their file follow-up. See http://pulizija.gov.mt/

From an IDM perspective, March 2004 saw the most significant advancement, when the Ministry for Investment, Industry and Information Technology (which replaced Malta's Central Information Management Unit (CIMU) in September 2005) launched the Electronic Identity (eID), a programme developed by Microsoft Corporation.
Unlike in many other Member States, the eID is not yet incorporated into an ID card. Rather, it is a simple certificate that Maltese citizens can use to identify and authenticate themselves when accessing certain public services. The eID is not mandatory, and must be requested in person at a District Office of the Department of Social Security with a copy of their paper ID card and a valid e-mail address. The e-mail address is then used to validate the eID request electronically.
(Source: https://gov.mt/portal/(wxducl55ohjuze55vhhpwteh)/randaregister.aspx?l=2)
eID cards are currently being examined, and a Maltese eID card is expected to be rolled out in 2008.
One further eGovernment service of note is the Electronic Payment Gateway (ePG - http://www.gov.mt/egovernment.asp?p=141&l=1), an online public payment platform. Maltese citizens can use the platform to pay their taxes or social contributions through the internet.

B Technology

[to be developed]

C Applications

Additional applications that will make use of the eID's capabilities are continuously under development. Current applications include:

- matters related to Income Tax and falling under the Department of Inland Revenue including electronic Income tax returns, tax reduction forms, corporate tax returns, Employers' Social Security Contributions (http://www.ird.gov.mt)
- The sending of official examination results by the Department of Education to students via mobile telephony as well as online applications for exams (http://www.exams.gov.mt)
- Online submission of VAT returns as well as facilities to view balances for tax periods, registration of VAT numbers through the VAT Department (http://www.vat.gov.mt)
- Online application and renewal of passports (http://www.passaporti.gov.mt)
- Online filing of reports to the Police (http://www.police.gov.mt)
- Online application and renewal of vehicle licences (http://www.licences.gov.mt)
- Online application for building permits issued by the Maltese Environment and Planning Authority (MEPA) (http://www.mepa.org.mt)
- A number of Social Services applications and statements launched by the Ministry for Family and Social Solidarity (http://www.msp.gov.mt)
- Online Registry of Companies launched by MFSA which also caters for electronic incorporation of companies and the electronic filing of company accounts (http://www.mfsa.com.mt)

(Source: https://gov.mt/portal/(0xnrry45gfnfec555kio4tbg)/randahelp.aspx?l=2)
The Maltese government also plans to make the system accessible to trusted third parties in order to ensure an optimal economic benefit.

1.3.17.2 Existing issues

- The Maltese government is currently a proponent of issuing a single electronic identity to each citizen and business alike, and even to extending temporary identities to non-nationals. These identities are managed by private sector parties, which requires extensive and rigid privacy protection mechanisms. It is currently unknown in what manner the necessary safeguards have been implemented.
- Additionally, the issuance of temporary IDs is an interesting workaround for certain difficulties surrounding the provision of cross-border eGovernment services, but it is certainly not a complete solution to this problem. While the Maltese government has never presented temporary identities as a solution to cross-border services, the availability of such identities may actually prove to be a deterrent to the development of real cross-

border interoperability in IDM systems.
- The eID solution was developed by the private sector, and is thus not exclusively under public sector control. This may increase the risks to future use (e.g. regarding openness of standards, expansion of capabilities, licensing issues etc.), depending on the contractual framework agreed upon.

1.3.17.3 Analysis: successes, failures and lessons learned

- The Maltese eID scheme is intrinsically flexible. Plans exist to issue temporary electronic identities to e.g. tourists, in order to access a limited set of public services.
- The Maltese government is also one of the most vocal supporters of m-government. As a result, the Maltese situation could potentially provide a test case for the uptake of and public demand for such eGovernment services.
- This intrinsic flexibility could also potentially facilitate the implementation of cross-border functionality.
- The Maltese governemnt has shown itself to be a proponent of public-private partnerships, not only through the eID programme (developed by Microsoft), but also for the m-Government solutions (offered through partnerships with go Mobile and Vodafone. This could improve a rapid uptake.

1.3.17.4 Expected future developments

The Maltese government announced their ambition of issuing electronic identities to all Maltese nationals and businesses in their latest eGovernment Strategy Plan (see http://www.miti.gov.mt/docs/ITStrategy.pdf). The allocation of temporary identities to non-nationals (e.g. tourists) is also currently being considered.
The existing eID mechanism will be refined in three steps. The first phase will be the provision of a pin code to each citizen for him/her to be able to authenticate himself when requesting e-Government services. The second level will be the widespread distribution of digital certificates to businesses and agents, whilst the third level would consist of smart card integration with the new identity cards being issued by central Government. (Source: http://www.gov.mt/egovernment.asp?p=113&l=1)
In addition, the following m-government services are currently being developed:
- Notification via SMS by the blood bank to advise registered blood donors when urgent needs for blood arise.
- Notification via SMS to parents from their children's school to inform them if their children are absent from school on that day
- Notifications via SMS from the public libraries to individuals who have placed a reservation for a book
- Bus schedule availability via SMS
- Notification of job opportunities from ETC to individuals who have selected specific areas of employment
- Reporting incidents or relevant information to the Police Force

(Source: http://www.gov.mt/egovernment.asp?p=106&l=1)

1.3.18 Poland

1.3.18.1 General status and most significant systems

Poland does not issue any electronic ID card or electronic identities in the form of digital certificates or any similar solution, and it seems like it is not planning to do so in the near future.
A legal framework is in place to support electronic signatures. In September 2001 the Polish Parliament approved the Law on the electronic signature and its regulation was put into practice in August 2002. (http://europa.eu.int/idabc/en/document/1161/408)
An e-government (http://www.egov.pl) portal provides access to public administration information and is intended for citizens and businesses.

1.3.18.2 Expected future developments

"The development of a 'Multifunctional Personal Document' (MPD) that will act as an intelligent, PKI-ready smart card to replace the current plastic ID card is also in the pipeline. However,

legislative changes will need to be made before this can be enacted." (src: http://europa.eu.int/idabc/en/document/984/585)
No further developments have been reported about this.

1.3.19 Portugal

1.3.19.1 General status and most significant systems

In early 2004, a new Citizen's Portal ('Portal do Cidadão', http://www.portaldocidadao.pt/PORTAL/pt) was launched, which replaced the earlier INFOCID Portal. While the name suggests otherwise, the portal provides services to citizens and businesses alike, through separate sections on the website.
From an IDM perspective, April 2005 can be considered a pivotal moment, as the Portuguese government initiated the citizen card project (Cartão do Cidadão - http://www.cartaodocidadao.pt/). The citizen card is envisaged to be a smart card solution covering multiple fields, including general ID, tax, social security, health insurance and electoral information. Distribution of the card is expected to start in 2006.

A History, Scope and Goals

The Portuguese administration's eGovernment initiatives originated mostly around 1996-97. This period saw the launch of the National Initiative for the Information Society (an action programme focusing on improving the use of IT across public services and in eBusiness services), followed by the creation of the Mission for the Information Society (MSI). The MSI drafted a Green Paper on the development of the Information Society, containing a number of eGovernment recommendations.
The first concrete initiative to follow from this is the well known Digital Cities programme (http://www.cidadesdigitais.pt/), which was intended to facilitate the provision of local administrative services to the citizens (specifically on a municipality/regional level). Initiated in 1998, the programme was extended for an additional five years in 2000, and it was subsequently expanded to cover the entire country. It remains operational to date.
Following the Portuguese presidency of the EU in the first half of 2000 and the adoption of the Lisbon Strategy for economic renewal and competitiveness (at the Lisbon European Council of 23-24 March 2000) and the eEurope Action Plan (at the Feira European Council of 19-20 June 2000), the following years saw the creation of:

- INFOCID, an eGovernment portal targeted at Portuguese citizens (2001). Through INFOCID's Direct Public Service application, citizens were able request birth, marriage, death, building and commercial certificates online.
- UMIC, the Innovation and Knowledge Mission Unit (2002), which coordinated the Portuguese government's eGovernment strategies, action plans and initiatives.
- the 2003 Action Plan for the Information Society, including the 2003 e-Government Action Plan.

In early 2004, a new Citizen's Portal ('Portal do Cidadão', http://www.portaldocidadao.pt/PORTAL/pt) was launched, which replaced the aforementioned INFOCID. While the name suggests otherwise, this portal also provides business services, through a separate section on the website. In this period, UMIC was also renamed to Knowledge Society Agency (http://www.infosociety.gov.pt/), becoming a permanent Government agency.
From an IDM perspective, April 2005 can be considered a pivotal moment, as the Portuguese government initiated the citizen card project (Cartão do Cidadão - http://www.cartaodocidadao.pt/). The citizen card is envisaged to be a smart card solution covering multiple fields, including general ID, tax, social security, health insurance and electoral information. The card will also constitute a travel document.
Distribution of the card is expected to start in 2006.

B Technology

As no eID citizen cards have yet been distributed (distribution is scheduled to commence in late 2006), technical details are presently unknown. Details will be published on http://www.cartaodocidadao.pt/ as soon as available.

Conceptually, the citizen card is a smart card that provides visual identity authentication with increased security and electronic identity authentication with biometrics (photo and finger print), as well as electronic signatures (two certificates: one for authentication, and one for electronic signatures, as with many other European solutions). The development of the Citizen's Card is a part of the Portuguese government's plan to simplify the administration and to modernize the public services.
The card is currently undergoing proof-of-concept testing in the form of the so-called Pegasus project, where a consortium involving a wide range of private sector parties is currently examining the technical characteristics and possible applications of the future card (see http://www.cartaodocidadao.pt/index.php?option=com_content&task=view&id=20&Itemid=31).
The final result will replace five presently existing cards - Identification Document, Tax Payer's Card, Social Security Card, Voter's Card, Health System Card - and will allow multichannel identity authentication (i.e. in physical presence of the bearer, through the Internet, or by telephone (with one-time passwords generated with the card), thus allowing the citizen to identify himself electronically and to use a legally valid electronic signature from a distance, contributing to the deployment of customer-oriented advanced public services. The Citizen's Card project is coordinated by the Coordination Unit for the Administration Modernization (UCMA) which works in strong partnership with the Knowledge Society Agency (UMIC) for operational matters.

C Applications

The Citizen's Portal (http://www.portaldocidadao.pt/) is the central digital channel for public services. Launched in the first quarter of 2004, The Citizen's Portal now offers more than 800 citizen-oriented 24/7 services (about 1/2 informational, 1/4 interactive, 1/6 transactional), provided by 125 public administration bodies.
More than half a million users access it on a regular basis, with 3 million page views per month originated from more than 33 countries of all world continents, mainly for such services as information on the public administration, income tax declaration, change of address notifications to public services, and official certifications requests from public bodies (including civil, commercial and land register excerpts).
The development of the Citizen's Portal has been continuous. Besides improvements on the user interface, since February 2005 it offers services supported by sms, and access through wap protocol by mobile phones and PDAs. An electronic payments platform was introduced at the end of 2005 allowing for different forms of payments, including the issuing of payment orders which can be completed through the unified ATM network widely available in Portugal or even without leaving home or office for people who have homebanking, in this case allowing full process dematerialization of requests.
The services provided to citizens will be further enhanced by the adoption of the electronic Citizen´s Card to be launched at the end of 2006.
(Source: http://www.infosociety.gov.pt/projects.htm#crds)

1.3.19.2 Existing issues

- The Portuguese smart card is one of the only IDM solutions in Europe which is engineered to cover five different application fields. This offers the clear benefit of ease of use to services, but also raises privacy concerns, particularly since the card will also provide access to privacy sensitive services, inluding health insurance, taxes and voting information (although such sensitive data will obviously not be stored on the card itself).

1.3.19.3 Analysis: successes, failures and lessons learned

- The Portuguese government allows ample opportunity for the development of local and regional services, most notably through the Digital Cities project. This has the advantage of catering to local interests, but also risks creation confusion if the services are organised in a too diverse manner.
- The Portuguese administration has an extensive tradition in issuing ID cards (including the generic Identification Document, Tax Payer's Card, Social Security Card, Voter's Card, and Health System Card). Furthermore, the Citizen Card will be valid as a European travel document. As a result, the single universal ID card is generally perceived as a positive simplification measure. Privacy issues remain to be examined, however.
- The Citizen Portal, despite its somewhat misleading name, provides a homogenic user

experience to a wide selection of eGovernment services, both for citizens and businesses. The integration of the future Citizen Card will further enhance user friendliness.

1.3.19.4 Expected future developments

The Portuguese Citizen Portal is under continuous development, and will notably be modified to incorporate the identification/authentication services of the Citizen Card when it is rolled out in late 2006.

1.3.20 Slovakia

1.3.20.1 General status and most significant systems

In Slovakia, there are two systems for issuing and holding unique personal identifiers in parallel. Within the old system, unique personal identification numbers are issued by the Ministry of Interior. They are created based on the citizen's date of birth plus a special number making the resulting identification number unique. Personal identification numbers together with some other personal data of a citizen, such as name, surname, maiden name, date and place of birth, sex and nationality, are stored in the central register of personal identification numbers.
In the course of 2006, the Ministry of Interior plans to replace the old system of unique identification numbers by a new system. This new system will create new personal identifiers – so called BIFO – using cryptographic algorithms. The new identifiers will no longer be unique for all sectors of applications. The new identifiers will be public sector oriented. It is also planned to enable online connections between different existing national registers that are creating these new identification numbers. The implementation of a central BIFO register is planned as well. Unfortunately, many Slovakian laws are explicitly bound up with the old personal identification numbers. Therefore, many laws still have to be adopted for using the new sectoral personal identification numbers.

Within Slovakian laws, the terms Identification and Authentication are already defined in general. These terms are given as follow:
Definition: Authentication of a user is the confirmation of user identity according to authentication level based on comparison of an access user identifier with a value saved in access resource. [339, May 2004, Vyhláška Národného bezpečnostného úradu o bezpečnosti technických prostriedkov]
Definition: Identification is detection of:

- name, surname, personal identification number or date of birth, type and number of identity card of person; in case of foreign person the nationality as well; in case of person legitimated to trade: the place of trade and trade identification number as well,
- name, residence and identification number of legal person
- in case of emancipated minor: the name, surname, personal identification number or date of birth, type and number of identity card of parent or legal representative
- identification number or similar code for client assigned for purpose of trade. [367/2000, October 2000, zákon o ochrane pred legalizáciou príjmov z trestnej činnosti a o zmene a doplnení niektorých zákonov]

1.3.20.2 Existing issues

A Electronic signatures

Slovakia has transposed the EU Directive for Electronic Signature (1999/93/EC) through its law on E-Signatures (law-no.: 215/2002), which entered into force in May 2002.

B Central eGovernment Portal

The Slovak government has created a centralised eGovernment portal, http://portal.gov.sk, which presently offers access to a limited number of eGovernment services. The system is accessible after registration, using a basic username/password system.
In the current pilot phase, the portal includes information on job vacancies in various regions of Slovakia, and search capabilities to determine if any given person has a valid trading licence based on a birth certificate number.

C Qualified certification authorities

In Slovakia, the National Security Authority (NBÚ) is the public regulatory authority which is responsible, amongst others, for:

- accrediting or de-accrediting qualified certification authorities;
- keeping records of certification authorities operating in Slovakia;
- certifying electronic-signature products.

Three qualified certification authorities are in place since 2005:

- EAVPU Certifikačná Autorita
- D.Trust Certifikačná Autorita, a.s.
- Prvej Slovenskej Certifikačnej Autority (PSCA)

The National Security Authority (NBÚ) acts as root certification authority.

D Electronic tax returns for individuals and businesses

The eTax services (electronic tax returns) for individuals as well as the eTax and eVAT services for businesses are available since 2004. To access these services, users need either a digital certificate or a password. A certificate issued by any of the three qualified certification authorities of Slovakia is accepted for granting access, but the tax authority aims to support certificates issued by any other European certification authority as well. For eTax services in general, prior first usage a registration procedure at a local tax authority is required. During this registration process, the identity of a user is proven by using conventional identity cards. After this initial procedure, the user can access his tax account using her username/password or her electronic certificate.

E University student cards

Since October 2004, each student of Slovakian universities possesses a student card in form of a chip card (standard MIFARE MF1 IC S70). The card electronically holds the personal data of a student; identifying students electronically is possible. Student cards are mainly used for library borrowing services, access control and public transport.

1.3.20.3 Analysis: successes, failures and lessons learned

Up to now, Slovakia still issues unique identifiers for citizens, which are used within all sectors of applications. For the future, a new IDM system has been planned with a new form of personal identifiers. These new kind of identifiers are no more unique. They are created exclusively for dedicated sectors of the state using cryptographic methods. Thus, even Slovakia is going to use sectoral identifiers in the future.
Slovakia has no electronic identity token for all citizens in place. Digital certificates for electronic signatures can be used for accessing eTax services, but only after an initial registration procedure in which the identity of the user is proven.
It is worth mentioning that Slovakian law has defined the notions of identification and authentication.

1.3.20.4 Expected future developments

In the course of 2006, the current IDM system of unique identifiers will be replaced by the new IDM system using sectoral identifiers.
Furthermore, the Slovak government has announced its intentions of making all eGovernment services available through its portal, http://portal.gov.sk, by 2008.

1.3.21 Slovenia

1.3.21.1 General status and most significant systems

Slovenia identifies natural persons by single unique identifiers:

- personal registration number (PRN; Slovenian abbreviation: EMŠO) - see below
- Tax number

These unique identifiers of natural persons are held in a database which allows translation from a given certificate serial number to PRN and Tax number.

Slovenia has adopted the EU Directive on electronic signatures by the Act on Electronic Commerce and Electronic Signature (ZEPEP) in the year 2000. In 2004, a further act amending act on Electronic Commerce and Electronic Signature was set into force in order to create a legal basis for an upcoming e-ID card project.

A Personal Registration Number of Citizen (PRN)

In Slovenia, due to the Central Register of Population Act (Official Gazette RS, no. 1/99) every Slovenian citizen is registered with the Slovenian Central Register of Population (CRP) thus is assigned a unique Personal Registration Number (PRN). Citizens usually become registered with the CRP at birth or immigration. Other individuals who have no PRN but have to exercise some rights or duties in Slovenia become registered with the CRP as well. For instance, even foreigners become registered with the CRP thus receive a PRN in the event of buying a Slovenian property or other events.

B Slovenian Governmental Public Key Infrastructure

Two governmental certificate service providers are in place:

- SIGOV-CA: productive since June 2000; issues certificates to governmental employees only
- SIGEN-CA: operational since July 2001; issues certificates to citizens and private sector

Beside these two governmental CAs, several private sector CAs are operational as well, e.g. HALCOM-CA, AC NLB, and POŠTA CA; but with respect to the upcoming e-ID card project only certificates issued by the governmental CAs are relevant.

1.3.21.2 Existing issues

A Slovenian e-ID Card Project

Slovenia has started to develop electronic identity (e-ID) cards in February 2003. The ID-card in Slovenia is not obligatory; nationwide issuance of e-ID's was planned for 2005, but was postponed for at least 3 years. The Slovenian e-ID card concept is to be the combination of a signature card and a conventional, visual ID-card.
Individuals will be required to request for a Slovenian e-ID card at a registration authority or an administrative office. As with present ID card the individual must be registered with the central population register (CPR) thus the individual has got her personal registration number (PRN) already. Based on the personal data the e-ID card will be personalized. The governmental certification authority SIGEN-CA issues qualified certificates for the individual which will be stored on the e-ID card. Certificate serial number (SN) is stored in a special database along with the PRN.
From the technical point of view, the smart card of the e-ID card shall hold

- personal data of the cardholder, such as name, etc.
- two key-pairs thus two electronic certificates: one certificate/key-pair for authentication and encryption purposes, a second certificate for creation of electronic signatures.
- Upon latter decision the card should be ready to upload additional biometric data.

Beside providing an electronic identity the Slovenian e-ID card shall be used as conventional ID card as well. Therefore, the layout of the front side is to contain the cardholder's personal data and her/his image.
This e-ID system will base on digital certificate and electronic identification number which is a part of the digital certificate:

- Electronic identification numbers, a part of the digital certificate, are used for this e-ID system; they are stored also in a governmental database.
- The electronic identification numbers are connected to PRN and Tax number through records stored in a special register. Otherwise PRN is along with other personal data stored in the central resident registers and the same is with Tax number, which is stored in the register of Tax numbers
- System is driven by a centralised authority; in detail: the e-ID system is driven by the Ministry of Public Administration; the register of Tax numbers is driven by the Slovenian Tax Authority; the Central Residents Registry is under the authority of the Ministry of Interior.
- The electronic identification number is unique; it is connected to person's personal registration number (PRN) and Tax number.

- The electronic identification number does not remain the same throughout a person's lifetime, although the personal registration number (PRN) and the Tax number are the same through person's lifetime
- The personal registration number (PRN) is obligatory for every citizen;
- The e-ID system is open to foreigners as well: foreigners can apply for certificates. The condition to obtain a certificate is to have a PRN and a Tax number in Slovenia.
- The e-ID system is not limited to e-government applications only; it can be used for other applications as well.

B e-ID Cards for Governmental Employees

This present e-ID card system is used for unique identification and authentication of governmental employees, encryption of documents, and digital signature. It does make use of a digital certificate and a unique electronic identification number, which is a part of digital certificates, as well as name, last name and e-mail. Neither certificate nor the card does contain further personal data. The certificate can be used in different applications, not only governmental.
This identification system base on digital certificate and electronic identification number which is a part of the digital certificate (see also description of the general e-ID system above):

- Electronic identification numbers, a part of the digital certificate, are used for this e-ID system; they are stored also in a governmental database.
- The electronic identification numbers are connected to PRN and Tax number through records stored in a special register. Otherwise PRN is along with other personal data stored in the central resident registers and the same is with Tax number, which is stored in the register of Tax numbers
- System is driven by a centralised authority; in detail: the e-ID system is driven by the Ministry of Public Administration; the register of Tax numbers is driven by the Slovenian Tax Authority; the Central Residents Registry is under the authority of the Ministry of Interior.
- The electronic identification number is unique; it is connected to person's personal registration number (PRN) and Tax number.
- The electronic identification number does not remain the same throughout a person's lifetime, although the personal registration number (PRN) and the Tax number are the same through person's lifetime
- The personal registration number (PRN) is obligatory for every citizen; the electronic identification number used for this e-ID system is issued only to civil servants.
- The e-ID system is not limited to e-government applications only; it can be used for other applications as well.

C Legal issues:

- The e-ID systems is built according to the Slovenian Data Protection Act.
- An Electronic Commerce and Electronic Signature Act is in place. An Electronic Signature part of the act is entirely in accordance with the EU Directive 1999/93/EC.
- Question of authentication is not especially emphasized by law.
- There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).

D Technical Issues:

- Smart card based system; smart cards are issued to civil servants only.
- The digital certificate stored on the smart card is valid either for 60 months (web certificate) or 36 months with the possibility of automatic issuance of new certificates (enterprise certificate).
- Persons are authenticated by password (PIN)
- Electronic signatures are used.

The following interoperability initiatives have been considered:

- eEurope Smart Card Charter
- EESSI standards
- European electronic citizen card - CEN TC224/WG 15
- Porvoo Group
- CEN eAuthentication Workshop

- EUCLID
- eEpoch

E IT-Security Aspects:

- Public Key Infrastructure (PKI) based on a single governmental CA is used.
- The unique identification number of this e-ID system is held in the certificate.
- Qualified signatures (SSCD plus qualified certificate) are used for governmental employees.

F e-Health Insurance Card System

The Slovenian Health Insurance Card System has been introduced in the years 1999/2000 by the Health Insurance Institute of Slovenia (HIIS) following the European Union recommendations for health card system. Within this system two types of electronic identification cards are used: the Health Insurance Card (HIC) and the Health Professional Card (HPC). The first one is issued to every insured person in Slovenia; the latter one is used to identify health care professionals. These cards are used to identify insured persons and health professionals within the health care system and health insurance system of Slovenia. They cannot be used for identification/authentication in eGovernment applications.

G Health Insurance Card (HIC)

The HIC is a microprocessor smartcard; it has been issued to all insured persons in Slovenia (about 2,100,000).
The following data are stored in the chip:

- details of the cardholder, such as the unique identification number (HIIS number)
- details of the contribution obligor, such as registration number, name, address etc.
- compulsory and voluntary health insurance details and validity of insurance policy
- selected personal physician details
- cardholder's decision about organ donorship
- dispensed drugs and medical technical aids

On the card body, the following information is visualised:

- unique identification number of the cardholder (HIIS number)
- name and surname
- date of birth
- card-number

Beside the cardholder, only authorised persons – authorised by the use of the Health Professional Card – are allowed to read and write data to the HIC.

H Health Professional Card (HPC)

Also the HPC is a microprocessor smartcard; it has been issued to about 18,000 health professionals in Slovenia. In order to authorise the health care professional, the HPC is equipped with a key to access data on the HIC.
The following data are stored in the chip:

- card holder's identification number
- serial number of the card
- card holder personal data
- profession
- country Code
- institute of Public Health code number
- specialization
- type of access rights

On the card body, the following information is visualised:

- unique identification number of the cardholder (HIIS number)
- name and surname
- date of birth
- card-number

I Future Developments:

In the future, the currently used generation of smartcards will be replaced. One major goal is also the introduction of a Public Key Infrastructure (PKI). Thus, also the new generation of Health Insurance and Health Professional Cards will be able to hold certificates and create electronic signatures. Especially for physicians, the introduction of qualified certificates/signatures is envisioned in order to achieve secure e-communication and e-signatures. Another aim is to gradually introduce online accesses using HIC and HPC.

1.3.22 Spain

1.3.22.1 General status and most significant systems

The Spanish Government's most recent eGovernment strategy is the so-called "Plan Conecta", the first version of which was presented in September 2004. A key component of this plan is the introduction of an electronic national identity card by the name of DNI Electronico, which will gradually replace the traditional Spanish identity card. Roll-out of the new card has started in March 2006, in the city of Burgos. By the end of 2006, eID cards are expected to be rolled out in 20 provinces, as well as in Ceuta and Melilla.
The card incorporates integrated eSignature/eAuthentication capabilities, and will be mandatory for any Spanish citizen over the age of 14.

A History, Scope and Goals

2001 can be considered the year in which Spain first set out the general principles of its eGovernment policies. The Spanish Certification Authority (CERtificación ESpañola - CERES - http://www.cert.fnmt.es/) was established as a part of the National Mint. CERES' main purpose is the creation and management of digital identities to citizens, in order to allow them to authenticate themselves when communicating with public institutions. CERES functions as a certification service provider.
2001 also saw the launch of the citizen service portal Administracion.es, which provides an overview of and access to a wide variety electronic services offered by the Spanish government. Certain services require the use of PKI through a certificate issued by CERES. A second portal, Ciudadano.es, focusing specifically on citizen services, will go live in 2006.
Finally, the Spanish eID project was also put into motion in 2001. The project was however delayed a number of times, and actual distribution of cards has begun in March 2006, through a phased roll-out. Similar to other European nations, the Spanish eID will contain two certificates: one for eAuthentication and one for eSignatures. The incorporation of biometric identifiers, most notably a fingerprint scan, is contemplated for the future, although at present the administration considers the photo and date of birth of the bearer to be the only biometric data.
The eID card, made by the Spanish National Mint, will be distributed through local police stations. Holdership of the card is obligatory for any Spanish citizen over the age of 14, and the total holder count is expected to eventually reach 35 million. The card is a national ID and a European travel document.
Additionally, an electronic notification system has been put into place in 2003. This system is particularly interesting because the Spanish government issues a unique e-mail address to all of its users, and because the electronically served notifications have the same legal value as their paper counterparts. Communication through this service is encrypted and requires a digital certificate.
The Spanish Government also supports a number of local/regional initiatives, such as through the Digital Cities programme, in order to best serve the users' needs.

B Technology

The eID card contains two certificates: one for eAuthentication, and one for eSignatures, which both require the user to enter a PIN. The certificates are valid for a period of 30 months. The certificates contain a unique identifier, the holder's name, date of birth, and nationality.
Additionally, in the future the Spanish administration is considereing the inclusion of a fingerprint scan of the holder, and an application for cryptography and Match-on-Card. Thus, the card will be

able to authenticate the user autonomously, a functionality which will be used to update the certificate.
Additional information is expected to be published on http://www.dnielectronico.es/.

C Applications

Specific applications that will make use of the new eID's capabilities are still under development, but include a common platform to validate electronic signatures and a single sign-on and time-stamping infrastructure. Online tax declaration and a variety of social security services are also planned. Interestingly, the recent eSignatures law requires all administrations to use the Spanish eID's signing mechanisms wherever possible.
Meanwhile, the citizen service portal Administracion.es contains a few overview of services presently available. The new portal www.ciudadano.es ("www.citizen.es", currently not yet on-line) will likely absorb part of the older portal's functionality.

1.3.22.2 Existing issues

- The use of biometrics is always somewhat controversial, and as the Spanish eID is one of the largest planned roll-outs, the public's reaction remains to be seen.
- While a number of eGovernment services already exist at the national and local level, the focus seems to be on autonomy rather than coordination.
- Presently, there are only plans for a general eID card. No separate electronic health service card appears to be planned at this time.

1.3.22.3 Analysis: successes, failures and lessons learned

- It is interesting to note that the Spanish law makers have chosen to oblige public services to use the eID's electronic functions whenever possible. It will be interesting to see if such an obligation has a significant impact on the uptake of the card. However, extensive information/promotion campaigns will certainly be a key requirement to assuring the card's success.
- The Spanish government allows ample opportunity for the development of local and regional services. This has the advantage of catering to local interests, but also risks creation confusion if the services are organised in a too diverse manner.
- The deployment of the eID card has suffered extensive delays, and the exact roll-out date is still uncertain. Budgetary reasons were certainly a factor in this delay. Possibly, the technical, legal and organisational requirements for the deployment for an advanced eID solution were also underestimated.
- The eID focuses on the core functionality of identification and serving as a travel document. It is not expected to be used for the provision of health services, banking, etc. While this fact is beneficial for reasons of data protection, it may prove to be a discouragement for uptake.

1.3.22.4 Expected future developments

The Spanish eGovernment infrastructure is expected to develop very rapidly in the following years. The roll-out and pilot projects of the new eID card has begun in March 2006.
There are currently also plans to examine if ePassport functionality could be integrated into the eID card.
Additionally, the general framework for eGovernment services in Spain is transforming rapidly, through the continued development of electronic data exchange infrastructure (both A2C and A2A) and the development of new portals such as ciudadano.es.

1.3.23 Sweden

1.3.23.1 General status and most significant systems

Together with its biometric passports Sweden has started offering national electronic ID cards to its citizens that contain biometric data. The eID card is not compulsory in Sweden, and has known little success. This is also due to the fact that another initiative, called BankID, is being used by both public sector administrations and private companies.

A remarkable initiative was the introduction of an open standard for mobile electronic identification by the Swedish government. This standard is now further maintained and developed by a non-profit association.

A History, Scope and Goals

In Sweden citizens get a unique national identifier that consists of the date of birth of the citizen and a 4-digit number that is added at the end. The number is used throughout the whole public sector.
In accordance of the European Directive on electronic signatures the Swedish Act on Qualified Electronic Signatures was published on November 2, 2000. Several Certification Authorities had been set up and initially electronic identity solutions were issued by Swedish banks and the Swedish post office, which is no longer running a CA.
BankID is an IT-infrastructure for electronic identification purposes that can be used by any bank fulfilling one of the following requirements: it must have a customer-identification process that guarantees the customer's identity, and it must provide some BankID-approved Internet security solution. At the moment 8 banks make use of this infrastructure. It has been used in the public sector by the National Tax Board and the National Social Insurance Board.
http://www.BankID.com/
In October 2005 the Swedish government started issuing biometric passports. These passports are compliant with ICAO recommendations for biometrics in machine-readable travel documents and with the regulations of the European Council on standards for security features and biometrics in passports and travel documents. There have been some privacy issues with the unencrypted storage of information on the RFID chip. In Sweden passports and identity cards are manufactured by SETEC and issued by the police.
At the same time the Swedish government started issuing electronic identity cards. These card also contain biometric data and are manufactured by the same supplier of the new passports. It is card that is similar to eID cards issued by other Member States. It proofs the identity of the holder and can be used as a travel document in the Schengen countries, however it is not compulsory for Swedish citizens to have one and it does not replace paper identity documents.
A remarkable initiative was the introduction of an open standard in June 2006 for the secure electronic identification by means of mobile devices. These systems will use the SIM card of a mobile phone and the mobile eID are mostly issued by Swedish banks. To further develop and maintain the mobile eID standard a non-profit association called WPKI was set up.
http://www.wpki.net

B Technology

The biometric passports contain a Radio Frequency Identification microchip which stores a digital photo and personal information of the holder. The passports are compliant with the ICAO recommendations for biometrics in machine-readable travel documents. In addition to the contactless chip, the national eID cards also contain a traditional chip that can be used for accessing eGovernment services.

C Applications

- In November 2004 an e-government portal (http://www.sverige.se) was launched. It provides Swedish citizens and people living in Sweden with links to online services, links to specific information and contact details for several public adminsitrations. It has a search engine that includes all public sector websites.
- Swedish taxpayers receive a pre-filled and pre-calculated version of their tax return. They can use a username and password offered by the National Tax Board, they can the electronic ID issued by one of the banks participating in the BankID initiative or use the National Tax Board's telephone service or an SMS.

1.3.23.2 Existing issues

- The use of a unique identifier brings up some privacy issues on the one hand and some benefits on the other hand. However this counts for all countries using unique national identifiers and the use of such a number by administrations should be properly regulated by legislation as it is the case in Belgium for example, where administrations have to be authorised to use that number. The divergent use and issuance of national identification

numbers is a hindrance for interoperability between different member states.
- In Sweden and other Scandinavian countries Certification Authorities are very often banks or other commercial organisations like with the BankID initiative. Authorities or companies that want to use the infrastructure need to go into an agreement with one of the banks participating in BankIK and they have to install certified validation software. As a consequence anyone willing to be BankID-enabled has to make significant investments to be able to support it.
- Data stored on the RFID chip is not ecnrypted and can be read out by anyone, which is a huge privacy issue. It is also not clear what will be the implications of storing biometric information in a central database.

1.3.23.3 Analysis: successes, failures and lessons learned

- The BankID identity seems to be the only successful initiative and because the banks only trust BankID-issued identities it is very unlikely that other eID initiatives will have any impact, especially in the private sector.
- It is worth noting that many other identity documents already contain biometrics data as most of them have an image of the holder printed on the outside of the card or stored on the chip. The difference with the Swedish cards is that they are ICAO compliant so that communication through contactless chips is possible and that the image on the chip was intentionally included to allow automated facial recognition. It is not clear if there were good reasons to also include biometrics on the national eID cards especially because they are not compulsary and most citizens tend to use the BankID system to authenticate themselves for online services such as the online tax declaration.

1.3.23.4 Expected future developments

No plans are mentioned to further promote the use of eID cards.

1.3.23.5 References

- http://www.BankID.com/BankIDCom/EnglishMaster.aspx
- http://www.wpki.net/index_eng.html
- http://www.skatteverket.se/english/main/electronictaxreturn.4.34a801ea1041d54f9e28000259.html Swedish National Tax Board
- http://www.police.se/inter/nodeid=10230&pageversion=1.html
- http://www.sverige.se/
- http://www.sweden.gov.se/sb/d/574/a/27293

1.3.24 United Kingdom

1.3.24.1 General status and most significant systems

The United Kingdom does not have a tradition of centrally managed identification systems, and plans to introduce such systems typically meet with strong opposition, both from a significant portion of policy makers and even more so from the public at large. As a consequence, the UK does not currently have a mandatory eID programme for the general public.
Plans to introduce eID cards have existed for some time, however, and actual design and roll-out planning has started in 2006, followed by the implementation of a legal framework through the Identity Cards Act of 2006 (see also: http://www.opsi.gov.uk/acts/en2006/2006en15.htm). As it stands, a compulsory eID card is expected to be issued to any UK resident staying in the UK for more than three months and over the age of 16. The first cards are expected to be rolled out in 2008/2009 (see: http://www.identitycards.gov.uk/index.asp).
While the technical details are not fully determined yet, the solution currently appears likely to be similar to the Belgian solution, offering an eID card with authentication and electronic signature features, and backed by a central National Identity Register containing authentic information. Plans to include biometric features on the card have also been retained, and biometric data to be included on the card will likely include digital fingerprints and iris scans (source: http://www.identitycards.gov.uk/scheme-what-produced.asp#recording).
In addition, there is a multitude of projects which can be qualified as advanced and which cover a variety of application fields. Chief among these is the Government gateway

(http://www.gateway.gov.uk), which issues credentials to registered users (individuals, organizations or agents). These credentials can be used to authenticate the registered entity across a variety of specific services.
Finally, there is a smaller number of national programmes which are generally limited to a specific application field, such as the eSources eProcurement/eTendering portal (http://www.homeoffice.bravosolution.com). The UK Government also provides a general eGovernment information portal through http://www.direct.gov.uk.

A History, Scope and Goals

The most generic central UK identification platform is the Government gateway (http://www.gateway.gov.uk). This portal went live in 2001, and was set-up by the e-Delivery Team (part of the UK eGovernment unit), which is also responsible for its maintenance. It has over 6 million active enrolments with more than 50 services from 25 different government entities. On this portal, users (individuals, organizations or agents) may choose to apply for either a userID/password or a digital certificate. The choice is mostly determined by the desired eService: as digital certificates offer more security, some services may require their use, while others may consider a username/password to be sufficient.
Upon receiving the credential of choice, the user may enroll for the desired eServices. Depending on the desired service, an activation PIN code may be sent through regular mail. After the user activates his credentials through the use of this PIN, he may freely use the avaible eGovernment services. A list of available services can be found on the project website, and currently includes a number of fairly specific services, such as:

- Procedure for the Electronic Application for Certificates from the HMI (PEACH) - for importers, exporters and processors of whole fresh produce into and out of the EU
- Department of Trade and Industry Export Licence Application - for exporters of items controlled for strategic reasons or because of sanctions
- Child Benefit Online - for individuals wishing to claim Child Benefit and those already in receipt of Child Benefit who wish to report changes in circumstances.
- Carer's Allowance - for individuals aged 16 or over who spend at least 35 hours a week looking after someone who is getting or waiting to hear about these benefits.
- Employer Direct Online - Employer Direct Vacancy Notification (for employers who wish to place vacancies with JobcentrePlus
- State Pension Forecast - for the full working age population - 16 years of age through to 4 months and 4 days from State Pension Age – currently 60 for women and 65 for men.
- A variety of local (municipality/county bound) initiatives.

The administrations that deliver these services provide online forms and information through their own websites.
In addition, the UK Home Office has expressed the desire to introduce a National Identity Cards scheme. Development and roll-out have purposely been spread over an extended period of time: while the principal decision to implement such a scheme was taken in November 2003, actual design and roll-out planning has started in 2006, followed by the implementation of a legal framework through the Identity Cards Act of 2006 (see also: http://www.opsi.gov.uk/acts/en2006/2006en15.htm. As it stands, a compulsory eID card is expected to be issued to any UK resident staying in the UK for more than three months and over the age of 16. The first cards are expected to be rolled out in 2008/2009 (see: http://www.identitycards.gov.uk/index.asp).
While the technical details are not fully determined yet, the solution currently appears likely to be similar to the Belgian solution, offering an eID card with authentication and electronic signature features, and backed by a central National Identity Register containing authentic information. Plans to include biometric features on the card have also been retained, and biometric data to be included on the card will likely include digital fingerprints and iris scans (source: http://www.identitycards.gov.uk/scheme-what-produced.asp#recording).

B Technology

No universal IDM system currently exists. The main tenets of the most generic central UK identification platform (the Government gateway - http://www.gateway.gov.uk) have been explained above: the user can apply for either a userID/password or a digital certificate.

Interestingly, users can also register as an Agent, who may be chosen as a representative to act on behalf of other users. Thus, the Gateway incorporates a rudimentary mandate/proxy system. When certification is used for such services, certificates can be purchased through Equifax and Chamber SimplySign. The PKI system is not entirely platform independent, excluding certain browsers and operating systems. The certificate contains information about the user's identity (such as its name, email address, the date the certificate was issued and the name of the certificate authority which issued it). The certificate also contains the 'public key'; whereas the 'private key' is stored on the user's local hard disk.
The national identity card programme is still under development, and no technical details are available at this time.

C Applications

While there is no universal IDM system which allows access to all available eGovernment schemes, the UK Government Portal does offer a multitude of possibilities, as indicated above. There are a number of other online services which depend on different identification solutions, such as the eSources portal.

1.3.24.2 Existing issues

No universal IDM system currently exists. The ModinisIDM project intends to follow up on the development of a more general IDM eGovernment system in the UK, with specific attention for the possibility of a new eID card scheme.

- There is no common solution for eGovernment services, and services offered through the Government Portal are somewhat disparate, relying on two different authentication tracks depending on the service used.
- Current plans to introduce a biometric eID card are controversial. It remains to be seen if sufficient consensus can be reached regarding the planned scheme to permit a successful rollout.

1.3.24.3 Analysis: successes, failures and lessons learned

As there is no generally accepted eID solution yet, only a limited number of conclusions can be drawn:

- The question of acceptability as it presents itself in the UK is a striking example of the importance of socio-cultural elements which must be taken into account before any IDM system can be rolled out.
- The planned eID card system is one of the first systems to include biometric features. Thus, it will be a test case for the usability and added value of such data.
- The Government portal offers a relatively large number of services and the possibility of further growth, but depends on two distinct authentication tracks. It does however offer a mechanism for mandates/proxies.

1.3.24.4 Expected future developments

As indicated above, much of the future of eGovernment IDM in the UK depends on the deployment of a generic authentication mechanism, which the eID card certainly could offer. While the Government Portal already offers a functional substitute, its disparate service bundle and two-tracked authentication mechanism may be a limit to its growth.

1.3.25 The Netherlands

1.3.25.1 General status and most significant systems

Public administration in the Netherlands traditionally depends principally on the social security number – SSN or "sofi-number") and the public register number (i.e. the administration number used in population register - A-number). However, a programme intended to introduce one single identification number for e-ID purposes is currently being deployed (the Citizen Service Number ("Burgerservicenumber"), in addition to the DigiD programme. Additionally, the introduction of an electronic identity card by 2007 is being considered. This section will briefly describe the key characteristics of Dutch eGovernment IDM policy.

A History, Scope and Goals

The development of electronic access methods for eGovernment services has increased in the Netherlands since 2003, when DigiD development began. This system allows the electronic identification of persons on the internet. Briefly summarised, DigiD is a joint undertaking between the Ministry of Internal Affairs and Kingdom Relations, the Ministry of Economic Affairs, ICTU (the Government ICT Unit), the Dutch Tax Service and a number of other stakeholders. The platform is open to citizens, enterprises and government services. By 1 January 2006, at least 50 municipalities and 6 implementing bodies will be connected and there will be a minimum of 75.000 users.
DigiD is a three-tiered system. For citizens, the basic access level depends solely on the use of a user name/password, whereas the second level will use a basic PKI infrastructure. The third level will use Bankpass Easytrust and PKIO.
On a separate level, the Dutch government has taken the first steps to introducing a so-called Citizen Service Number (CSN), which aims to assign a unique identity number to each natural person, equaling their social security number. The main difference is that the CSN will allow a much broader use than the sofi-number, which is subject to rather stringent legal restrictions. Although each citizen will have only one CSN, this number is planned to be given a new denomination in each application field (such as Care Information Number ("Zorg Informatie Nummer") and Education Number ("Onderwijsnummer"), despite being otherwise identical.
In a later phase a Companies and Institutions Number (CIN) will be assigned to each legal person (based on the existing Register of Companies). This number will then be used in every communication between administrations and citizens/businesses, as well as in the information exchange between administrations. The introduction of the CSN is envisaged to begin in January 2006; the CIN will follow in a later phase. In the long run, only the CSN/CIN will be used for online entity authentication.
Additionally, a number of Key Registers are being worked on to facilitate and optimize information collection and exchange. By using these Key Registers, all data should be collected only once, and there should only be one authentic source for each piece of data. The six registers are planned to cover natural persons, companies, plots, addresses, buildings and maps. Other contemplated registers include the income and wealth register, the non-resident register and social security register.
In parallel with these programmes, the introduction of an e-ID card provisionally named eNIK (Elektronische Nederlandse Identiteitskaart – Electronic Dutch Identity Card) is planned by late 2006/early 2007, mirroring the developments surrounding the new (biometric) passport (although the inclusion of biometric characteristics has not yet been decided upon). This e-ID will be used as a general means of identification and as a European travel document, and as a tool for on-line applications based on PKI. As such, eNIK will likely eventually integrate the functionality of DigiD. However, eNIK is still in an early stage and details are scarce at this time.
The legal background for a hierarchical nationwide PKI is already in place. The Act on Electronic Signatures of 8 May 2003 entered into force on 21 May 2003 and implements the e-Signatures directive.

B Technology

At present, the CSN and eNIK are not yet operational. CSN is expected to be functional in January 2006, while eNIK will not be made available until October 2006 at the earliest. Thus, only DigiD's technical characteristics are presently available. These characteristics are summarised in DigiD's project description above. Other technical details are dependent on further development.

C Applications

At present, the CSN and eNIK are not yet operational. CSN is expected to be functional in January 2006, while eNIK will not be made available until October 2006 at the earliest. Thus, only DigiD presently offers any functionality.
The DigiD site (www.digid.nl) offers an overview of presently available applications (http://www.digid.nl/burger/over-digid/wie-doen-mee/) (Dutch only). The most significant service providers are the communities, 18 of whom now offer a digital counter. Using a DigiD username/password, citizens may use these counters to request copies of official documents, such

as birth certificates or specific licenses. Several employment and social services also support the DigiD-system. More applications are expected to be added in the following months.

1.3.25.2 Existing issues

The analysis of the situation in Netherlands shows that electronic authentication is still evolving rapidly, and that this report will likely need to be amended and updated frequently. The ModinisIDM project intends to further elaborate on the following aspects:

- Privacy issues resulting from the use of unique numbers based on single centralised registers. However, during the registration and verification process name and address data is drawn from the central register (to send an activation code by post to the registrant). This address data is destroyed after use, so DigiD does not contain address data. In this sense, DigiD also protects privacy. A privacy policy has also been put in place as well as other security controls. All sensitive communication is SSL encrypted.
- The system currently already uses centralised application specific registers, and the Dutch government is planning to add/develop further centralised key registers (covering amongst others natural persons, companies, plots, addresses, buildings and maps).
- DigiD is not obligatory. The use of DigiD is optional for most services related to municipalities or central government. People can always revert to a physical government office. DigiD is also not obligatory for service providers. The system may however become obligatory in the future for e.g. income tax applications for citizens and businesses.
- This system is limited to e-government: Citizen-to-Government domain (C2G) and Business-to-Government domain (B2G)
- National legislation on digital signatures is in place. This legislation is not applicable to authentication provision.
- There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).
- Electronic signatures functionality has not been integrated yet, but will be added in due time: e.g. bank token (challenge/response) and electronic ID (qualified signature).

1.3.25.3 Analysis: successes, failures and lessons learned

The following elements stand out as lessons to be learned from the deployment of the Dutch e-ID solutions thus far:

- In principle the DigiD e-ID system is opened to foreigners, although the possession of a Dutch SSN is required, which excludes certain categories of foreigners (such as (some) expats, tourists, most types of refugees)
- DigiD is not obligatory. The use of DigiD is optional for most services related to municipalities or central government. People can always revert to a physical government office. DigiD is also not obligatory for service providers. The system may however become obligatory in the future for e.g. income tax applications for citizens and businesses.
- In the future other authentication methods such as SMS authentication (planned for 2005), challenge response systems, and eNIK are planned to be integrated in DigiD. Due to its modular approach, this should be technically well feasible.
- The number of available applications is currently quite limited. While additional applications are in the works, there is thus far no "killer application" that clearly demonstrates the usefulness of the Dutch IDM platform to the general public.

1.3.25.4 Expected future developments

As indicated above, DigiD will be joined by the CSN in January 2006 and by the eNIK in late 2006/early 2007. It remains to be investigated:

- to what extent these different authentication platforms will overlap/be integrated.
- which services will be developed for each platform.

1.4 Analysis and categorisation

This chapter will provide a brief overview of the main conclusions which can be drawn from the country reports outlined above, and provides a summary of these reports by grouping the Member States into different categories, according to their status and deployment choices.

1.4.1 Variation between national approaches and the principles of local validity and interregional intransposability

Based on the profiles above, it is clear that the status of IDM solutions in the Member States varies greatly, both in sophistication, conceptual approach and technical choices. Local socio-cultural and historical background plays a large role in determining the choices made by the national governments in deploying their solutions. By way of demonstration, some nations (e.g. France) prefer to keep their IDM infrastructure entirely under governmental control (barring the outsourcing of certain technical processes, such as ID card production), whereas others (e.g. the Scandinavian states) generally allow more extensive partnerships with the private sector (e.g. the banking and financing sectors). Yet others (e.g. Estonia) rely to a very great extent on private sector input, not only for the creation of the IDM infrastructure, but even for service provision (eTransport, eBanking, and even eVoting).

Taking this consideration into account, it is not difficult to deduce two basic principles that should be considered as restrictions to the design of any large scale (e.g. pan-European) eGovernment IDM system:

- *The principle of local validity*

  This first basic principle simply entails that any national IDM system has been designed according to the desires, constructions and concerns of the target user group (this group being (a subsection of) the national population), at least to such an extent that the system would be able to gain sufficient acceptance within this target group. Of course, there will undoubtedly be exceptions to this rule, where the implementation of a given IDM system is unable to gain any traction due to concerns with its user base; but such systems can be left out of consideration for the purposes of the **modinis**^{IDM} study, as interoperability with marginal systems that are not actually used within their originating country is not a main concern.

  While rudimentary, this basic principle, which we have dubbed the local validity principle, suggests that it will be difficult to make substantial changes to any national IDM infrastructure; not only because of the typically substantial resource outlay concerns, but also because the existing design inherently caters to the needs of its user base. Therefore, any fundamental changes to the designs risks alienating the user base, because it deviates from the norms which they have considered to be important. Thus, major changes are likely to result in a drop-off in usage.

- *The principle of interregional intransposability*

  The second basic principle, interregional intransposability, is a logical consequence of the principle of local validity. If it can be said that each national IDM system has been designed and set up in such a manner that it satisfies local demands and concerns, and that such choices are significantly different between Member States (as the country profiles and the examples above have demonstrated), then this means that a perfectly workable and fully operational solution in one Member State can not necessarily be transposed to another Member State.

This is a significant consideration, as it puts the importance of best practice cases in perspective. While best practice cases certainly demonstrate which practices are considered widely acceptable within a specific Member State, it is not always possible to generalise best practice cases into a format which would be possible to implement in a different Member State. Thus, when identifying best practice cases, it is essential to correctly assess which aspects of the case make it a best practice case, and to assess if the general principles underpinning such aspects are susceptible of being transposed into a foreign context.

At any rate, it would be folly to think that a best practice case in a specific EU Member State would by definition be successful or even acceptable in a different Member State.

1.4.2 Phases of development status

Not all Member States have advanced their eGovernment IDM infrastructure at the same pace. While certain Member States have a long standing tradition in operating an IDM infrastructure, other Member States are currently still in the design phases.

For the purposes of this overview, the **modinis***IDM* study distinguishes between four successive phases in eGovernment IDM infrastructure design, implementation and operation:

- *Phase I: Conceptual / Design*

Member States in this initial phase have not yet deployed any large scale IDM solution that would be relevant to the **modinis***IDM* study, but are still examining the available solutions. This is typically only the case in some of the smaller Member States and a few of the newer Member States.

- *Phase II: Development / Roll-out*

The second phase consists of the actual development and deployment of the solution. Member States in this phase have (virtually) completed the design work, but have not yet established a significant user base, nor are popular and publicly accessible services available yet.

- *Phase III: Update / Review*

In the third phase, existing IDM solutions are being reviewed and modifications/updates are being considered. This is typically the case with Member States that have deployed basic solutions (e.g. username/password portals) several years ago, and which are now looking to refine such solutions, e.g. through the integration of PKI.

- *Phase IV: Consolidation*

In this final phase, only minor modifications to the existing IDM infrastructure are considered, but the infrastructure in itself is considered to be fairly mature, and presents a longer term solution. While there is no such thing as a definitive IDM system, larger scale changes are not currently being considered by Member States in this phase.

It goes without saying that all Member States have several eGovernment IDM systems deployed, and that some systems will be more advanced than others, thus making it impossible to consistently place any Member State into only one category. However, such a categorisation is still attempted below, in which the decision to place a country in a specific category is mostly based on the predominant IDM system, as identified in the national profiles above.

The 25 examined Member States can thus be grouped as follows:

Conceptual/Design	Development/Roll-out	Update/Review	Consolidation
Cyprus	Germany	The Netherlands	Austria
Czech Republic	Latvia	France	Belgium
Greece	Lithuania	Ireland	Denmark
Hungary	Portugal	Malta	Estonia
Luxembourg	United Kingdom	Slovenia	Finland
Poland			Italy
Slovakia			Spain
			Sweden

1.4.3 eID card based solutions

While the **modinis**^{IDM} study is not solely focused on eID card based solutions, it is an inescapable conclusion that many Member States are gravitating towards a PKI based eID card solution. For this reason, the following table provides an overview of Member States according to their preference in this regard.

It should be noted that, in compliance with the guidelines in section 1.2.1.2., the table only includes information on eID cards, i.e. ID cards with a chip or other technological component; thus excluding traditional (purely paper) ID cards.

No eID card	eID card is planned	eID card available to the public
Cyprus	The Netherlands	Austria
Czech Republic	France	Belgium
Denmark	Germany	Estonia
Greece	Latvia	Finland
Hungary	Lithuania	Italy
Ireland	Poland	Slovenia
Luxembourg	Portugal	Spain
Malta	United Kingdom	Sweden
Slovakia		

1.4.4 PKI based solutions

Similar to the overview above, the table below indicates the Member States which provide services to their user based using a PKI infrastructure. While all major eID card initiatives rely on PKI, it is of course also possible to offer PKI services without an eID card being involved, so that the tables are not identical.

No PKI solution	PKI solutions are available to the public
Cyprus	Austria
Greece	Belgium
Ireland	Czech Republic
Latvia	Denmark
Lithuania	The Netherlands
Luxembourg	Estonia
Poland	Finland
Portugal	France
	Germany
	Hungary
	Italy
	Malta
	Slovakia
	Slovenia
	Spain
	Sweden
	United Kingdom

1.4.5 Private sector intervention

One of the major points of difference between the Member States is the degree to which private sector intervention is invited / permitted in establishing an eGovernment IDM infrastructure. Whereas some Member States prefer to keep full control of all IDM related processes, others are more content to outsource certain aspects of their IDM systems. The table below gives an indication of the extent to which such private sector initiatives is allowed / encourages in the Member States

Public sector control; only minor private sector intervention	Public / private partnerships; significant aspects of IDM services are privately controlled	Very extensive private sector intervention; including providing eGovernment services
Belgium	Austria	Estonia
Cyprus	Czech Republic	
The Netherlands	Denmark	
France	Finland	
Germany	Italy	
Greece	Malta	
Hungary	Sweden	
Ireland		
Latvia		
Lithuania		
Luxembourg		
Poland		
Portugal		
Slovakia		
Slovenia		
Spain		
United Kingdom		

1.4.6 Planned/existing biometrics

While not extremely significant yet, the introduction of biometrics (fingerprints – iris scans – voice prints - …) into IDM solutions is considered to be promising by many public administrations. The table below indicates the stage of acceptance in the different Member States, ranging from "no planned biometrics"' to "active roll-out" of biometric solutions.

It should be noted that, for the purposes of this overview, the **modinis*IDM*** study team has elected not to consider photos of a card holder (either in print or in digital form) as biometric data. While such data does carry certain privacy implications, and technology might some day allow efficient automated facial recognition, such photos are none the less extremely common and widely accepted by the public. In order to keep the current overview balanced, such photos will not be considered as biometric data, as the emotional weight attached to this expression seems disproportionate to the relative insignificance at this time of a mere photo.

Additionally, it bears repetition to stress that the overview focuses only on major general purpose IDM systems, specifically excluding sector- or service specific IDM mechanisms such as passports, in which biometrics are expected soon to be generalised in all Member States.

No biometrics planned	Biometrics are being considered	Biometrics are being rolled out / are already in use
Austria	The Netherlands	Italy
Belgium	France	Slovenia
Cyprus	Germany	Sweden
Czech Republic	Spain	
Denmark	United Kingdom	
Estonia		
Finland		
Greece		
Hungary		
Ireland		
Latvia		
Lithuania		
Luxembourg		
Malta		
Poland		
Portugal		
Slovakia		

1.4.7 Local service solutions

While all Member States offer a certain level of diversification in offering services at the most suitable level, some Member States place a broader emphasis on local services. This can be useful, as it allows the most suitable regional level (e.g. municipality – province – community – state – etc.) to provide the needed services, thus ensuring that the offered services show a clear and immediate link to the needs of its user base. The flipside of the coin is that an excessive diversification of services could confuse the user bas, if such services are not sufficiently homogeneous.

The table below indicates the importance the different Member States accord to local service provision.

Only centralised services / incidental localisation	Significant local eGovernment projects	Unknown
Austria	The Netherlands	Cyprus
Belgium	Estonia	Czech Republic
Denmark	Finland	Germany
Ireland	France	Greece
Luxembourg	Italy	Hungary
Malta	Portugal	Latvia
	Spain	Lithuania
		Poland
		Slovakia
		Slovenia
		Sweden
		United Kingdom

1.4.8 Portal based solutions

In an attempt to ensure consistency of the eGovernment user experience, many Member States have taken to creating a centralised eGovernment service portal. Such portals can be helpful, by providing citizens and other users with a one-stop-shop-experience for eGovernment communication.

The table below indicates the portals made available by the different Member States. Only portals specifically providing access to eGovernment services (and not general public sector or eGovernmentactivity / specific service portals) are included in the table.

No portal available	Portal available	Address
Austria		
Belgium		
Cyprus		
Czech Republic		
Denmark		
The Netherlands		
Estonia		
	Finland	http://suomi.fi/english
	France	http://www.service-public.fr
Germany		
Greece		
Hungary		
Ireland		
	Italy	http://www.italia.gov.it
	Latvia	http://www.eparvalde.lv
Lithuania		http://www.govonline.lt/index.do
Luxembourg		
Malta		
	Poland	http://www.egov.pl
	Portugal	http://www.portaldocidadao.pt
Slovakia		
Slovenia		
	Spain	www.ciudadano.es
	Sweden	http://www.sverige.se
	United Kingdom	http://www.gateway.gov.uk

Prepared by:

The **Modinis**^{IDM} Study Team under the Service Contract number 29042, from DG INFSO, EUROPEAN COMMISSION

For further information about the eGovernment Unit

European Commission
Information Society and Media Directorate-General
eGovernment Unit

Tel (32-2) 299 02 45
Fax (32-2) 299 41 14

E-mail EC-eGovernment-research@cec.eu.int
Website europa.eu.int/eGovernment_research