Brendan Van Alsenoy, Danny De Cock

Due processing of personal data in eGovernment?

A Case Study of the Belgian electronic identity card

In this article, the authors are evaluating the current authentication mechanisms for eGovernment employed in Belgium. Particular focus is placed on the Belgian electronic identity card (eID) and the use of national identification numbers. After evaluating the current situation the authors proceed to highlight possible alternative.

1 Introduction

Over the past few years, a large amount of eGovernment initiatives have been deployed in Belgium. For citizens probably the most visible eGovernment initiative was the introduction of the electronic identity card (eID) in 2003. With the eID Belgium has instituted a means that allows the cardholder to identify and authenticate herself, as well as to place a qualified electronic signature within the meaning of Directive 1999/93/EC on a Community framework for electronic signatures.[1] It is expected that by the end of 2009, over 8 million Belgians over the age of 12 will possess an eID.

The Belgian eID card is a classic smartcard, based on traditional public-key technology where the private keys are generated in the card and the corresponding public keys are protected with a public-key certificate. Two standard X.509v3 certificates[2] are associated with a citizen's eID card. The first serves for online authentication of the card holder, whereas the second can be used to produce qualified electronic signatures. These certificates form the leaves of a 3-layer certificate hierarchy tree: (i) the top level of this tree consists of a commercial Root CA certificate owned by GlobalSign and is embedded in all major client-side applications (e.g., browsers, email clients); (ii) the second level is formed by the Belgium Root CA ; and (iii) the third level is that of the Citizen CA that issues the citizen certificates.

Each CA manages its own certificate revocation lists (CRLs) to indicate which certificates should not be considered valid. The CAs support, besides a CRL service, a second mechanism for certificate status validation: the Online Certificate Status Protocol (OCSP). With this mechanism, relying parties in online transactions delegate answering the challenge "has this certificate been revoked or suspended at this very moment?" to a third party, namely the OCSP Responder. This responder can provide three answers: "yes", "no", or "I do not know." The latter answer is produced whenever the revocation status of an unknown certificate is challenged.

Each Belgian eID holds three private keys. The first private key, also known as the basic private key, is used during card management and can be used to provide proof to external applications that the card is genuine; the second and third private keys are used to compute authentication and qualified signatures, respectively. Any use of the latter two is protected with a single personal identification number (PIN) that consists of 4 to 6 digits.

The identity file contains the citizen's name, first names, gender, national registry number, nationality, birth location and date, noble status, special status, SHA-1 hash of citizen photo, eID card chip number, card number, the card's validity begin and end date, card delivering municipality and document type.[3]

Belgium currently issues three types of electronic identity cards: Belgian eID cards, Kids-ID cards, and foreigners' eID cards. Each consists of the same chip with identical functionalities, but they do not all contain the same certificate types.[4] The citizen's national identification number is stored in the identity file, in the authentication certificate,

Brendan Van Alsenoy

Fulltime researcher at ICRI, K.U.Leuven, working under the academic guidance of prof. dr. Jos Dumortier
E-Mail: brendan.vanalsenoy@law.kuleuven.be

Danny De Cock

Fulltime researcher at COSIC, K.U.Leuven, working under the academic guidance of prof dr. ir. Bart Preneel
E-Mail: danny.decock@esat.kuleuven.be

1 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures, O.J. L 13, 19 January 2000, p. 12.

2 Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, RFC2459

3 See D. De Cock, "Belgian eID card technical overview", 28 January 2008, available at http://godot.be/eidtechnicalities (last accessed 28 January 2008).

4 A Kids-ID issued to children younger than six does not hold any certificate, and can therefore not be used to calculate authentication or qualified electronic signatures. For more information on the Kid's ID card visit http://www.ibz.rrn.fgov.be/index.php?id=564&L=1.

and in the qualified certificate. This number is a 'meaningful' identifier and is formatted as follows: YYMMDDNNNCC, where the first six digits refer to the citizen's birth date, the following three digits refer to a sequence number (odd values refer to males, even values to females); the last two digits form a checksum to detect typing errors.[5]

For foreigners, the number used is the same as the one employed in the social security sector (also known as the 'INSZ').[6]

In summary, a Belgian eID supports one non-electronic, and three electronic applications. The electronic functions include: (i) digital identification of the card holder; the production of (ii) authentication and (iii) qualified electronic signatures. The card also allows for (iv) ordinary visual identification of the card holder.

For ordinary visual identification of the card holder, the usual identifying information is printed on the eID card (names, nationality, national number of the citizen, gender, birth place and date, handwritten signature…). The chip contains similar information, plus a digital picture of the cardholder; an identity file with identifying information; a file with the citizen's official address; digital signatures issued by the National Register to protect the integrity of these files; and the necessary certificates to verify these signatures. Thus, a total of five certificates are stored in the eID card: the citizen's two certificates used to authenticate herself or to verify qualified electronic signatures, the Citizen CA certificate that issued these two certificates, the Root CA certificate that issued the Citizen CA certificate and the certificate of the National Register that protects the information stored in the identity and address file.

Anybody who accesses the chip can read all these files, i.e., no special access control mechanisms have been put in place to protect unauthorized reading of these files. Finally, it is important to note that the National Register's digital signatures on these files protect the integrity of the card's information.[7]

2 Context and purpose of the Belgian eID card

The release of the Belgian eID card is (quite naturally) considered an integral part of Belgian eGovernment in general. It may be considered as the primary means of authentication for citizen and business transactions with the government in an online environment. For several eGovernment services, there are in fact *three* different authentication mechanisms available to citizens, namely (i) the eID, (ii) the "federal token", and (iii) a conventional username/password which may be obtained through the federal portal.

Stronger authentication mechanisms typically depend on the following two factors, i.e. a combination of "something you have" (e.g., an eID card or another token) and "something you know" (e.g., a personal identification number (PIN) or a password). Simple username/password authentication is known as a weak form of authentication because passwords could easily be guessed, eavesdropped, or even passed on.[8] eID cards however, are less easily shared among people due to their official and personal nature. Furthermore, smartcards are also considered to provide a higher level of security due to their cryptographic authentication functionalities. A federal token can be issued to a citizen or a civil servant and provides a medium strength authentication mechanism. This token consists of 24 codes, each 6 characters long. Whenever the citizen or civil servant needs to authenticate herself, she is challenged to present one of the 24 codes. For certain (lower risk) transactions, citizens may also acquire a simple username and password from the federal portal (www.belgium.be) to serve as credentials. In order to do so, users must provide their National Registry Number (NRN), the card number of their identity card, as well as the card number of their so-called 'SIS-card' (the identification card of a person with respect to social security services[9]). For more sensitive transactions (e.g. tax-on-web), either use of the eID or a combination of both username and password and the federal token is required. The further lifespan of the latter two –arguably less secure – authentication mechanisms is yet to be seen. Based on our interviews with eGovernment officials, it appears as if these alternative authentication mechanisms were introduced based on eInclusion considerations. The federal token was thus introduced to bridge the time gap during which not all Belgian citizens had an eID card yet. As soon as all Belgian citizens have been issued an eID card, there will be hardly any need to issue new or still support existing federal tokens.

Crucial for the rest of our analysis, is the observation that the eID card is intended (and is being promoted) for applications outside of eGovernment.[10] This may be said to be in line with the nature of the European directive on electronic signatures: its purpose is to promote electronic commerce. eCommerce can only truly become common practice if service providers are able to prove that their services were requested (and by whom), and consumers will only use services if they feel confident in the identity of the service providers. Either requirement depends on the correct remote identification of the other party. As indicated above, the Belgian eID not only provides a means for trustworthy online authentication of the citizen but also enables citizens to sign digital documents with a qualified electronic signature. For the remainder of this article we focus solely on the eID card as it is also the primary authentication mechanism.

5 A recently published Royal Decree informs us that the process of assigning National Registry Numbers will be even 'less meaningful' for certain "difficult" categories of registrants (see Royal Decree of 20 December 2007 modifying Royal Decree nr. 15 of 3 June 1970 relating to the composition of the identification numbers of people registered with the National Registry, *B.S.* 11 January 2008.

6 The specification of the identification number of social security services (INSZ) is available at http://www.ksz.fgov.be/Fr/faq/faq_5.htm (French) or http://www.ksz.fgov.be/Nl/faq/faq_5.htm (Dutch).

7 For more information on the registration process preceding the issuance of the eID see http://www.ibz.rrn.fgov.be/index.php?id=598&no_cache=1&L=11. See also M. MEINTS and M. HANSEN (eds.), "D3.6: Study on ID documents", December 2006, p. 94 et seq., available at www.fidis.net (last accessed 15 November 2007). Hereafter: [FIDIS D3.6].

8 See also X. HUYSMANS, "D1.2: Conceptual Framework for Identity Management in eGovernment", v1.0, October 2006, p. 122 et seq.. Hereafter: [IDEM D1.2].

9 http://www.ksz.fgov.be/nl/carteSIS/cartesis_1.htm

10 See also *infra*; in particular endnote 32.

See also C. DIAZ (ed.), "Adapid D2: Requirements Study", April 2006, p. 17 et seq. and H. BUITELAAR (ed.), "D13.3: Study on ID number policies", September 2007, p. 59 et seq. Hereafter [FIDIS D13.3].

3 Risk Model

▸ **a) Unrestricted access to the identity file**

The identity file, address file, digital photo and citizen certificates are freely readable by any application that reads the eID card chip. These files include personal and identifiable information, e.g., the card holder's national number, gender, her address, etc.[11]

This implies that a digital copy of this sensitive information may be more easily exposed whenever an eID card is used in an online or offline transaction.

▸ **b) Systematic and extended recourse to the same identifier**

From a general identity management (IdM) perspective, the following privacy risks ("threats") need to be given due consideration when seeking to incorporate privacy safeguards in the design of an identity management system:

1. **Unlawful data exchange**: data is communicated from one entity to another in violation of data protection principles in the strict sense (i.e. proportionality, finality etc.) or in violation of otherwise agreed policies;
2. **Loss of confidentiality**: an attacker, i.e. an unauthorized entity, is able to learn attributes (here: personal data other than identifiers) corresponding to a particular entity while it is not authorized to do so (either through unauthorized access or interception);
3. **Loss of "transactional" privacy**: an attacker may be able to monitor and link the (trans)actions performed by a particular entity and may be able to continue this activity when the observed entity engages in (trans)actions at a later time;
4. **Unlawful data aggregation**: an attacker, who may be authorized to learn certain attributes of an entity for a particular purpose, is able to bring these and other attributes together for an unlawful purpose (be it an entirely different unlawful purpose or an excessive amount of attributes with regards to a particular legitimate purpose);
5. **Unlawful profiling and Knowledge Discovery in Databases (KDD)**: refers to the situation where, once data has been aggregated or otherwise collected, the attacker proceeds to manipulate these data (e.g. through data mining), to assess, predict or otherwise gain knowledge with regards to the subject;
6. **Identity theft**: an attacker is able to fraudulently impersonate another entity.[12]

Much of the research into privacy techniques in recent years has focused on one or more particular threat model(s) (e.g., monitoring of online actions; see a.o. "Anon"[13]). Based on our literature studies, we perceive a growing consensus among privacy advocates, standardization bodies and data protection authorities that *systematic or extended recourse to the same* (unique) *identifier* (in repositories for attribute storage and/or for transactions), *increases the risks for the aforementioned forms of unlawful processing*.[14] One should immediately add however that for most of these privacy risks the augmentation due to systematic recourse is more attenuated in some instances than in others. For instance, transactional privacy is probably the most directly threatened by recourse to the same identifier for every communication. Similarly, the risk of unlawful data aggregation increases greatly when the same identifier is continuously employed for attribute storage and communication. On the other hand, confidentiality is threatened more indirectly by systematic recourse to the same identifier. The primary security mechanisms to ensure confidentiality are access control and encryption. However, knowing the relevant "identification key" is almost indispensable when seeking to obtain the payload data associated with the identifier(s) in question. The most 'removed' privacy risk is likely to be identity theft.[15]

When looking at the Belgian electronic identity card, the risks when using a Belgian eID card for an extended period of time are primarily caused by:

1. the personal information stored in the eID (identity file, address file, digital photo, certificates, etc.) is freely accessible to any application that accesses the eID card's chip;
2. the NRN, whose usage is in principle restricted to entities expressly authorized by law or Royal Decree, is propagated outside the governmental context each time the card is presented to a private relying party (through its inclusion in both certificates and in the identity file);
3. the two signing keys of the eID are protected with a single PIN, which makes it difficult for the citizen to determine which signing key will be activated after having presented this PIN;

11 See also *supra*; endnote 7.

12 See also N. AUERBACH, "Anonymous digital identity in eGovernment", Dissertation der Wirtschaftswissenschaftlichen Fakultät der Universiät Zürich, Juni 2004, p. 75 et seq.

13 Visit http://anon.inf.tu-dresden.de.

14 Note that the list enumerated here is a synthesis of various opinions, advices and articles, and has not as such been adopted by any particular data protection authority. Prominent examples of relevant opinions include: Article 29 Data Protection Working Party, "Working Document on online authentication services", 29 January 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf; "Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6", 30 May 2002, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf; "Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG Group)", 23 January 2004, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp86_en.pdf CDCJ, "Guiding principles for the protection of personal data with regard to smart cards", accessed at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_of_data_protection_committees/P-Guiding_principles_smartcards_2004.asp#TopOfPage; CJ-PD, "The introduction and use of personal identification numbers: the data protection issues (1991)", Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991, available at http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_of_data_protection_committees/X-Pins_1991.asp#TopOfPage (all documents last accessed 28 January 2008). It should be noted that, the major concern in all these instances is raised not so much by the usage of any particular unique identifier as such, but due to the use of the same identifier across multiple or all contexts or sectors.

15 In this case, the risk is increased due to the fact that when extended recourse is taken to the same identifier, the identifier tends to become more widely known. In practice, many registration processes still request identification numbers as corroborative evidence. This practice is quite common by private companies in the United States (e.g. with regards to the Social Security Number), but also takes place in Belgium, namely when obtaining a username and password through the federal portal (cf. *supra*). As we will see further, use of eID propagates national registry number (NRN). This means that it will generally not be very difficult for an attacker to obtain the NRN of any citizen once the eID card starts being used frequently. Consequently, one of the three elements of corroborative evidence to be produced in obtaining a username and password through the federal portal becomes easy to obtain.

4. the online use of the eID in authentication protocols permits a service provider to link the citizen's transactions that were executed during distinct online transactions;
5. if multiple service providers collude, they can profile the actions of a cardholder who used their online services;
6. data logged pursuant to the online certificate status protocol (located with the OCSP Responder – i.e. the most direct certificate status verification procedure), might also serve to profile the activities of a citizen, as it can derive which citizen interacts with which service providers.

4 Evaluation

▸ **a) Inclusion of the national identification number in the data file and certificates**

As indicated earlier, both the citizen authentication and signing certificates, as well as the identity file, contain the National Registry Number (NRN), which is consequently propagated at every certificate or card-present transaction. The most prominent reason to include the NRN in the authentication certificate is to facilitate the mapping of a remote user/citizen to a service provider's account or database system. However, use of the NRN, such as for the purpose of establishing network connections, is governed by the Law of 8 August 1983 instituting a National Registry of natural persons.[16] It essentially restricts the usage of the NRN to entities expressly authorized by law to do so.[17] The Law instituting the electronic identity card[18], which introduced the NRN in the certificates and identity file of the eID cards of Belgian citizens does not explicitly contain a similar provision. This has led several authors to conclude that the "mere reading" of the NRN does not qualify as "usage".[19]

The debate surrounding the usage of single national identification numbers has longstanding historical roots.[20] EU countries have sought to regulate their national number(s) in a variety of ways.[21] Art. 8.7 Directive 95/46/EC provides that "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed", indicating that governments should carefully consider how they allow their national number(s) to be used.[22] This provision is no doubt the outcome of a political compromise, seeing as Member States still differ greatly in opinion as to whether and how national identification numbers should be used.[23] Regardless of how national identification numbers are (or are not) regulated in each respective State, they always (due to their very nature) constitute 'personal data' within the meaning of Directive 95/46.

▸ **b) Confidentiality and security of processing**

Art. 16 and 17 of the Directive 95/46 impose upon the controller a general confidentiality and security obligation, which includes inter alia the obligation for the controller to take all reasonable measures "*to prevent all other unlawful forms of processing*" (art. 17). Regardless of the possible perception that the current eID scheme might lead to massive data aggregation and profiling by the government, on the value of which we bare no judgment, it is manifestly clear that the NRN *was not intended for use outside the governmental context*.[24] In addition, the general privacy threats due to systematic recourse to the same identifier discussed earlier continue to apply with full force. This has left us with a rather interesting situation: because of a political compromise, caused by greatly varying historic traditions, the usage of national identification numbers by Member States may not be said to be proscribed by the Data Protection Directive; whilst other provisions indicate that such "global" identification practices might run afoul with other basic data protection principles. This evaluation of course largely depends on risk perception and analysis; as well as any (organizational) measures which may be in place (such as e.g. prior authorization requirements) to mitigate certain privacy risks.[25]

One may also not lose sight of the fact that the security obligation of art. 17 is an 'obligation of means'. Cost and state-of-the-art are equally important elements to take into account when assessing whether the controller has adequately quitted himself of his obligations. At the time of the initial eID release, more privacy-friendly alternatives were in fact discussed, however, the maturity of these alternatives was considered insufficiently proven, and the infrastructure that would have been necessary to implement those alternatives had not yet been prepared. Today one should also take into account the following: an ever increasing amount of IdM architectures and applications have emerged in which uniform cross-sectoral identification is clearly no longer an interoperability requirement.[26] At the time of its introduction, use of a global unique identifier was however considered a necessary interoperability component by prominent policymakers.[27] The question is whether

16 B.S., 21 April 1984. Adapted over time, this law sets forth the basic framework governing the establishment of "network connections" using the NRN. The baseline principle is that every such connection must receive prior authorization by the Belgian Privacy Commission (see in particular art. 8 et seq.).

17 See D. DE BOT, "Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart", Vandenbroele, Brugge, 2005, p.177 et seq.. See also [FIDIS D13.3], p.54 et seq.. As an additional safeguard, the law also introduces an "authorization scheme", whereby each network connections must be approved in advance by (a Sectoral Committee of) the Belgian Privacy Commission. See also *infra*.

18 See primarily the Law of 25 March 2003 modifying the National Registry Law and the Law governing the population registries and the identity cards and the Law 1983 concerning the National Registry, as well as all implementing Royal Decrees (in particular those of the same date of official announcement and publication). (*B.S.*, 28 March 2003).

19 D. DE BOT, *o.c.*, 189; [FIDIS D13.3], p. 58.

20 See [FIDIS D13.3], p. 13 et seq.

21 See Art. 29 Data Protection Working Party, "Working Document on E-Government", 8 May 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_en.pdf (last accessed 28 January 2008).

22 See also [FIDIS D13.3], p. 28 et seq.

23 See Art. 29 Data Protection Working Party, "Working Document on E-Government", *l.c.*, p. 8 et seq..

24 See also [FIDIS D13.3], p. 59. This may reasonably be derived from the scheme of prior authorizations inserted in the National Registry Law and Royal Decrees..

25 See also *infra*; endnote 28.

26 See ETSI, Liberty Alliance, Card Space, Idemix, Credentica.

27 J. Deprest and F. Robben, "eGovernment: approach of the Belgian Federal Administration", Brussels, June 2003, p. 21, available at http://www.law.kuleuven.be/icri/frobben/publication%20list.htm, last accessed 28 January 2008. This policy paper may be said to have directly contributed to the current legal framework and developments regarding the use of the NRN and eGovernment IdM in Belgium as whole. To safeguard privacy, the authors in-

now, as the state-of-the art with respect to online transactions and interconnection between service providers has considerably evolved, a different approach will be sought. The most prominent reason for maintaining the current situation is to avoid re-registration. Unique identifiers are used to link credentials (such as authentication certificates and tokens), to other credentials that are issued at a later stage (e.g., in the event of card loss or expiration). We will come back to this issue in the following section.

► **c) Possible alternative approaches**

The alternatives being developed in the AdapID project (https://www.cosic.esat.ku-leuven.be/adapid) can be summarized as follows: in the first phase of the project (which has recently been completed), advanced applications were designed to allow citizens to obtain so-called 'private' credentials (pseudonymous, i.e. without propagating the NRN, attribute assertions), whilst still using the current eID as a bootstrap. The disadvantage of this model is that the users are obligated to first obtain these private credentials online prior to interacting with a relying party. In the second phase of the project however, research will focus on possibilities for a future release of the eID card whereby private credentials would be integrated among the cards basic functionalities.

In the meantime, the Belgian government is planning the next release of eID cards for the end of 2008. This version of the eID would have an increase in storage space, much of which has not been spoken for. This version is expected to allow citizens to specify different PINs to better protect the (distinct) authentication and qualified signing functionalities; but is not yet expected to include identifiers or pseudonyms other than the NRN. As indicated at the end of the previous section, the main reason not to change the identifiers (NRNs) already being used, is to avoid re-registering: if a new identifier replaces the previous identifier associated with that user, how will the relying party know which account to attribute it to?

The Belgian government could nevertheless consider using the extra space to include additional certificates (and corresponding private keys[28]) in the card, which would contain identifiers (pseudonyms) other than the NRN. The issue of re-registration could be accommodated by utting in place an infrastructure which would allow mapping of the pseudonyms where legally permitted.[29] As indicated above, Belgian legislation concerning the use of the NRN restricts its usage (e.g., for account management[30]) to enumerated categories of entities, and imposes the requirement that authorization first be sought before the Privacy Commission. As a rule, the NRN is only to be used in the (semi-)governmental context for account management purposes. The promotion of eID usage outside the governmental context is simply at odds with the governing legal framework, unless additional measures are taken to limit the exposure (and propagation) of the NRN outside the governmental sphere.[31]

5 Conclusion and Outlook

Debates surrounding eGovernment initiatives shouldn't be about identifiers alone. In addition, one should consider the following. The current Belgian eID card clearly raises serious privacy concerns if maintained in its current form over the long term. However, it is equally clear that the current card will by no means pose a real societal issue from one day to the next. Although its usage may be said to increase, the Belgian eID card is still quite far removed from being the primary authentication means for all online (trans)actions among private entities. Such usage may however, at the very least, be said to be "stimulated" by the Belgian government.[32]

In addition, the debate concerning the use of national identifiers might need to shift. The reason is the introduction of mediator, integrator and discovery services in more and more advanced IdM applications.[33] These trusted (occasionally third) party services could in principle also be designed to enable cross-context data exchange without using the same identifier. As indicated earlier, it is not so much the use of unique identifiers, as the use of "globally unique" identifiers, which raises the most serious privacy concerns.[34] The entity performing the mapping and conversion could be placed under the direct supervision of the Belgian Privacy Commission. If pro-

troduced the scheme of prior authorizations by the Belgian Privacy Commission, a proposal which is to be greatly applauded. However, other than basic access control mechanisms and use of cryptography to ensure confidentiality, little or no *technical* security measures are proposed (other than the post fact auditing of logged activities). Compare art. 17 of Directive 95/46/EC (both organizational and technical measures).

28 Note that public keys are also identifiers in and of themselves. Merely introducing additional certificates would therefore not eliminate linkability concerns.

29 The following scenario could be imagined: the Belgian Privacy Commission has repeatedly insisted –thus far without result – upon the creation of a separate 'patient identification number' in the context of the emerging 'BeHealth' platform (with regards to the introduction of so-called 'Patient Identification Numbers', see the following opinions issued by the Belgian Privacy Commission: Advice nr. 14/2002 of 8 April 2002; Advice nr. 19/2002 of 10 June 2002; Advice nr. 30/2002 of 12 August 2002; Advice nr. 33/2002 of 22 August 2002; Advice nr.1/2005 of 10 January 2005 and Advice nr. 05 / 2006 of 1 March 2006 (all available on the website of the Privacy Commission, available at www.privacycommission.be). Citizens seeking to access their medical file through the BeHealth portal could be provided the ability to select their BeHealth credentials (partial identity) if the appropriate user interface is provided. This could be a significant step forward in reducing the 'global' nature of the identifiers employed in Belgium eGovernment.

30 See e.g. Privacy Commission, Advice nr. 13/2006, 24 May 2006, available at www.privacycommission.be.

31 See J. DUMORTIER, "eID en de paradoks van het Rijksregisternummer", *Trends Business ICT*, March 2005. Source: http://www.law.kuleuven.ac.be/icri/publications655Column_BusinessICT_06_eID.pdf (accessed 26 April 2005).

32 In addition to the fact that a the certificate hierarchy contains a commercial Root CA certificate owned by GlobalSign and is embedded in all major client-side applications (e.g., browsers, email clients) (cf. *supra*); the fact that the eID is increasingly requested when entering (semi-)public buildings; it was announced during a press conference on 1 February 2005 by the Belgian Minister Informatization Peter Van Velthoven and Microsoft's Bill Gates that, "in order to help make online transactions and communications more secure" the Belgian government is working with Microsoft "to ensure that our technologies support [the Belgian] e-ID [card]", in particular with regards to popular applications such as MSN messenger. (http://www.belgium.be/eportal/application?languageParameter=nl&pageid=contentPage&docId=37771) (published 1 February 2005) (last accessed: 28 January 2008).

33 It is important to note that certain types of mediator, integrator and discovery services have already been introduced at various levels in Belgian eGovernment The most notable examples being the Crossroads Banks for Social Security, the Flemish Integration Platform, the Walloon Integration Platform … See [IDEM D1.2], p 140 et seq.. These entities however do not currently support identifier conversion and mapping services other than with regards to the data model used.

34 Cf. *supra*; endnote 15.

vided with sufficient means, the Privacy Commission could audit and certify correct application of policies and procedures.[35] And perhaps the unique identifiers associated with the eID could, as a general matter, be less 'global'.[36]

Citizens' trust in eGovernment services needs to be earned. When considering possible alternatives and improvements, one should keep in mind the following maxim of democratic society: 'Justice must not only be done, it must also be seen to be done'.[37] Increased transparency through applications such as 'my file' (Dutch: "*mijn dossier*") we hope marks the beginning of a more broadly enforced transparency in Belgian eGovernment.[38] This could be a most valuable additional democratic safeguard, significantly reducing the "knowledge asymmetry"[39] brought upon by the dramatic increase in data exchange in eGovernment in general.[40]

6 Acknowledgements

We thank Claudia Diaz, Koen Simoens, Els Kindt, Fanny Coudert and Joris Ballet for providing their comments on the draft of this article.

This publication has been made possible thanks to funding received in the context of the Flemish IWT Project AdapID ('Advanced applications for electronic Identity cards'). K.U.Leuven is also a partner in the EU NoE FIDIS (http://www.fidis.net).

35 The practice of "privacy seals" has already been introduced by ICPP in Schleswig-Holstein. For more information see https://www.datenschutzzentrum.de/guetesiegel/eria/index.htm.

36 See also Cameron's 4th Law of Identity regarding 'unidirectional' and 'omni-directional' identifiers (available at www.identityblog.com). We do not however condone a model whereby public entities are stimulated to resort to such 'omni-directional' identifiers as a default; except perhaps in the specific example of passports (due to the fact that the monitoring of border crossing may be said to be a context on its own).

37 Visit (among many others) https://www.lawlink.nsw.gov.au/lawlink/Supreme_Court/ll_sc.nsf/pages/SCO_spigelman200905.

38 Visit https://www.mijndossier.rrn.fgov.be. "My File" offers Belgian citizens an instrument to check and rectify their personal data online in the National Register in Belgium. It also enables users to see who has consulted their data. Official documents such as birth certificates, family composition and civil status documents can be downloaded and transmitted. These documents are electronically signed by the National Registry. (source: http://www.epractice.eu/cases/myfile). See also https://ww.mijndossier.rrn.fgov.be (Dutch) and https://ww.mondossier.rrn.fgov.be (French) for more information. At moment of this writing, the "My file" application does not yet extended to any of the numerous other databases or consultations in Belgian eGovernment.

39 See M. HILDEBRANDT and B.-J. KOOPS, "D7.9: A Vision of Ambient Law", October 2007, p. 14. See also M. HILDEBRANDT and S. GURTWIRTH (eds.), "D7.4: Implications of profiling practices on democracy and the rule of law", September 2005, both available at www.fidis.net.

40 With regards to possible more advanced transparency functionalities see also B. VAN ALSENOY and H. BUITELAAR (eds.), "D16.1: Conceptual Framework for Privacy-Friendly Identity management in eGovernment" and "D16.3: Requirements study" (both forthcoming on www.fidis.net).