# eID Interoperability for PEGS

# NATIONAL PROFILE IRELAND

November 2007

**This report / paper was prepared for the IDABC programme by:**

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

**Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3**

# Disclaimer

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

## Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Irish eGovernment applications.

# Table of Contents

# 1 Documents

## 1.1 Applicable Documents

| [AD1] | Framework Contract ENTR/05/58-SECURITY |
|-------|----------------------------------------|

## 1.2 Reference Documents

| [RD1] | eGovernment in the Member States of the European Union – 5th Edition – May 2006 |
|-------|----------------------------------------|
|       | http://ec.europa.eu/idabc/servlets/Doc?id=24769 |
| [RD2] | European Electronic Signatures Study |
|       | http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl |
| [RD3] | DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures |
|       | http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf |
| [RD4] | Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 |
|       | http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf |
| [RD5] | DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts |
|       | http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf |
| [RD6] | IDABC Work Programme Third Revision |
|       | http://ec.europa.eu/idabc/servlets/Doc?id=25302 |
| [RD7] | DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors |
|       | http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf |

# 2 Glossary

## 2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- o *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- o *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- o *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- o *Authentication*[1]:  the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- o *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- o *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- o *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

---

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

o *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

o *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

o *Advanced electronic signature*: an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

Again, this definition may cover non-PKI solutions.

o *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

o *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

---

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

## 2.2 Acronyms

**A2A**............................................. Administration to Administration

**A2B**............................................. Administration to Businesses

**A2C**............................................. Administration to Citizens

**CA**.............................................. Certification Authority

**CRL**............................................ Certificate Revocation Lists

**CSP**............................................ Certificate Service Provider

**eID** ............................................ Electronic Identity

**eIDM**........................................... Electronic Identity Management

**IAM**............................................ Identity and Authentication Management

**IDM** ........................................... Identity Management

**OCSP**.......................................... Online Certificate Status Protocol

**OTP**............................................ One-Time Password

**PKCS** ......................................... Public-Key Cryptography Standards

**PKI**............................................. Public Key Infrastructure

**SA**.............................................. Supervision Authority

**SOAP** ......................................... Simple Object Access Protocol

**SCVP** .......................................... Server-based Certificate Validation Protocol

**SSCD** .......................................... Secure Signature Creation Device

**USB**............................................ Universal Serial Bus

**TTP**............................................ Trusted Third Party

**XAdES** ........................................ XML Advanced Electronic Signature

**XML** ........................................... eXtensible Markup Language

**XML-DSIG**.................................... XML Digital Signature

# 3 Introduction

## 3.1 General status and most significant eIDM systems

The most significant eIDM system in Ireland is based on the "Personal Public Service" (PPS) number), which is a unique identifier issued to all Irish residents and to other individuals who have had reason to deal with the public services in Ireland.

For Irish residents the number is now allocated at birth. The PPSN, along with a prescribed set of personal data, forms a person's Public Service Identity (PSI). A set of services built upon the PPS number and PSI also allow for the exchange of personal information between government agencies.

Alternative tokens used regularly in Ireland include the Driver's licence, Passport, and other function-specific electronic and paper based certificates issued by both public and private bodies.

Almost 6 million PPS numbers have been issued to date, this equates to roughly 150% of the population. Since 2004 a significant proportion of the numbers issued have been to nationals of EU accession states.

## 3.2 Background and traditional identity resources

### 3.2.1 eGovernment structure

Ireland's first Action Plan for the information society, which was published in January 1999, (Department of the Taoiseach, *Implementing the Information Society in Ireland: An Action Plan*, January 1999) set out a three-stranded approach to online delivery of public services:

- Strand 1 – information services: ensuring all public service information is available online through the websites of Departments and Agencies, and at the same time as it is delivered through traditional channels

- Strand 2 – interactive services: delivery of public services online, enabling complete transactions to be conducted through electronic channels

- Strand 3 – integrated services: rearrangement of information and service delivery around user needs, and available in an integrated manner through a single point of contact with government.

The key developments towards the objectives set out in the first Action Plan as reported in the subsequent Action Plan, *New Connections: A Strategy to Realise the Potential of the Information Society (*Department of the Taoiseach, *New Connections: A Strategy to Realise the Potential of the Information Society*, March, 2002*)* were:

- the development of guidelines and standards for all public sector websites

- the establishment of the Reach Agency in 1999 to develop a strategy for the integration of public services and the implementation of e-government.

– the imposition of a requirement for all government Departments to produce e-strategies for the delivery of public services online, and to report on progress with implementation in their Annual Reports.

In May 2000, Government agreed on the Public Services Broker model as the framework for the integrated delivery of public services through multiple channels, accessible from a single point of contact. This model was to be implemented by the Reach agency. The portal website www.reachservices.ie was established as the public face of the Public Services Broker. It is intended to act as a single point of access to online public services in Ireland. After some delays, Reach completed work on establishing the Public Services Broker in 2005.  In May 2005, an enhanced version of the reachservices portal was launched which allowed for secure registration for online services via the internet.

### 3.2.2  Traditional Identity Resources

Ireland does not have a national identity card, and has never had a population register. The main registers of identities in the country are the Registers of Births, Deaths, and Marriages. These have been interpreted by the Irish High Court as being registers of historical events, and as such are not updated other than to record the occasion of a new birth, death or marriage, or to correct an error of fact that existed at the time the record was originally created.

On the registration of a birth, death or marriage, a paper certificate issues from the office. The certificate relating to the birth of an individual has generally been one of the primary documents used to prove ones identity.

Before 1979, there was no single unique identifier in use in the State. The creation of the "Revenue and Social Insurance" (RSI) number in 1979, and its subsequent development into the PPS number in 1998 has been the main focus for the horizontal integration of government services.

Until 1998, the RSI number, as it then was known, was used primarily for the delivery of social welfare, and for tax collection. In 1997 and subsequent years the purposes for which the number could be used were broadened considerably.[3]

---

[3] It is now used for purposes as diverse as: social welfare, free travel passes for the elderly, student identity, medical cards, and driver testing.

A database of identities linked to the PPS number has been developed for authenticating entities that interact with public services. This is known as the "Public Service Identity" (PSI] database. The information to populate this database was drawn at the first instance from social security records. Since 2004, the PSI database is horizontally integrated with the Register of Births Deaths and Marriages and it is populated by it.

The PSI information is used to populate other function specific databases maintained by individual government agencies. As a result there is a reduced need for entities to resubmit personal information to different agencies.

### 3.2.3  eGovernment and Horizontal Integration

The need a more integrated delivery of public services and the development of a more universal eID system was first considered in a 1996 *"Inter-departmental Report on the Development of an Integrated Social Services System"*. This report suggested the development of a unique identifier, and placed particular emphasis on reducing the need of entities to submit the same information to multiple government agencies.

Since 1997 a legislative framework which facilitates the sharing of personal information has been developed incrementally. Furthermore, an XML-based architecture to enable information sharing, known as the "Public Service Broker" is in place. The front-end for this service is available at www.reachservices.ie. This web service uses the PSI to authenticate identity, and has the potential to allow entities to interact with multiple government agencies using the Public Service Broker as a medium of communication. At present however, only the Revenue Commissioners (Taxation Authority) and the Employment Equality Tribunal use the facility.

### 3.2.4  Non EEA nationals

Section 9 of the Immigration Act 2004 mandates the creation of a register of non-nationals who have permission to be in the country. Following registration with immigration officials, the individual is be issued with an "Immigration Certificate of Registration". which is the size of a credit card and includes the individual's name, address, photograph and residence details. It is sometimes called a "GNIB card" as it is issued by the Garda National Immigration Bureau (GNIB). The non national is obliged to notify any changes which may affect the accuracy of the register within 7 days, while if he or she moves to a different registration district, the registration officer must be notified within 48 hours. Section 9(4) provides that where a non-national who is required to register is lodging or staying in the household of another, it is the duty of the householder to ensure compliance with the Act by reporting the individual. Section 11 of the Immigration Act 2004 provides that it is an offence for any person other than a citizen of Ireland or the UK to enter Ireland without a passport or identity document stating their identity and nationality. Section 12, which essentially reproduces section 15 of the Aliens Order 1946 provides that unless a satisfactory reason for not doing so is provided, a non-national

must produce on demand to a garda or immigration official, a passport or document showing his nationality and identity, and a registration document, if registered or

required to be. The non-production of such identification is a criminal offence and a member of An Garda Síochána may arrest without a warrant someone who is suspected of committing such an offence.

### 3.2.5  Business registers

The Companies Office (www.cro.ie) is responsible for administering the registration of companies registered under the Companies Acts 1963-2005 and business names under the Registration of Business Names Act 1963.

## 3.3  eIDM framework

### 3.3.1  The Personal Public Service Number

Along with provisions relating to the sharing of personal information, the PPS Number was introduced by Part IV of the Social Welfare Act, 1998 to allow "greater efficiency across the public service [and] facilitate the reorganisation and integration of services around the customer".[4] The practical result of the 1998 legislation was to expand the uses for which the pre-existing "Revenue and Social Insurance Number" could be put.

The PPS number consists of seven digits and one letter. Only one number is ever issued to an individual. The only exception to this relates to the now discontinued practice of issuing married women with their husband's PPS number suffixed with the letter "W". Those issued with a "W" number may apply for the number to be changed, or to revert to their pre-marital number.

The PPS number is currently printed on official correspondence from Revenue and Social Welfare offices. The 1998 legislation introducing the number also made provision for the introduction of a "Social Services Card". This was introduced, but does not serve any practical purpose other than as a memorandum of the PPS number. The card is not capable of identifying its holder, nor does it provide any security to the use or misuse of the PPS Number.  The card itself contains:

1. Person's Name
2. PPS Number
3. Primary Account Number (PAN)
4. Date of Issue
5. Encoded on a magnetic strip are the following details:

---

[4] *Dáil Éireann*: Volume 498, Col 1059, 15 December, 1998

    i. Date of Birth

    ii. Gender

    iii. PAN[5]

    iv. Expiry date of card (set artificially to 1999)

    v. Card Service Code.

This card is no longer issued as a matter of course, and will be replaced in the near future by an eID token.

For the most part the PPS number may only be used by government agencies that have legislative permission to do so. Use of the number is described in the Personal Public Service Number Code of Practice[6].

## 3.3.2  The Public Service Identity

The Public Service Identity (PSI) database was established in 2002 as being an authentic source for personal identity information. It contains the following:

1. Surname;
2. Forename;
3. Date of birth;
4. Place of birth;
5. Sex;
6. All former surnames (if any);
7. All former surnames (if any) of his or her mother;
8. Address;
9. Nationality;
10. Date of death (if applicable);
11. If the individual is under 18 the public service identity of his or her father and mother.

The PSI may be accessed by any entity entitled to use the PPS number for the purposes of authentication, or where the information is required in performing their public functions.

---

[5] The PAN comprises firstly, the issuer number allocated by the International Organisation for Standardisation,  secondly, the PPS number, with any letter converted to a digit in the form a=01, and thirdly, the card sequence number.

[6] http://www.welfare.ie/topics/ppsn/cop.html

### 3.3.3  The Public Services Broker

The Public Services Broker (PSB) has as its aim the provision of an integration framework and shared services platform to support the provision of public services.  It comprises two distinct parts:

The user interface is the "Reach Services" website at www.reachservices.ie. The purpose of the website is to provide a "one-stop-shop" for online government services. Upon registration an entity must chose a username and password. In order to use the website to access services electronically, the entity must submit certain personal information, which in turn is authenticated against the PSI. On successful authentication an activation code is posted to the registrants address.

The second element to the PSB is the integration framework . This is an asynchronous messaging hub to which all public bodies may connect in order to share information. Information is shared using standardised XML envelopes. Any agency connected to this central service can exchange data or documents with any other connected agency using the same technology and protocols. It is designed to be a reliable, secure, auditable, and scalable system.

See http://www.reach.ie/government/exchange.html

### 3.3.4  The Public Services Card

A functional specification for a Public Services Card (PSC) has been drawn up, and it is intended that this will be made publicly available along with a request for tenders sometime in late April or early May 2007.

The PSC is likely to use chip-and-pin technology, and it will be used to  authenticating an entity against their Public Service Identity. It will be based on a  "thin client" architecture, whereby data would tend to be stored in back-end systems rather than on the card.

The first application for this token is planned to be the Free Travel Scheme. It is expected to be rolled out in late 2007 or early 2008 and it will have the same approximate dimensions as a bank card. At the outset authentication will be on the basis of information printed on the face of the card, without any electronic input

### 3.3.5  Legal Framework

The first time the RSI number was put on a statutory basis was under Section 23 of the Social Welfare Act 1993, which gave the Minister for Social Welfare the power to issue a "personal social services number" and laid out the identification procedures required before a number be issued. The

RSI number was renamed the "Personal Public Service" (PPS) Number by Part IV of the Social Welfare Act, 1998. The change in name marked a change in the use of the number, from being used only by the Revenue Commissioners and Department of Social Welfare, to being used by public services in general. The current legislative basis of the PPS number is to be found in s.223(2) of the Social Welfare (Consolidation) Act 2005, which provides that "the Minister may allocate and issue a personal public service number to each person who is the subject of a transaction with a specified body". A "specified body" originally consisted of the following: a) a Minister of the Government, b) a local authority, c) a health board, d) the Revenue Commissioners, e) an Foras Áiseanna Saothar, f) An Post, g) An tArdChláraitheoir, h) the Legal Aid Board, and i) An Garda Síochána and Defence forces for their own members.[7] However the concept of a "specified body" has been expanded every year since, except 2001, and it now includes 63 listed bodies, some of which are broadly defined such as "a person who provides, organises or procures a program of education or training".[8] As a result there exist many hundreds of "specified bodies". A complete list of all specified bodies can be found at http://www.welfare.ie/topics/ppsn/cop.html#appbbodies

See further PPS Number - Code of Practice, the purpose of which is to is to promote and facilitate the proper use of the PPS No. in accordance with legislation: http://www.welfare.ie/topics/ppsn/cop.html

The Social Welfare (Miscellaneous Provisions) Act 2002 (Section 12(1)(b)) provided the legal framework for the development of the concept of the "Public Service Identity". Section 262(1) of the Social Welfare (Consolidation) Act 2005 specifies that the Public Service Identity includes the PPS number, and the information below as provided for under s. 262(3):

> (i) Surname;
>
> (ii) Forename;
>
> (iii) Date of birth;
>
> (iv) Place of birth;
>
> (v) Sex;
>
> (vi) All former surnames (if any);
>
> (vii) All former surnames (if any) of his or her mother;
>
> (viii) Address;
>
> (ix) Nationality;
>
> (x) Date of death (if applicable);
>
> (xi) Such other information as prescribed by the Minister as being
>
> relevant and necessary.
>
> (xii) If the individual is under 18 the public service identity of his or
>
> her father and mother.

---

[7] Social Welfare (Consolidation) Act 1993, Section 223(1) as amended by the Social Welfare

Act 1998, Section 14

[8] Social Welfare Act 2000 Section 32(1)(c)(ii)

### 3.3.6 Technical Aspects

As noted above, the Public Service Broker consists of two elements, a web based interface at www.reachservices.ie which allows entities to access public services available online, and the integration framework which assists in data sharing, and in bringing public services together for central access.

The framework is an asynchronous electronic data interchange system using standardised XML envelopes and a separate abstraction layer providing different channels of access to individual data formats such as HTML,J2EE and Microsoft Biztalk. The structure of the XML envelopes is available from http://sdec.reach.ie/.

In 2006, work began on developing a functional specification for an eIDM token known as the "Public Services Card".[9] This work has been completed at the time of writing but the specifications are not as yet available in the public domain.

The eID however is unlikely to provide any service other than authentication via "chip and pin". PKI will not be part of the specification, and, since private entities are not allowed to use the PPS numbers of others for their own purposes, the use of the card in the private sector will be limited.

In the initial phase authentication will be by manual inspection, and the card will contain a number of visual security features. Ultimately it is envisaged that the card may be used for online authentication. A secure biometric may also be available for offline authentication.

### 3.3.7 Organisational Aspects

In order to register with reachservices, an entity must chose a username and password. In order to use the website to access services electronically, the entity must submit certain personal information, which in turn is authenticated against the PSI. On successful authentication an activation code is posted to the registrants address.

### 3.4 Interoperability

---

[9]

http://ted.europa.eu/Exec?DataFlow=ShowPage.dfl&Template=TED/N_one_result_detail_curr.htm&docnumber=150185%202006&docId=150185-2006&StatLang=EN **(http://tinyurl.com/384ls4)**

In terms of national interoperability, guidelines to assist agencies in addressing issues of interoperability have been developed by REACH and are made available on the SDEC (Services and Data Exchange Catalogue) website. We are not aware of any national developments which address the issue of cross-border interoperability.

## 3.5  eIDM Applications

eIDM applications are limited to the public sector.

### 3.5.1  Applications currently available through reachservices include:

a)  PAYE On-Line

This service, which is provided in conjunction with the Revenue Commissioners (Taxation Authority] enables taxpayers to manage their tax affairs through the internet. In order to avail of this service users, as well as registering with reachservices, must use a unique PIN provided to them by the Revenue Commissioners.

b)  Employment Equality Tribunal

Through reachservices it is possible to lodge a complaint of discrimination online.

### 3.5.2  IAMS

IAMS, the Inter-Agency Messaging Service, was developed by the Reach agency to support the electronic exchange of customer data amongst public service agencies. It is currently used to populate the PSI database with information gathered from the Register of Births.

## 3.6  Future Trends/Expectations

### 3.6.1  The Public Services Card

As noted above, a Public Services Card is currently being developed, it is expected that it will be deployed by late 2007 in the form of a Free Travel Pass.

### 3.6.2  New legislation regarding registration of non-EEA nationals

New immigration legislation is under preparation by the Department of Justice. One aspect of the Bill concerns the registration of non-EEA nationals. The draft provision relating to this matter which is contained in the scheme of the Bill published in September 2006 provides for the maintenance of a register of foreign nationals.[10] It requires foreign nationals to supply information including biometric information "to create an accurate entry in the Foreign Nationals Register and to maintain the accuracy of the Register".

## 3.7  Assessment

Use of eIDM systems in Ireland is still at a very early stage of development. At present, no identity card, electronic or otherwise, is in use.  Use of the PPS Number is limited to the public sector and applications involving identification which are based on the PPS Number are very limited. Given the proposals relating to the development of a Public Services Card referred to above, this seems set to change in the not too distant future.

---

[10] Scheme for the Immigration, Residence and Protection Bill, September 2006, Head 28: http://www.justice.ie/80256E010039C5AF/vWeb/fIJUSQ6TDJ3V-en/$File/Scheme.pdf
.