eID Interoperability for PEGS

NATIONAL PROFILE BELGIUM

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 Belgian eGovernment applications.

Table of Contents

EXECUTIVE SUMMARY 3

1 DOCUMENTS 5

1.1 APPLICABLE DOCUMENTS 5

1.2 REFERENCE DOCUMENTS 5

2 GLOSSARY 6

2.1 DEFINITIONS 6

2.2 ACRONYMS 8

3 INTRODUCTION 9

3.1 GENERAL STATUS AND MOST SIGNIFICANT EIDM SYSTEMS 9

3.2 BACKGROUND AND TRADITIONAL IDENTITY RESOURCES 10

3.2.1 EGOVERNMENT STRUCTURE 10

3.2.2 NATIONAL EGOVERNMENT COOPERATION AND COORDINATION 11

3.2.3 TRADITIONAL IDENTITY RESOURCES 12

3.3 EIDM FRAMEWORK 14

3.3.1 MAIN EGOVERNMENT POLICIES WITH REGARD TO EIDM 14

3.3.2 LEGAL FRAMEWORK 21

3.3.3 TECHNICAL ASPECTS 22

3.3.4 ORGANISATIONAL ASPECTS 27

3.4 INTEROPERABILITY 28

3.5 EIDM APPLICATIONS 28

3.5.1 EID CARD APPLICATIONS 28

3.5.2 FEDERAL PAPER TOKEN APPLICATIONS 29

3.5.3 SIS CARD APPLICATIONS 30

3.6 FUTURE TRENDS/EXPECTATIONS 30

3.7 ASSESSMENT 30

3.7.1 ADVANTAGES: 30

3.7.2 DISADVANTAGES: 31

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.

- *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.

- *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.

- *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, …

- *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").

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

- *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.

- *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.

- *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.

- *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.

- *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.

- *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].

- *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 Belgium is based on the Belgian Personal Identity Card (BELPIC), a mandatory electronic identity card that is intended to facilitate access to eGovernment services for all Belgian citizens from the age of 12 and up, as well as offering access to 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). The card contains a chip holding two certificates: one for authentication purposes, and one for qualified signatures.

The system is closely linked to the Belgian National Register (*Rijksregister/Régistre national*), which contains a key set of authentic attributes for all Belgian citizens registered in it. Many of the attributes stored in the authentication certificate of the eID card are obtained directly from the National Register.

The eID card is linked to the National Register through the National Register number, which functions as a unique identifier for Belgian citizens in eGovernment services. Apart from being the main access key to the National Register, this number is also included as a serial number on the certificates of the eID card. The price of the card varies from commune to commune, but generally ranges between 10 and 15 €.

Alternative tokens include the paper federal token which can be issued to certain residents of Belgium (typically because they have not yet been issued an eID card), the social security card (SIS-card), private sector issued certificates (either software certificates or smart card based), and the recently introduced kids-ID, an eID card intended for children under 12. Alternative identifiers include the identity card number and the social security number.

Identification information with regard to legal persons is primarily stored in the so called Crossroads Bank for Enterprises, which identifies legal persons (and natural persons – entrepreneurs) by the so called enterprise number.

All of these systems will be discussed in greater detail below.

From a practical perspective, usage and uptake can be summarised as follows:

eIDM system	Potential user base	Actual penetration	Actual use
National eID card	Estimated at 8 million (around 80% of the population)	5.790.033 on 24 September 2007 (around 58% of the population, and around 72% of the potential user base)	No public statistics are available; see http://map.eid.belgium.be for a list of applications.

Federal paper token[3]	Estimated at 8 million (requires eID card and SIS-card, in principle)[4]	Estimated at 350.000 (around 3.5% of the population, and around 4% of the potential user base)	No public statistics are available (but always limited to eGovernment services)
SIS card	Estimated at 10.5 million	Estimated at 10.5 million (around 101%[5] of the population, and around 100% of the user base; i.e. rollout is complete).	No public statistics are available (but always limited to social security services)

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

Although Belgium is a federal state, the use of eIDM systems in the context of eGovernment is coordinated reasonably well. In the past years, several eGovernment applications have been developed at the federal, regional and local level. eGovernment projects in Belgium are often vertically integrated, i.e. within the same area of competence, such as tax or social security. Nevertheless, steps are being taken towards horizontal integration covering several departments and institutions.

One of the purposes of horizontal integration is to share information so as to avoid requesting it twice from citizens or companies. This is the so-called “authentic source” principle: once information has been requested from the user, it should be stored in a single authentic source. All other eGovernment services are then expected to access the information through the authentic source whenever possible, rather than requesting it multiple times.

EGovernment, in particular horizontal integration, is driven by the following services:

- *Federal eGovernment*

  Federal eGovernment initiatives are lead and coordinated by FedICT, the Federal Public Service for Information and Communication Technology (www.fedict.be).

[3] See http://www.belgium.be/security/nl_BE/application_help/application_help_0334.htm

[4] It is possible to contact FEDICT through servicedesk@fedict.be if an aspiring user does not have one of these cards, but this procedure is rarely used. Since the federal paper token is a temporary solution which will be phased out in the next few years, popularity is unlikely to increase significantly.

[5] The card is also issued to non-Belgians who are subject to the Belgian social insurance system; hence the fact that the actual distribution figure is larger than the Belgian population.

- *Regional eGovernment*

  Regional eGovernment initiatives are lead and coordinated by the respective regional services.
  - CORVE, the coordination service for Flemish eGovernment (http://www.corve.be);
  - EASI, the coordination service for Walloon eGovernment (http://easi.wallonie.be);
  - BRIC, the Brussels Regional Informatics Centre, for the Brussels Capital Region (http://www.bric.irisnet.be/site/en).

- *Local eGovernment*

  Local eGovernment initiatives are lead and coordinated by local authorities, mostly municipalities. For authentication purposes, several municipalities set up an online interactive desk for the provision of eGovernment services. These solutions are developed by private parties, and include iLoket (www.iloket.be), developed by the IT service provider for communes CIPAL (www.cipal.be); eloket offered by CEVI (http://www.cevi.be/); and Digi-Lok, developed by Schaubroeck N.V. (www.schaubroeck.be). These systems rely on the authentication mechanisms offered on a federal level, usually[6] the eID card or token offered by FEDICT (see below for a description of each option). In practice, the user visits the communal website to access a local portal, which verifies the user's credentials through a SAML based framework offered by FEDICT. Upon successful authentication by FEDICT on a federal level, the end user can access the local service.

  Several municipalities encourage secure communication through integration of the e-ID in dedicated or in general standard applications. The Belgian eID card can effectively be combined with the signature modules of some widely used standard Windows applications such as Adobe Acrobat, Microsoft Office or Mozilla Thunderbird, as described below. It is also supported in some Linux distributions (for instance Novell/Suse).[7] Some municipality websites provide practical guidelines on how to use these authentication mechanisms. E.g. the commune of Bornem provides services using the Digi-Lok platform[8], whereas the commune of Diepenbeek relies on iLoket[9].

3.2.2 National eGovernment cooperation and coordination

The need for integrated cooperation between the various levels was laid down in an agreement between federal, regional and communal authorities. This agreement stresses the need for a strong legal framework and interoperability framework at the organisational, semantic and technical level. For the area of electronic signatures, essential requirements must be met to avoid isolated use of a signature solution and to increase trust in the signature.

---

[6] iLoket supports both the federal token and the eID card; whereas Digi-Lok supports only the eID card. See http://www.eid-shop.be/index.php?page=eidready

[7] http://www.novell.com/products/linuxpackages/suselinux/e-ID-belgium.html

[8] See http://www.bornem.be/h111wlbb201hj.aspx

[9] See http://diepenbeek.iloket.be/

In the light of the interoperability framework, a special website dedicated to interoperability in the context of eGovernment and the information society was set up (www.belgif.be). This framework is compatible with the European Interoperability Framework (EIF). As follows from the BELGIF website, the rules, agreements and recommendations that make part of the Belgian interoperability strategy are regularly updated and are open to external contributions. As far as eIDM is concerned, ongoing efforts are currently focused on the adoption of internationally accepted standards and protocols, including LDAP, SAML and Kerberos[10]. Given that the key infrastructure has already been put in place, it is uncertain if these activities will have any significant impact.

As described above, most eIDM systems in eGovernment applications have been designed at the federal level, through two common frameworks:

1) for trust links: direct authentic sources access (LDAP being one of the possibilities);

2) for untrusted links: indirect links thanks to SAML authentication.

As a result, internal Belgian interoperability difficulties are few.

3.2.3 Traditional identity resources

Identification towards Belgian eGovernment services traditionally relied mostly on the combination of the National Register, the creation of which began in 1963 and was completed by 1983, and the mandatory paper based identity card, introduced during the German occupation in World War I. The National Register is a national database which is kept up to date based on registers managed at the commune level.

Each commune maintains both a population register[11] and a non-nationals register (which respectively contain identification data of Belgian citizens and of natural persons without the Belgian nationality who have been mandated to remain within Belgian borders) and a waiting register (for non-Belgian natural persons who have not (yet) been mandated to remain within Belgian borders; i.e. (candidate-)refugees; operational since 1995). It is the communes who maintain the contents of these registers, by updating them when changes are notified to them. Persons are first entered into these databases depending on their status, but the most common possibilities include registration at birth, naturalisation or asylum requests and/or decisions (which are reported to the communes by the competent authorities), and official notifications of changes of domicile by the person involved at his commune.

Persons registered in the population register (i.e. Belgian citizens and non-nationals mandated to reside in Belgium) are issued an identity card. Depending on the case, this card would be an 'identity

[10] See http://www.belgif.be/index.php/Authentication/authorization

[11] Dating back to Napoleontic times, initially regulated by the decree of 7 messidor of year II (i.e. 25 June 1794).

card' (Belgian citizens), 'residence card for non-nationals' (non-nationals with an E.U./E.E.R. nationality), or 'identity card for non-nationals' (other non-nationals).

The identity card contains a number of data printed on it, specifically: last name, first name(s)[12], nationality, date and place of birth, gender, place of issuance of the card, validity period of the card, title and number of the card, picture of the bearer, official residence[13], and National Register number. The card is mandatory, and is issued to any child in the population/non-national register from the age of 12. It remains valid for a period of five years[14].

Residence cards for non-nationals (the so-called 'blue cards'[15]) and identity cards for non-nationals (the so-called 'yellow cards'[16]) are similar, containing largely the same data. Finally, persons in the waiting registers are issued so-called 'white cards'[17].

The National Register contains information for all persons included in the population registers, the non-nationals registers and the waiting registers[18]. For each of these persons, the National Register contains: last and first names, date and place of birth, gender, nationality, main place of residence, place and date of death, occupation, marital status, family composition, source register, administrative status of persons in the waiting register[19], reference to eID card certificates (if applicable)[20], and legal cohabitation[21]. Any changes to this information must be notified from the date from which it has legal effect. Information is kept until 30 years after the date of death. Access to the information in the National Register is obviously restricted.

Information regarding legal entities was traditionally kept in trade registers, which were maintained at the tribunals of commerce in the regions where the legal persons were established, and since 2003 in the National Register for legal persons. While the data held in these registers varied depending on the type of legal entity, it generally contained the information of acts which were published in the Official Journal (i.e. which were publicly accessible). In 2003, these various registers were bundled in the so-called Crossroads Bank for Enterprises (see below).

---

[12] Specifically, the two first names and the initial of any third first name (e.g. 'John William S.'); although the use of multiple first names has somewhat grown out of fashion in the last decades.

[13] This latter bit of information has been intentionally omitted from the eID card, as will be explained below.

[14] In fact, the uniform five year duration was introduced along with the eID card. Traditionally, duration could vary depending on the likelihood of the bearer's appearance changing significantly (i.e. the card of older people could be valid for much longer than that of younger persons).

[15] See http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=770#

[16] See http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=723#

[17] See http://www.vmc.be/vreemdelingenrecht/wegwijs.aspx?id=712#

[18] Also, there are separate registers held in diplomatic missions and consular posts abroad, which are also included in the National Register.

[19] E.g. asylum requested, asylum rejected – appeal pending, etc.

[20] This provision was obviously introduced after the introduction of eID cards.

[21] A legal alternative to traditional marital relationships with a more restricted scope.

Summarily, the Crossroads Bank contains information on all legal persons established under Belgian law or having an establishment or requirement to register in Belgium, as well as natural persons who are independently professionally active as entrepreneurs. Given this diversity of subjects, the registered information also varies, but it generally includes the name, place of establishment, legal form (in case of legal persons), legal status[22], date of establishment, management and mandatories, economical activity by NACE-code, and any other legally required identification data and/or permits.

Thus, the traditional identity infrastructure can be said to consist of centrally kept but locally maintained paper registers for natural persons and legal persons, and of an identity card to certain natural persons.

It is interesting to note that regional governments use a so called Enriched National Register and an Enriched Crossroads bank for enterprises, linking the basic information of the original databases to any relevant information being held with regard to the entities concerned on a regional level.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

The eID card

The Belgian Council of Ministers decided in July 2001 to introduce an electronic identity card, to be issued to every Belgian citizen over the age of 12, as a replacement of the traditional mandatory paper eID card which had been in vogue before.

Deployment of this card has commenced in the second half of 2003, and presently around 4.5 million cards have been issued[23]. Cards are issued by the communes, both by issuing them to 12-year olds who are required to obtain their first card, and to older citizens who are replacing their traditional card. The price of the card is determined locally by the communes, but generally costs between 10 and 15 EUR. Roll-out is expected to be completed by early 2009.

The card has the dimensions of a bank card, and contains all identity data that was printed on the traditional identity card (see above), both printed on the eID card and integrated electronically on a chip. The exception is the holder's address, which is only stored electronically, but not printed on the card, because of its inherently changeable nature which would require the cards to be updated too frequently, thus needlessly increasing costs[24].

[22] This includes e.g. state of bankruptcy or being wound up.

[23] For up to date statistics, visit http://godot.be/eidgraphs or http://eid.belgium.be.

[24] This has resulted in the temporary problem that card holders' official address can no longer be verified by simply looking at the card, which has caused difficulties to law enforcement. This problem was solved in a rather makeshift manner, by issuing a paper statement declaring the official address when the eID card is

The chip also contains two certificates, allowing the authentication of the citizen and the use of a qualified electronic signature[25]. One specific goal was to improve government efficiency, since electronic authentication would allow the government to automatically retrieve the electronic information about the holder that it already has, thus reducing data redundancy and 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).

It should be noted that, while the signature certificate is considered to be qualified, the authentication certificate has emphatically not been given this label. This choice was justified by concerns of legal certainty: the authentication certificate should not be used for signature purposes, and for this reason only the signature certificate is considered qualified. This way, parties are expected to take adequate precautions to ensure that the authentication certificate is not misused.

It should also be noted that the certificates on the eID card are not activated automatically. When the card is issued, the receiver may also opt to leave them inactive, so that the card can only be used as a traditional paper ID card. Obviously, in this case the card offers no eIDM functionality to the holder.

Since the general eID card is only issued to Belgian citizens and non-nationals mandated to reside in Belgium over the age of 12, there is obviously quite a large community that is ineligible for this specific solution. The Belgian government is therefore working on a number of other eID card solutions, including:

- the recently introduced Kids-ID[26] pilot. An entirely optional paper ID card for children under the age of 12 (mostly issued for identification purposes abroad) has existed for some time, and since late 2006 the Kids-ID can be issued to this same group in a number of pilot communes[27]. Its size, appearance and contents are largely similar to that of the general eID card[28], with the noteworthy difference that the chip contains only an authentication certificate, but not a signature certificate (as the legal value of signatures of children under the ages of 12 is generally considered to be negligible). This certificate can only be activated when the child has reached the age of six. In addition to the traditional function of identification abroad[29], the main purpose of this card was to allow children secure access to services intended solely for their age group (e.g. children's chatrooms), and to familiarise them with the technology. The card automatically becomes null and void when the child reaches the age of 12.

handed out. This requires card holders to also keep this (A4 sized) declaration with them at all times; an obligation which is largely ignored in practice. This problem will likely be overcome

[25] It should be noted that the signature certificate is automatically revoked at the time of issuing when the receiver is less than 18 years old, as stated in Certiposts CPS, since the signature of underage persons was considered of limited legal value.

[26] See http://eid.belgium.be/nl/navigation/documents/42993.html

[27] Stated here: http://eid.belgium.be/nl/navigation/42915/index.html

[28] See http://eid.belgium.be/nl/navigation/43038/index.html

[29] The Kids-ID is accepted as an identity document in all Member States, except Slovakia.

- Secondly, a pilot has been initiated in early 2007 in three communes[30] to issue electronic foreigners cards, which will replace the traditional blue, yellow and white cards[31] (for persons ages 12 and up). Size, appearance and contents will be largely similar to that of the general eID card, and the cards will contain both certificates for authentication and for signatures. The main goal of the project is to improve security, eliminate inequality between nationals and non-national, and improve administrative efficiency. If successful, the pilot will be extended to all of Belgium by the end of 2007.

Thus, the main groups excluded from eID holdership will be visitors/tourists, and persons residing illegally in Belgium.

The paper federal token

Most people use the authentication and signature features of their eID card. However, the declaration can also be done by using a special key and token card, to be obtained from the federal government by registering via the federal portal website (www.belgium.be). Obviously, this system is not mandatory.

This federal token is a small paper card with 24 personal codes, which was put into use before the launch of the eID card. Registration is typically[32] done on the basis of the identity card number, the national registry number and the social security card number. The card is then sent to the applicant's official address, as noted in the National Register, by regular mail.

From a practical perspective, the user can authenticate himself with this paper token in a number of applications (e.g. electronic income tax declarations[33]) by two-factor authentication: the user enters his chosen username and password, and the system prompts him for one of the 24 personal codes on the token. If successful, the user can enter the system and conduct his business. It should be noted that the federal token can only be used to push information (e.g., the tax declaration application Taxonweb is accessible both via federal token and eID card, but the first only allows you to push/submit your declaration, while the second also allows you to review previous declarations.

Where interoperability is concerned, the federal token is particularly interesting for people who are not yet in the possession of an e-ID but want to obtain access to secured online services. However, the token also presents certain limitations, specifically with regard to the user group (which only covers natural persons who possess the three numbers needed to acquire a token, thus excluding legal entities and certain non-nationals, namely those who have no national identity card and can thus not present an identity card number). As a result, for users outside of this group the system is presently not accessible. Furthermore, security could be a concern when using the token, since no physical identification of the requesting party is made.

[30] Antwerp, Tubeke, and Uccle.

[31] See http://www.dofi.fgov.be/nl/1024/frame.htm

[32] Certain exceptions exist (e.g. when a potential users does not have the required numbers, but does have a passport); but in those cases face to face registration is required.

[33] See www.taxonweb.be

It seems likely that, given the new initiatives for additional eID cards explained above, the federal token will be phased out in the relatively short term.

The SIS-card[34]

Prior to the introduction of the national eID card, roll-out of the so called Social Information System (SIS) Card was concluded in 1998. The SIS card is a memory card with a bank card format, similar to the generic eID card but without a photo of the bearer. It is mandatory, and the card is issued by any insurance fund to any person subject to the Belgian health care regime, starting at birth (i.e. including employees, the self employed, unemployed, children, public officials,…) and regardless of nationality.

The following information is printed visibly on the card: the national register number, last name and two first names, date of birth, gender, SIS card number, and expiry date of the card.

The chip on the card contains the same information in encrypted form, as well as the health insurance fund (by identification number of the fund and of the holder within this fund) and medical benefit information (i.e. social insurance status (e.g. employee, self employed,…) which determines the refund rate for specific medication.

The card is used by health professionals, specifically by hospitals, doctors and pharmacists, to verify the public medical insurance status (i.e., it contains administrative data, but not actual health information). This requires a specific reader[35], which is only issued to mandated persons and organisations, and a specific card (the SAM card) to decrypt the information stored on SIS cards.. The card is not secured with a specific PIN-code, since the information can only be read through those readers in combination with a SAM card.

Other systems

Three specific systems need to be mentioned further, since they form the backbone of a substantial number of e-government applications: the crossroads bank for social security, the crossroads bank for enterprises, and the Bis-register. Finally, the Limosa-project will also be discussed. This is a recently initiated project aiming to register foreign enterprises and foreign workers who are temporarily professionally active in Belgium, and who are not included in any other registers.

Crossroads bank for social security[36]

[34] See http://ksz-bcss.fgov.be/nl/carteSIS/Sis_home.htm

[35] For specifications, see http://ksz-bcss.fgov.be/nl/documentation/document_3.htm

[36] See http://ksz-bcss.fgov.be/En/CBSS.htm

The Crossroads Bank for Social Security (CBSS) was created 15 years ago as a way of improving the efficiency of Belgian social security organisations and to streamline services to the affected users. The key notion to understand is that this crossroad bank is not an official register in the strict sense (i.e. a container of attributes for a specific set of entities). Rather, the crossroad bank is a reference repertory in the form of a relational database, which can refer to the authentic source for any given piece of data, but which does not contain any data about the subjects itself. Thus, it minimises data redundancy (by retaining only one authentic source for any information) and improves efficiency (since this information can be located directly through the crossroads bank).

By automating information transfers between decentralised service providers, this goal could be achieved without impairing privacy by collecting all information in a gigantic central database. Information exchanges between the databases of social security organisations are strictly regulated, and are only possible after obtaining an appropriate mandate to do so by law[37], or by the sector committee of social security, a committee within the Belgian Privacy Commission[38].

As a practical necessity of the Crossroads bank, the so called 'Bisregister of the Crossroads bank of social security' was created, as an alternative database for anyone who is not entered in the National Register, but who is none the less subject to Belgian social security regulations. This alternative database contains a minimal identification dataset, consisting of the Crossroads bank number, first and last name(s), place and date of birth, gender, nationality, official address and invoicing address, place and date of death, and marital status. The information is first registered when one becomes subject to Belgian social security by the entity who is personally confronted with the new subject, and is thereafter kept up to date by the institutions of the social security. As a consequences, all persons in the Bisregister can also take advantage of social security services, even if they are not entered in the National Register.

Crossroads bank for enterprises[39]

Despite the similar names, the Crossroads bank for enterprises functions in a very different way, since it actually materially contains all basic information regarding enterprises, entrepreneurs (natural persons) and their establishments exercising an economic activity in Belgium (i.e. it is not purely a reference database to other databases). This basic information includes the official denomination, legal form in case of legal persons, legal status (e.g. normal, bankruptcy,…), fields of activity (based on NACE code), certain financial information and local establishments[40].

[37] Specifically the Law of 15 January 1990 establishing and organising a Crossroads Bank of social security. See http://www.juridat.be/cgi_loi/loi_a.pl?language=nl&caller=list&cn=2000102040&la=n&fromtab=wet&sql=dt='wet'&tri=dd+as+rank&rech=1&numero=1

[38] See http://www.privacycommission.be/machtigingen/Sociale_zekerheid.htm

[39] See http://mineco.fgov.be/enterprises/crossroads_bank/home_nl.htm

[40] For a full list of possible attributes and their acceptable values, see http://mineco.fgov.be/enterprises/crossroads_bank/bce_kbo_nl.htm

All entities in the Crossroads Bank for Enterprises are identified through a so called Enterprise Number, which replaced a series of older unique identifiers, including the VAT number and the National Register of legal persons number[41]. A publicly accessible application[42] allows one to find basic identification information based on the Enterprise Number (or inversely, to find the Enterprise Number based on certain information, such as the name of the undertaking).

The Crossroads Bank provides access to information held in the National Register of legal persons, the trade register, VAT registers, and social security registers. As with the Crossroads Bank for social security, information in these registers is maintained by the institutions that have traditionally been competent[43], and access to the Crossroads Bank is only possible after obtaining an appropriate mandate to do so by law[44], or by the sector committee of enterprises, a committee within the Belgian Privacy Commission[45]. Entities are registered in these databases through the so called enterprise counters (*ondernemingsloket/guichet d'entreprise*), non profit organisations which have been accredited to assist entrepreneurs in the establishment of new undertakings.

From a technical perspective, the Crossroads Banks operate over a closed internal network called FedMAN[46], using a specifically developed Universal Messaging Engine[47].

As has already been mentioned above, it is interesting to note that regional governments used a so called Enriched Crossroads bank for enterprises, containing the basic information of the Crossroads bank as well as any relevant information being held with regard to the entities concerned on a regional level.

Limosa

---

[41] For enterprises which had been established prior to the Crossroads bank, the conversion of numbers is in fact trivial: an old VAT number (e.g. 499.999.960) or an old national register of legal persons number; (e.g. 399.999.987) is now lead by a zero (i.e. respectively 0499.999.960 and 0399.999.987).

[42] The so called Public Search; see http://kbo-bce-ps.mineco.fgov.be/ps/kbo_ps/kbo_search.jsp?lang=nl&dest=ST

[43] This includes specifically the federal public services of Finance (for VAT registers), Social Security (for social security registers), Justice (trade registers held at the tribunals of commerce) and the enterprise counters (see main text).

[44] Specifically the Law of 16 January 2003 establishing a Crossroads Bank of Enterprises, modernising the trade register, establishing accredited enterprise counters and pertaining to diverse other provisions. See http://mineco.fgov.be/enterprises/crossroads_bank/pdf/law_BCE-KBO_nl_001.pdf

[45] See http://www.privacycommission.be/machtigingen/kruispuntbank%20van%20odernemingen.htm

[46] See http://www.belgium.be/eportal/application?origin=navigationBanner.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=5930

[47] See http://www.belgium.be/eportal/application?origin=navigationBanner.jsp&event=bea.portal.framework.internal.refresh&pageid=indexPage&navId=5937

Finally, the Limosa project[48] was recently initiated, aiming to register foreign companies, organisations or self-employed persons wishing to employ someone in Belgium, or wishing to establish themselves in Belgium in order to pursue a temporary or partial activity as a self-employed person. For persons already registered in a Belgian official register, there was already a requirement to register such changes electronically using the so called Dimona application[49]. However, for other persons (natural or legal) who are not subject to Belgian social security, this obviously presents a problem if no prior entry in an official register exists.

For this reason, the Limosa application was created (although it is not yet active at the time of writing), which requires temporary/partial employees to register electronically before they can begin any professional activities[50]. The declaration must be done by the employer or organisation that sends somebody to Belgium, or by the person himself if he is self-employed and coming to work temporarily/partially in Belgium. After an electronic registration process, the person receives a username and password which can be used to electronically declare the activity, after which a so called Limosa-1-certificate is issued electronically. This certificate must be printed out and carried at all times by the foreign worker in Belgium. Furthermore, the Belgian client is legally required to check this certificate. At the time of writing, the application is not yet operational, although this will likely happen soon.

Limosa is the first electronic registration system for foreign workers in Europe, and it is hoped that the system could serve as a model for a pan-European solution.

Authentication policies

There is no official authentication policy in Belgium that defines a strict hierarchy of the different authentication systems in use. However, unofficial declarations[51] show that there is a certain hierarchy which functions as a theoretical model for assessing authentication requirements. With regard to natural persons, the following hierarchy is occasionally presented[52]:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line by entering the national register number, identity card number and SIS card number	By assigned user number in combination with a password chosen by the user	Information/services of limited sensitivity

[48] See www.limosa.be

[49] See https://www.socialsecurity.be/site_nl/Applics/dimona/index.htm

[50] See also http://www.law.kuleuven.ac.be/icri/frobben/presentations/20070212.pdf

[51] See e.g. the following presentation (in Dutch): http://www.law.kuleuven.ac.be/icri/frobben/presentations/20061108.ppt

[52] Translated from the original Dutch presentation referred to directly above, slide 10.

2	Level 1 + send-out of a confirmation e-mail with activation URL to an address indicated by the citizen, and send-out of a paper token to the registered address noted in the National Register	Level 1 + entering one random letter sequence mentioned on the token (which contains 24 sequences)	Information/services of average sensitivity
3	Physical identification at the commune for the acquisition of an eID	Authentication certificate on the eID + session based password	Information/services of high sensitivity
4	Physical identification at the commune for the acquisition of an eID	Authentication certificate on the eID + signature certificate on the eID + password per transaction	Services requiring an electronic signature

Thus, there are four levels of authentication above public access: basic username/password (after registration using official register numbers), use of the aforementioned federal token, use of the eID card's authentication, and use of the eID card's signature and authentication.

It should be noted that, since the token will be phased out, in the future the eID will become the main tool for authentication.

3.3.2 Legal framework

The main legal framework for the eID card is laid down in:

- the Law of 19 July 1991 regarding the population registers and identity cards, which is the basic legal source
- the Royal decree of 25 March 2003 on identity cards, which introduced the basic provisions (including form aspects) with regard to the eID card;
- the Law of 25 March 2003 modifying the law of 8 August 1983 establishing a National Register of natural persons and the law of 19 July 1991 regarding the population registers and identity cards and modifying the law of 8 August 1983 establishing a National Register of natural persons, which modernised these existing registers, in particular with a view of using them as an authentic source for electronic identity data;
- the Royal Decree of 5 June 2004 establishing a system of rights of access to and correction of the information which is electronically stored on the identity card and of the information stored in the population registers or in the National Register of natural persons
- the Royal Decree of 1 September 2004 related to the general introduction of the electronic identity card, through which the roll-out was extended outside of pilot communes.

Other relevant legislation includes:

- the Law of 16 January 2003 establishing a Crossroads Bank of Enterprises, modernising the trade register, establishing accredited enterprise counters and pertaining to diverse other provisions;
- the Law of 15 January 1990 establishing and organising a Crossroads Bank of social security.
- the Law of 9 July 2001 establishing certain with regard to the legal framework for electronic signatures and certification service providers.

It should be noted though that Belgium has no specific regulations with regard to the process of authentication in general. The e-Signatures law of 9 July 2001 faithfully transposes the provisions of the e-Signatures Directive, but does not apply to authentication as such.

As described elsewhere in detail, the main eIDM system for the general public is the eID card, which is mandatory for citizens over the age of 12. While its authentication functionality is presently still mainly used for public sector purposes, it is open for private sector uptake.

The main restriction in this regard is that eGovernment applications largely depend on the National Register for their functionality, using the National Register number as a unique identifier. However, the use of this number (as well as access to the National Register itself) is restricted by the Law of 19 July 1991. As a result, private partners can use the authentication framework offered free of charge by FEDICT (which is sufficient for authentication purposes), but they may not access the National Register themselves, or use the National Register number for internal information management, unless they have received a separate mandate to do so by law or by virtue of the sector committee of the National Register, a division of the Belgian Privacy Commission[53].

3.3.3 Technical aspects

The eID card is the dominant eID token in Belgium at this time, and will continue to be for the foreseeable future.

As stated above, the eID card is based on PKI technology, and incorporates two certificates: one for authentication, and one for electronic signatures, with only the latter being considered as qualified. 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 a so called 'local registration authority' on behalf of the National Register, which is the formal registration authority and provides the actual information to be included on the card), and has a validity of 5 years. The cards are produced, initialised and personalised by private company ZETES (http://www.zetes.com), the card manufacturer 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, with Certipost (a joint venture of Belgacom and the Belgian Post, www.certipost.be) acting as the CSP.

The identity card itself is an Axalto (ex-Schlumberger) Cryptoflex JavaCard 32K, equipped with a 16 bit microcontroller (Infineon SLE66CX322P) and an additional crypto processor (for RSA and DES computations). The card has ROM, EEPROM and RAM. A Java Applet handles all communications

[53] See http://www.privacycommission.be/machtigingen/Rijksregister.htm

with the outside world, through the interfaces described below. The chip contains two PKI key pairs and certificates (respectively for the purposes of authentication and signature, no encryption key) and one PKI key pair for the card itself (without certificate).

Where specific hardware is concerned, the card can be read by a wide range of card readers. The government publishes a website with a catalogue of various types of smartcard readers that can be used in combination with the e-ID (http://www.cardreaders.be/en/default.htm).

Specific middleware intended to be used together with the card has been developed for the Belgian government by Zetes. The source code has been made publicly accessible on http://www.belgium.be/zip/middleware_source_code_nl.html.

It is this middleware which constitutes the key interface for most eGovernment applications. It is implemented into each specific application by bridging between the application itself and the device actually performing the cryptographic operations (the e-ID card, in conjunction with the compatible card readers described above). It consists out of two independent interface implementations.

For Microsoft® standard applications, a so-called Cryptographic Service Provider (CSP) is created that implements the cryptographic operations from the smartcard. An application calls this implementation through a standard interface called Crypto API. This API enables application developers to add authentication, encoding, and encryption to their Win32®-based applications. Application developers can use functions in the CryptoAPI without knowing anything about the underlying implementation, in much the same way as they can use a graphics library without knowing anything about the particular graphics hardware configuration. The CSP part of the middleware establishes the link between the abstract CryptoAPI and the underlying PKCS#11 interface. The developer will never call any of the functions of the CSP directly, but only through the CryptoAPI.

Although the CSP only supports digital signatures, it is still registered as a PROV_RSA_FULL type of CSP. This is done in order to allow the usage of the CSP in standard Microsoft® applications. Calling Crypto API functions that are not used in a digital signature context will result in a returned error value indicating that the API function is not implemented.

Secondly, typically in non-Microsoft applications, the PKCS#11 (v2.11) interface is used. Custom applications can also make use of this interface instead of the CryptoAPI interface. The PKCS#11 interface is sometimes also called Cryptoki. A detailed description of this interface can be found on the website of RSA Laboratories (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/).

During the authentication process, the underlying library itself will show a GUI to either ask the user to enter her PIN. Noteworthy is that the Belgian e-ID card currently uses one PIN for accessing the authentication and the signature key.

An e-ID application development kit is available at http://www.belgium.be/zip/e-ID_datacapture_nl.html. Development cards that are functionally equivalent with true e-ID cards can be ordered via “the e-ID shop” of the e-ID project partners Zetes and Certipost (http://www.e-ID-shop.be/).

The certificates on the e-ID are issued by Certipost acting under the name of "Citizen CA" (or "Foreigners CA" when issuing certificates to be stored in resident cards held by foreigners living in Belgium). The certificates follow the X509v3 standard. More details on the certificates and the CSP can be found on the CA's website: http://repository.eID.belgium.be/

The description of the fields of the authentication certificate is contained[54] in the table below[55]:

eID citizen Authentication Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the RRN	Dynamic
Signature		X		Sha-1WithRSAEncryption	
Validity					
NotBefore		X		Key Generation Process Date	
NotAfter		X		Certificates issued before 5th of June 2005: Key Generation Process Date + 5 years[13] Certificates issued after 5th of June 2005: Key Generation Process Date + 5 years and 3 months[13]	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
CountryName	{ id-at-6 }	X		BE	Fixed
CommonName	{ id-at-3 }	X		Citizen CA	Fixed
SerialNumber		X		Certificates issued before 5th of June 2005: N/a Certificates issued after 5th of June 2005: <yyyy><ss>[14]	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by RRN	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of first given name, surname and certificate purpose between brackets	Dynamic
Surname	{ id-at-4 }		YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }		NO	optionally provided by RRN (0, 1 or 2 given names)	Dynamic
serialNumber	{ id-at-5 }		YES	provided by RRN (11 Digits numeric value)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	

[54] Note: in the table below, RRN stands for 'Rijksregister – Régistre National', or National Register.

[55] See http://repository.eid.belgium.be/NL/downloads/Citizen/CPS_CitizenCA.pdf

policyIdentifier		X		2.16.56.1.1.1.2.2	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
					Fixed
Qualifier		X		http://repository.eid.belgium.be	Fixed
KeyUsage	{id-ce 15}	X	TRUE	N/a	
digitalSignature				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		Certificates issued before April 2004: http://crl.eid.belgium.be/eidc0001.crl http://crl.eid.belgium.be/eidc0002.crl Certificates issued after April 2004 and before the 5th of June 2005: http://crl.eid.belgium.be/eidc2004-1.crl Certificates issued after 5th of June 2005: http://crl.eid.belgium.be/eidc<yyyy><ss>15.crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sslClient - smime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			
accessLocation		X		http://certs.eid.belgium.be/belgiumrs.crt – Points to RootSigned Belgium Root CA.	
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://ocsp.eid.belgium.be	

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, as will be discussed below.

Since almost all authentication applications in the Belgian eGovernment sector are making use of the Belgian electronic identity card (and this number will only increase in the future), it suffices to a large extent to describe how the authentication function has been conceived in order to understand each of the separate applications in which this function has been included.

The e-ID Citizen CA belongs to a broader domain of CAs of the Belgian State. The Belgian State has set up a CA hierarchy with a Belgium Root CA (BRCA) at the top, for which FEDICT acts as the CSP. The BRCA has certified the private keys of the CAs in the government domain including the e-ID Citizen CA. The reference certificates used in the Belgian e-ID card certificate hierarchy are provided at http://certs.eID.belgium.be.

At the top the e-ID hierarchy consists of a combination of a two-layered and a three-layered model.

In the two-layered model the eID Citizen CA and the Self-Signed Belgium Root CA form a hierarchy, which in an off-line mode allows validating the eID Citizen signing and authentication certificates. In this model the key of the Belgium Root CA is self-signed. In that case the party that performs the validation can use the Self-Signed BRCA certificate from its own eID card, and use it to validate the eID Citizen CA certificate and e-ID citizen certificates from the card to be validated.

In the three-layered model the e-ID Citizen CA, the Root signed Belgium Root CA and the GlobalSign Root CA form a hierarchy. In this model the same private key as used for the Self-Signed Belgium Root CA is this time certified by the GlobalSign Root CA. This approach allows the automated validation of electronic signatures within the most widely used applications that rely on web interfaces, because most browsers have already embedded the GlobalSign Top Root CA certificate and list it as a trusted one. Just as the e-ID Citizen CA inherits trust from the BRCA, the BRCA inherits trust from the GlobalSign Root CA. This three-layered model eliminates the need to individually import the Self Signed Belgium Root CA certificate.

Because both the Self-Signed Belgium Root CA and the Belgium root signed Top Root CA share the same key pair (albeit using two different certificates), a certificate signed by the private key of that key pair can be validated with both Belgium Root certificates.

In most case the application builder will have foreseen one of both models to be used, and the end user will not have to choose between the two models. More details are available on the website of the Belgian Root CA: https://stage-pki.belgium.be/

More technical details about other aspects of the Belgian e-ID can be found on two webportals of the Belgian federal government:

- http://www.rijksregister.fgov.be/cie_fr/cdocu.htm (website of the National Register)
- http://e-ID.belgium.be/fr/navigation/12000/index.html (website of the Federal Public Service for ICT).

For the validation of electronic signatures created by means of the e-ID both Certificate Revocation Lists (CRLs and delta CRLs) or the Online Certificate Status Protocol (OCSP) can be used, in addition to a simple web interface:

- http://crl.eid.belgium.be to retrieve a CRL or a delta CRL;
- http://status.eID.belgium.be/ to retrieve the status of a certificate through a web interface; or
- http://ocsp.eID.belgium.be/ for the OCSP responder.

For the profiles of CRLs and OCSP responses we refer to the CPS of the e-Citizen CA: http://repository.eID.belgium.be/

Procedures have been put in place to suspend or revoke certificates when the e-ID card is lost or destroyed. These procedures can be initiated by filing a report with the local police or city hall. Card

holders are informed of their obligation to notify their local police in case of loss or compromise of the card, and an eID card stop telephone number is provided.

3.3.4 Organisational aspects

In practice, authentication services using the eID card (including private sector applications) implement the specific middleware provided by the federal government. The user then authenticates himself using a standard interface prompting him for his PIN code, using a generic PC and generic card readers[56]. The four number PIN-code is initialised randomly when the card is first issued, but can be changed at choice by the bearer. Oddly, the card has only one shared PIN-code for both certificates. While currently mostly in use for public sector applications, the mechanism is available for take-up by the private sector, free of charge.

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. This cooperation has been renewed in 2005 which puts the focus on the development of an integrated eGovernment in Belgium. 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, so that the Belgian eID card system is essentially federated. This system was described above.

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 printed on the card and stored on its chip. No biometric data is involved or currently planned. The printed information can obviously not 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.

As noted above, identification of the citizen is primarily based on his national registry number. Use of this number is strictly monitored, and subject to prior approval by a sector committee within the Privacy 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).

[56] An extensive list of supported readers is published on http://www.cardreaders.be/en/defaultcatalogue.htm. It is also worth noting that the Belgian government is in contact with several major PC vendors to encourage them to integrate card readers directly into their systems for the Belgian market. Several vendors have done this, and a few of their systems can be found on the aforementioned link.

Using the authentication functionality of the eID card, the holder can verify which data of his is stored in the National Register[57], although updating this information directly is not possible (nor is it desirable, since this would mean that the printed information on the card is no longer accurate).

With regard to authorisation/mandate management, there is no generic policy or infrastructure in place yet. A few ad hoc solutions exist, the most notable of which is the possibility of authorising an accountant/tax consultant to file an electronic income tax declaration. At this stage, this requires the mandate giver and the mandate holder to jointly fill in a set of (paper) documents[58], which are then sent in by traditional mail to the tax offices. The tax official will then register the parties concerned in a separate relational database, indicating that the consultant may act as a proxy of the mandate giver. However, this mandate does not relieve the mandate giver of final responsibility for a timely and correct declaration. Mandates are revocable unilaterally by the mandate giver.

3.4 Interoperability

As stated in the introduction above, the Belgian eID card is only issued to a limited number of permanent residents, including Belgian citizens and certain groups of foreigners. Initiatives to open up Belgian authentication services to non-nationals have thus far focused on issuing Belgian eID cards (or other tokens) to such persons, as is aptly demonstrated by the recent pilot initiatives to issue foreigner eID cards. This approach obviously requires prior registration in one of the Belgian official registers, so that it is of limited use to temporary visitors and tourists.

In contrast, no noteworthy initiatives have thus far been taken to ensure the interoperability of foreign eID cards or tokens with Belgian applications. While smaller scale projects exist, involving specifically the Estonian and Austrian solutions, these projects are limited in scope and focus on e-signature functionality rather than electronic authentication.

3.5 eIDM Applications

This section will provide a short overview of key applications for the eIDM systems.

3.5.1 eID card applications

Aside from public sector use, the Belgian government is encouraging private sector uptake of the authentication functionalities of the national eID card.

[57] See https://mijndossier.rrn.fgov.be/

[58] See http://ccff02.minfin.fgov.be/taxonweb/static/nl/help/proForm.pdf

Public sector applications include consultation of the National Register[59], on-line registration of applications for public functions[60], on-line tax declarations[61], safe chatting for minors[62], and ordering attestations for provided medical aid[63].

For a more complete list, see http://map.eid.belgium.be.

Private sector applications (while still at an early stage) include:

- the Planet wInner system, which automates entering customer information for hotels and restaurants; see http://www.planet-winner.com/
- the KeyTrade access management system, offering secured access to e-banking applications; see http://www.keytradebank.com/pdf/eID_nl.pdf
- the Internet banking system from CortalConsors which allows the creation of new bank accounts; see https://www.cortalconsors.be/eid_formul1/processform1_nl.html

For a more complete list, see http://map.eid.belgium.be.

3.5.2 Federal paper token applications

The federal paper token is only used in public sector applications, in particular:

- the TaxOnWeb application for online tax declarations[64];
- a variety of applications using the iLoket framework, as described above. This includes a number of commune portals, including in the communes of Genk, Turnhout, Vilvoorde, Overijse, Diepenbeek, and a number of others. For a more complete list, see http://eid.belgium.be/nl/navigation/44187/index.html

It should be noted that the federal paper token is expected to be phased out it the next few years in favour of the national eID card. Therefore, it is not surprising that all applications above also support the eID card.

[59] See https://www.mijndossier.rrn.fgov.be/

[60] See https://www.selor.be/login/login.aspx?ReturnUrl=/candidat/CVOnline/CvOnLineCockpit.aspx

[61] See http://www.taxonweb.be/

[62] See http://www.saferchat.be/

[63] See http://www.medattest.be/

[64] See www.taxonweb.be

3.5.3 SIS card applications

The SIS card is only used as described above, i.e. by persons or institutions which are professionally involved in health care services and which have been mandated to use the specific readers needed to read/edit the data on the SIS card. From the user's perspective, the only application is therefore the automatic reading/verification of this data, so that the appropriate benefits can be provided (e.g. refunds for medication) and the correct administrative follow-up is ensured.

3.6 Future trends/expectations

As indicated above, the Belgian approach is strongly centred around eID cards. The current eID cards will increasingly become the standard for authentication services in Belgian eGovernment processes, and additional cards are being issued to population groups which have thus far been overlooked.

Additionally, the Belgian government is looking at extending the functionality of the eID card, especially by encouraging further private sector uptake.

The eID card model is an access key model. This means that the eID card can potentially be used to replace other cards (including the SIS card), but not by copying the SIS card data onto the eID card but rather by allowing eID card authentication to be used to access a central SIS card database. This is a possible avenue for the future.

3.7 Assessment

The Belgian approach has a number of advantages and disadvantages, which can be briefly summarised as follows.

3.7.1 Advantages:

- 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, as demonstrated by the Crossroad Banks initiatives described above, so that benefits are shared between users and the administration. Traditional (non-electronic) channels also remain available, in principle at the same costs as the electronic version. Of course, the fact that Belgium already has a tradition of mandatory identification documents is also an important socio-cultural factor.

- Additional features can be built into the eID system, and extension by private sector parties is encouraged by offering up open and free libraries.

- Possibly the greatest success element is the rollout of an IDM system within an administratively complicated federal state, that is functioning on a federal/regional/community/municipality level.

3.7.2 Disadvantages:

- Accessibility to non-nationals: the Belgian system is largely built for Belgian nationals. Plans to extend authentication functionality by deploying additional types of eID cards are currently being rolled out, but the reality remains that only Belgium issued eID tokens can be used in contacts with Belgian administrations. From that perspective, Belgian interoperability initiatives are limited to internal harmonisation (i.e. ensuring that Belgian applications have a common working base), rather than looking at cross-border functionality.

- 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.

- 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, it is 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, relying primarily on a national register number which is protected by strict privacy regulations, privacy management is legally quite complex. While this centralisation also allows the implementation of strong control mechanisms, its scalability remains to be tested if and when the rollout of new applications increases. Also, the importance of protected unique identifiers may be a barrier to cross border functionality.