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 Citizen 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 With this mechanism, relying parties in online transactions delegate answering the challenge “has this certificate been revoked or suspended at this very moment?”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.vansenloy@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


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


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: YYMDDNNNCC, 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.  

For foreigners, the number used is the same as the one employed in the social security sector (also known as the ‘INSZ’).  

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.  

### 2 Context and purpose of the Belgian eID card

The release of the Belgian eID card is (quite naturally) considered an integral part of 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. 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). 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 exclusion 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. 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).


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

9 See also [www.ksz.fgov.be/nl/carteSIS/cartesis_1.htm](http://www.ksz.fgov.be/nl/carteSIS/cartesis_1.htm)