Prepared for the eGovernment Unit
DG Information Society and Media
European Commission

Modinis
Study on Identity Management in eGovernment

eID Good Practices

31 July 2006

Table of contents

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

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 has identified good practice projects on identity management and did 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 final consolidated version of a status report of the most significant IDM systems used throughout the 27 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.

The document is the final iteration of a document that has been continuously developed throughout the project. 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).

1. Introduction

1.1 Motivation

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 aims to identify good practice projects on identity management and 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.

The survey has been created in two phases. In a first phase identity management projects have been collected in order to get an exhaustive overview of existing or planned identity management systems in Europe. The so-called Good Practice Project Lists are the outcome of this first phase identifying potential good practice projects. In a latter phase, a number of "very" good practice cases has been be selected from the preceding Good Practice Project Lists. The selected good practice cases may influence other Member State's identity management initiatives as well or are most likely to show potential for generalisation and/or cross border functionality.

1.2 Document Scope

The present document gives an overview of identity management systems used in e-Government applications in the Member States. The present collection of good practice projects is a progression of the preceding Good Practice Project List PL2, deliverable D3.7 respectively.

In contrast to the preceding list PL2, which aimed to present an exhaustive overview on the situation regarding identity management in all Member States, this list focuses on concrete identity management projects considered to be good practice cases.

The information of the good practice cases presented in this document was collected through a variety of sources:

- Information that was directly known to the project team 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.

One of the main tools of the MODINIS Study in general is the e-Government Good Practice Framework (GPF) which has been put in place by MODINIS lot 2. The e-Government Good Practice Framework aims to be a platform for interchanging information of good practice cases in e-Government. This platform asks e-Government experts to report their e-Government projects and

to keep the information of their projects up-to-date. So the framework should be a source of latest information on good practice cases in e-Government.

During the creation of the Good Practice Framework, case descriptions of good practice cases in the field of identity management have been provided by the **modinis*IDM*** study. The initial set of good practice cases have been taken from the preceding Good Practice Project List PL2. However, the cases initially reported by the **modinis*IDM*** study team were modified and verified by connoisseurs of the cases thus the current information stored within the good practice framework is up to date.

Therefore, this document contains good practice cases in the area of identity management that have been reported to the Good Practice Framework by the **modinis*IDM*** study team as well as by e-government experts. This document represents the information on identity management projects reported to the framework as seen on the 20th April 2007.

2. List of Good Practice Projects

This section contains the good practice projects in the area of identity management as reported to the Good Practice Framework (GPF). The list has been created by extracting the information from the GPF-database.

The list is sorted alphabetically by Member States; each section describes a particular good practice project.

2.1 Austria: Good Practice Case "Austrian Citizen Card"

*2.1.1 **Case Summary***

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 which eID token to activate. In this technology neutral approach currently several public sector and private sector smart card initiatives have taken up the concept, as well as a mobile service provider that allows using any cell phone capable of receiving SMS to act as a citizen card.

The major rollouts are the health insurance card (roll out completed end of November 2005, available to each), Bank cards (each bank card issued since March 2005), A1 signature (a service launched in March 2004 to activate mobile phones as citizen card).

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

*2.1.2 **Further Details of the Case***

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 for the market, i.e. to remain open for other smartcards or other technologies.

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 be capable being an "Austrian citizen cards". 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.

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), etc.

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 open source server-side modules (referred to as) 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.
- Future interoperability standards: Adoption of future interoperability standards seems difficult, if these are getting into too much technical detail. Given the massive rollouts in various technologies make it hard to argue to replace these investments. However, integration of implementations of such standards is rather easy, as the integration of the Belgian or Estonian eID into the Austrian system 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, card reader costs have partly been sponsored by banks and the government.

2.1.3 ***Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 197, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=197

- Web-Site of the case: http://www.buergerkarte.at

2.2 Belgium: Good Practice Case "Belgian Personal Identity Card (BELPIC)"

2.2.1 Case Summary

The ID card of the Belgian citizens who reside on the national territory will become electronic. This means that the citizen will have a secured tool to access the electronic window of his commune.

2.2.2 Further Details of the Case

With the electronic ID card, you will be able:

- to access the records kept by the local authorities about you. For instance, you will be able to consult your own population record or your National Register record on https://www.mondossier.rrn.fgov.be;
- to request on-line documents for which you now have to go to your administration personally and sometimes queue for a considerable time (for instance to obtain a copy of your birth certificate);
- to exchange information on-line with your administration, private companies or organisations through a secured channel. For instance, you will be able to fill in your tax declaration of the natural persons on the internet ("tax-on-web") via www.belgium.be;
- to make statements or transactions (social services, banks, post, insurance) from a distance;
- to get in touch with your municipal authority. Many municipalities have developed a website where all information regarding the services offered is available: library, sports, population, public transport; Several municipalities are already equipped with electronic windows that enable you to make requests by filling in electronic forms. The advantages of using your electronic ID card (electronic identification and signature) will make contacts with your local authority 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 you to contact all other Federal Public Services and to find the information you need to know. You can also consult:
  - the Flemish portal at http://www.vlaanderen.be/
  - the Walloon portal at http://www.wallonie.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 your electronic signature on documents (the electronic signature has the same legal value as a handwritten signature). You will also be able to send electronic messages with a legal signature, to sign contracts on the Internet;
- to use all applications which will be put at your disposal in the future by the State as well as by the private sector. You will be able to make bookings, registrations, payments, to place 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.

*2.2.3 **Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 28, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=28
- Web-Site of the case: http://eid.belgium.be/

2.3 Estonia: Good Practice Case "A Population-Wide ID card (Estonia)"

*2.3.1 **Case Summary***

Estonia has implemented ID card as the primary document for identifying its citizens and alien residents living within the country. The card, besides being a physical identification document, has advanced electronic functions that facilitate secure authentication and legally binding digital signature, in connection with nationwide online services.

The first Estonian ID cards were issued in January 2002. The total number of ID cards issued by September 08, 2006 was 989073 (over 70% of the whole population). These numbers included 231080 cards issued to foreigners.

ID card has two main functions. First, it is very convenient to use it as a regular ID, such as proving your age or identity when paying at a retailer using a bank card, or at a local government office.

The ID card also functions as an electronic identity, enabling one to use services online conveniently and securely. The card is not limited to specific services. Any organization, be it public or private, has the opportunity to "ID enable" its service and thus start serving people online.

One can also use her/his ID card to give digital signatures. According to Estonian law, digital signatures are equivalent to handwritten ones if the systems used to give and process it meet certain regulations.

Each ID card contains various pieces of data, such as the name of card, personal code (national ID code) of the card holder, card holder birth time, citizenship, and other. In addition, the card contains two certificates and their associated private keys protected with PIN codes. The certificates contain only the holder's name and personal code (national ID code). In addition, the authentication certificate contains the holder's unique e-mail address.

The card issuing as well as its further operation is done in close public private partnership. There are three main organizations that are associated with issuing and operating the ID card and the associated infrastructure. The Estonian Citizenship and Migration Board is the government organization responsible for issuing identification documents to Estonian citizens and alien residents. AS Sertifitseerimiskeskus functions as the certification authority, maintains the electronic infrastructure necessary for issuing and using the card, and develops the associated services and software. TRÜB Baltic AS, subsidiary of Swiss TRÜB AG, is the company that personalizes the card.

2.3.2 ***Further Details of the Case***

ID card and the certificates that it holds can be used in all possible applications in public and private sector. This includes both authentication and digital signature applications.

By the end of 2006, over 70% of the population in Estonia has the ID card. A number of applications have already been deployed and the number is increasing. The ID card has become ubiquitous and can be used when communicating with most organizations, be it just for authentication or for full-fledged two-way paperless communication using digital signatures.

During development of the Estonian ID card, the following question arose: for a population-wide ID card, it is necessary to find a good balance between the functionality, privacy, and security. From the functionality viewpoint, it is better to include as much personal and possibly other data on the card as possible. From the privacy and security viewpoints, the amount of data on the card should be minimized. It is also crucial to have the right standards in place.

In the case of the Estonian ID card, the solution is as follows. The ID card contains the holder's surname, given names, sex, citizenship, date of birth, place of birth, personal code, photo, signature, date of issue and date of expiry, and document number. For resident aliens with valid papers, the ID card also contains residence and work permit data. In addition to many security features, the card has a machine-readable code and a chip, an electronic device containing the visual data on the card and two security certificates to verify the individual and supply digital signatures.

The Estonian ID card is used to gain access to a number of Internet-based services, including viewing and changing data in the Estonian Citizenship and Migration Board systems, running queries to the national registers, using the E-Tax Board, gaining access to several banks, giving digital signatures, purchasing and using ID-tickets, and many others.

The main learning points of this case are:

- A nation-wide ID card is feasible, when carefully planned, initiated, deployed, and supported.

- For the card be really used, it is critical to develop useful applications, to stimulate people to purchase equipment, and to educate people to use the applications.

- This experience might be used by other governments when developing their nation-wide ID card infrastructures.

This case became operational on 1st January 2002.

2.3.3 *Further information*

- Good Practice Database of the Good Practice Framework, Use-Case No. 191, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=191
- Web-Site of the case: http://www.id.ee/pages.php/0303

2.4 Finland: Good Practice Case "Katso"

2.4.1 *Case Summary*

Katso system is an identity management, authorization and authentication platform for organizations. Katso system is maintained by government organizations, currently National Board of Taxes and the Social Insurance Institution of Finland. Katso is the first implementation of a large outsourced identity management solution, which is built on the Ubilogin IDM Framework. Katso provides the platform and tools to outsource the identity management of organizations and representatives of organizations to an independent service. It is completely role based and can therefore help government eServices to implement true RBAC services.

2.4.2 *Further Details of the Case*

Government organizations are offering on-line services to organizations and citizens and require strong authentication of users to some of the services, where others require organization level authentication, i.e. a person who is accessing the services are authenticated and authorized as a representative of an organization.

Katso and the associated authentication infrastructure implement international standards in authentication and attribute distribution. Katso and the Ubilogin Authentication Server implement Oasis SAML 2.0 and Liberty ID-WSF 2.0 standards in user authentication and attribute queries.

The Katso system has an enormous user base, as all of the Finnish companies need to have a Katso ID in order to conduct business online with the Finnish board of taxes. This makes Katso one of the largest deployments of outsourced identity management, authentication and attribute distribution solutions in the world. In the months and years to come Katso will be the de-facto identity management solution for all Finnish organizations.

Katso is the enabling platform / program / initiative for identity management, authentication and authorization of businesses and business representatives to eGov services. There are currently a few high volume services utilizing Katso; by the end of 2007 there are estimated 20-30 eGov services are using Katso in various segments of government.

This case became operational on 31st of January 2006.

2.4.3 *Further information*

- Good Practice Database of the Good Practice Framework, Use-Case No. 1966, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=1966
- Web-Site of the case: http://yritys.tunnistus.fi

2.5 Finland: Good Practice Case "Identification Service tunnistus.fi"

2.5.1 *Case Summary*

The identification service tunnistus.fi is co-operated by Tax Administration, Ministry of Labour and the Social Insurance Institution of Finland.

It is an identification service for web services of member organisations (www.tunnistus.fi, only in Finnish and Swedish). The system is using national smart cards and net bank identification. Over 95% of identifications are made by the use of bank IDs.

The use of tunnistus.fi is limited to E-Government only.

2.5.2 *Further Details of the Case*

The identification service tunnistus.fi is co-operated by Tax Administration, Ministry of Labour and the Social Insurance Institution of Finland. It is an identification service for web services of member organisations (www.tunnistus.fi, only in Finnish and Swedish). The system is using national smart cards and net bank identification. Over 95% of identifications are made by the use of bank IDs.

It is a centrally driven e-ID system using identification numbers. The identification numbers used are unique; they are taken from the central resident register and from customer information of banks. The numbers used remain the same throughout a person's lifetime. This identification system is not obligatory and it is limited to E-Government only.

Legal issues:

- In Finland, there are specific regulations regarding electronic authentication enacted:
  - Act of Personal Identification card (Henkilökorttilaki 28.7.1999/829); Personal Data Act (http://www.finlex.fi/en/laki/kaannokset/1999/en19990523).
  - Act on Electronic Signatures is in place.
- Specific regulation: In governmental services for citizens both, national smart cards and net bank IDs can be used.
- The Social Security ID constitutes proof of identity.

- There is a regulation with respect to interoperability with other identity management systems (including through international interoperability agreements) in place.
- A regulatory framework to provide a multi-tiered identification system is in place.

This case became operational on 1st January 2005.

2.5.3 Further information

- Good Practice Database of the Good Practice Framework, Use-Case No. 200, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=200
- Web-Site of the case: http://www.tunnistus.fi

2.6 Hungary: Good Practice Case "Enforcement of e-Government regulations of the new act on administration processes and services – Case 1: Authentication by password"

2.6.1 Case Summary

This is identity management system is used to access and make use of the Hungarian Governmental Gateway.

The person must register before using the central government gateway. During registration the central population register is used for checking purpose 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.

2.6.2 Further Details of the Case

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 person's lifetime, although some personal data may change (e.g. name, E-Mail addresses).
- The following personal data are used: Name(s), Surname(s), Place of Birth, Date of Birth, Parent names, E-Mail addresses
- 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.

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
- The regulative framework provides a multi-tiered identification system. This ID system makes use of username/passwords to authenticate/identify persons. GPF-case #199 describes an analogous system using electronic signatures.

*2.6.3 **Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 198, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=198
- Web-Site of the case: http://www.meh.hu/szervezet/hivatalok/ekk/

2.7 Hungary: Good Practice Case "Enforcement of e-Government regulations of the new act on administration processes and services - Case 2: Authentication by digital certificate"

*2.7.1 **Case Summary***

This is identity management system is used to access and make use of the Hungarian Governmental Gateway.

The person must register before using the central government gateway. During registration the central population register is used for checking purpose and a new entry will be added to the registration database.

The person enters the authority's system using a digital certificate. After identification the authority sends the personal data to the provider of the certificate for authentication purpose.

2.7.2 *Further Details of the Case*

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 person's 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.

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 digital certificates/electronic signatures to authenticate/identify persons. GPF-case #198 describes an analogous system using usernames/password.

2.7.3 *Further information*

- Good Practice Database of the Good Practice Framework, Use-Case No. 199, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=199
- Web-Site of the case: http://www.meh.hu/szervezet/hivatalok/ekk/

2.8 Ireland: Good Practice Case "ePassport"

2.8.1 ***Case Summary***

The development of an e-Passport was a key project for the Irish government, the completion of which had to be met against an aggressive schedule. Under the United States visa waiver programme, participating countries are required to move to full production of biometric passports before 26 October, 2006. This has serious implications for Ireland, which is one of the top 10 visiting nations, with an estimated 500,000 Irish citizens visiting the U.S. last year. The bulk of these visits were visa free.

2.8.2 ***Further Details of the Case***

The project involved creating a new, high-tech passport that includes secure electronic chips to store an encrypted digital version of the holder's identity. Special features of Ireland's new e-Passport include:

- Securely stored biographical information and digital image that are identical to the information that is visually displayed in the passport
- Contactless microchip embedded in the passport that allows the information to be read by special chip readers at a close distance
- Digital signature technology to verify the authenticity of the data stored on the chip, alerting officials if the information has been tampered with

The project involved the modification of Ireland's Automated Passport System (APS) to allow the capture of biometric information from the applicant's photograph, and to ensure this was encoded in the e-Passport document in a secure fashion. The Irish Government also introduced facial recognition technology to coincide with the release of the e-Passport. This technology is used to improve identity verification and reduce identity-related fraud.

The project involved the modification of Ireland's Automated Passport System (APS) to allow the capture of biometric information from the applicant's photograph, and to ensure this was encoded in the e-Passport document in a secure fashion. The Irish Government also introduced facial recognition technology to coincide with the release of the e-Passport. This technology is used to improve identity verification and reduce identity-related fraud.

This project ensures that Ireland's passport document continues to one of the most secure travel documents in the world. In addition, holders of the Irish passport can continue to travel to the US under the visa waiver program.

Key learnings relate to the need to continually test and validate interoperability of the encoded passport with various passport readers to ensure that the documents can be read by border control agencies.

This case became operational on 2nd February 2007.

2.8.3 *Further information*

- Good Practice Database of the Good Practice Framework, Use-Case No. 1968, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=1968
- Web-Site of the case: http://www.dfa.ie/home/index.aspx?id=265

2.9 Italy: Good Practice Case "Carta d'identitá elettronica (CIE)"

2.9.1 *Case Summary*

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 as well 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 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 the emission to all persons living in Italy.

2.9.2 *Further Details of the Case*

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.

The Association of Italian Communes (Associazione Nazionale dei Comuni Italiani - ANCI) has collected experiences and has developed recommendations for the communes. In the first project phases the following problems have been encountered:

- Connectivity to the secure backbone network of the CIE (Sistema di Sicurezza della Carta d'identità Elettronica – SSCE)
- Lack of documentation
- Personal in communes is not trained causing problems with the technology

This case became operational on 19th of July 2000.

*2.9.3 **Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 207, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=207
- Web-Site of the case: http://www.anci.it/cie/

2.10 Malta: Good Practice Case "Malta's electronic identity solution"

*2.10.1 **Case Summary***

The Government of Malta has laid the foundations for the future of a digital world with the introduction of an e-ID system that allows every Maltese citizen and business to have personalized and secure access to data and online Government services after having registered and authenticated themselves once before a third party from the private sector. The latter is entrusted with the issuing of passwords and digital certificates. This administrative process chosen proves, inter alia, to be an outstanding example of how to drive the take-up of online services by reducing scepticism among the general public about online administrative procedures requiring the transmission of personal and sensitive data.

Until security issues are addressed, full development of the information society cannot take place. Recognizing that not all electronic transactions require the same level of security, the Government has ensured that authentication measures are appropriate to the service being provided. Consequently, Government Ministries and/or service providers can now deploy complex transactional electronic services after determining which of the three security levels is best for a given service.

The case also demonstrates that by creating an e-ID solution as a core module of overall e-Government architecture, it is possible to provide a unified authentication method that can be used across the public sector for integrated service delivery. The interoperability and integration capabilities of the technology used thus makes it possible to co-exist with other existing backend systems, resulting in lower application development costs and shorter implementation times.

The e-ID project was led and coordinated by the Ministry for Investment, Industry and Information Technology (MIIIT) and was developed in partnership with Microsoft and Exigy – a

local IT solutions company and Microsoft Certified Partner. It was customized by Malta Technology and Training Services Ltd. (MITTS), the Government IT agency.

Malta is currently looking into the possibility of creating a physically integrated identity smartcard which bridges the e-ID with the physical identity card.

*2.10.2 **Further Details of the Case***

The e-ID is a network key that can be used to securely access data and online services requiring a person's identification. Thus, its main objective is to enable the secure provision of value-added transactional e-Government services while continuing to offer flexibility and convenience to its users.

Moreover, the e-ID solution proposed by Microsoft and Exigy fits squarely with Malta's National ICT Strategy 2004 – 2006 (http://www2.miti.gov.mt/docs/ITStrategy.pdf), more specifically as a tool to reach inter alia the following objectives:

1. Allow citizens and businesses to gain personalized access to online Government services;
2. Increase confidence in the use of technology to interact with public administration;
3. Increase the take-up of online public services that require an authentication procedure;
4. Use ICTs to improve the quality of life of Maltese citizens;
5. Use ICT as an effective management tool within the public sector as an efficiency-realization mechanism and as a vehicle to improve the quality of working life of public employees;
6. Proliferate the delivery of first-class, accessible and secure e-Government services;
7. Act as a guarantee for the identity of local businesses, thus gaining access to the larger global market by participating in the e-Business community;
8. Promote the role and the contribution of the Maltese information society in the global ICT market

The e-ID solution is one of several core horizontal e-Government services, or shared components, that have been created for use across Government. Others include the Government portal, the electronic payment gateway, the central citizen data repository, and the m-Government service. The latter enables mobile phones to be used as an additive service delivery channel. Together with the e-ID, these systems constitute Malta's e-Government platform.

This case became operational on 18th March 2004.

*2.10.3 **Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 153, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=153
- Web-Site of the case: http://europa.eu.int/idabc/en/document/2345/355

2.11 The Netherlands: Good Practice Case "DigiD"

2.11.1 ***Case Summary***

DigiD is an authentication provider for citizens and business interacting with government, for local, regional and central administrations. It verifies the identity of the customer for service providers. It has been made available to citizens since 1 January 2005.

The citizen can register with her social security number (SSN). Legislation has been amended in order to use the administration number (A-number) for identification purposes in case of services for which the SSN - the use of which is strictly limited - is not allowed.

Governments that want to provide services with DigiD as authentication provider are required to do a risk analysis to determine if the level of trust of the method is suitable for the type of service that is provided. In September 2005 the authentication system will become available for B2G communication

2.11.2 ***Further Details of the Case***

The Dutch government initiated the development of digital identities for Dutch e-Government services in the year 2003 by launching the DigiD project. The scope of DigiD is to identify citizens on the internet on the basis on a single identification number. From the organisational perspective, DigiD is a joint project of the Ministry of Internal Affairs and Kingdom Relations, the Ministry of Economic Affairs, the Government ICT Unit), the Dutch Tax Service and a number of other stakeholders.

From a technical point of view, DigiD is a multi level system regarding authentication. It provides three levels of authentication: password based authentication, PKI-based authentication and authentication using existing and trusted infrastructures such as Bankpass Easytrust and PKIO.

In order to identify natural persons DigiD introduces a unique identifier for citizens, the so called Citizen Service Number (CSN). A CSN is assigned to every Dutch citizen; in a first phase of DigiD the CSN is similar to the Dutch social security number which was used to identify citizens in the past. Contrarily to the social security number the Dutch law allows to use the CSN in a broader context. In addition to unique numbers for natural persons, the DigiD project also plans to introduce so called Companies and Institution Numbers (CIN) in order to uniquely identify legal persons.

The architecture of DigiD follows a centralised approach. This means that a service requesting for a citizen's identity will be redirected to a central authentication provider which identifies and authenticates the citizen. In answer to the service's request the authentication provider returns the citizen's attributes.

DigiD provides authentication and identification of natural and legal persons. It is not intended to use DigiD in a commercial context. This means DigiD is currently limited to be used by governmental services only.

This case became operational on 22nd of September 2005.

2.11.3 ***Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 204, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=204

- Web-Site of the case: http://www.digid.nl/

2.12 Slovenia: Good Practice Case "eID Cards for governmental employees"

2.12.1 ***Case Summary***

The scope in the first phase of Slovenia's e-ID programme was to issue e-ID cards to governmental employees only. Each of Slovenia's governmental employees receives an e-ID card which holds two certificates. The first certificates is for personal use and is intended to be used for authentication purposes, to create electronic signatures, for encryption and for secure e-mail services. The second certificate of an employee's e-ID card is a so called web-certificate that the governmental employee might use for secure web communications.

2.12.2 ***Further Details of the Case***

Slovenia identifies natural persons by single unique identifiers. 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; Slovenian abbreviation: EMŠO) . 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.

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.

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

This 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.

E-Identification numbers, a part of the digital certificate, are used for this e-ID system; they are stored also in a governmental database. The unique e-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.

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-Identification number used for this e-ID system is issued only to civil servants.

The 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 e-ID system is not limited to e-government applications only; it can be used for other applications as well.

Legal issues:

The e-ID system is built according to the Slovenian Data Protection Act. An Electronic Commerce and Electronic Signature Act are in place. An Electronic Signature part of the act is entirely in accordance with the EU Directive 1999/93/EC.

The question of authentication is not especially emphasized by law. There is even no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).

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.

This case became operational on 1st January 2002.

*2.12.3 **Further information***

- Good Practice Database of the Good Practice Framework, Use-Case No. 1972, http://www.egov-goodpractice.org/gpd_details.php?&gpdid=1972
- Web-Site of the case: http://www.mju.gov.si/en/

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