The Belgian Electronic Identity Card (Overview)

Danny De Cock, Christopher Wolf, and Bart Preneel

Katholieke Universiteit Leuven,
Department of Electrical Engineering–ESAT SCD/COSIC
Kasteelpark Arenberg 10, B-3001 Heverlee-Leuven, Belgium
http://www.esat.kuleuven.be/cosic
{decockd,cwolf,preneel}@esat.kuleuven.be

Abstract. Currently, Belgium is introducing an electronic version of its identity card. In this article, we shortly describe the card, and give a brief introduction to its cryptographic features. In particular, we focus on the Public-Key Infrastructure (PKI) associated with the card.

Key words: Electronic identity card (eID), Nation-wide Public-Key Infrastructure (PKI), Certificate Revocation Lists (CRL).

1 Introduction

Due to new challenges, both on the side of electronic commerce and security, more and more countries decide to replace their paper-based identity cards by electronic ones. Belgium is currently the only European country that has decided to issue an electronic identity (eID) card to all its citizens aged 12 years or older. Estonia also has very extensive coverage; and Austria, Italy and Spain are also making good progress in deploying eID cards. Each of these countries have implemented their individual eID system. Where the Austrian system [dB] relies on the Bürgerkarte concept (this concept does not require the use of a smart card) as a tool to create an electronic signature, this article focuses on the eID card system designed and implemented in Belgium. This short paper outlines some of the card's design issues and practical consequences.

2 Card Description

The Belgian eID card has the size of a normal smart card, e.g., a bank card. The visual design (cf.

Fig. 1. Belgian eID card's visual aspects

Fig. 1) is similar to the previous identity card and contains name (family name, up to two given names, and the initial of a third name), title, nationality, place and date of birth, gender, and a photo of its holder. Moreover, it contains a hand written signature of its holder and also of the civil servant who issued the card. It also mentions the validity dates of the card (the card is valid for five years), the card number, the national number of its holder, and the place of delivery of the card. All this information is also stored on the chip in a so-called "identity file." The identity file is around 200 bytes long, and is signed by the National Register (RRN). In addition to the identity file, there is also an

address file (about 150 bytes). This file is kept independently as the address of its holder may change within the validity period of the card. The RRN signs the address file together with the identity file to guarantee the link between these two files. The corresponding signature is stored as the address file's signature. As biometric feature, Belgium decided to use a photo (3 KBytes, JPEG format). This photo is (indirectly) signed through the RRN, as its hash is part of the user's identity file.

The chip on the card can perform digital signatures and key generation. There are no concrete plans to integrate decryption functionalities in the eID card.

3 Roll-out

Initial Planning. On September 22, 2000, the Belgium council of ministers approved an eID card concept study. This study was a direct consequence of the publication of the European Directive, cf. [Par00], on electronc signatures. The contract to implement the system specified in the study was assigned in January 2002 to the private company NV Steria. In particular, it was decided to issue certificates for individual citizens, and to start with a pilot phase in 11 selected municipalities. In addition, it was decided *not* to integrate the social security card or the citizen's driving license with the newly developed national identity card because of incompatibilities with the Belgian legal framework. From a technical point of view, this integration would have been easy.

Pilot Phase. The pilot phase started in March 2003 by issuing the first 4 eID cards to civil servants. The contract to prepare and produce the first eID cards had been awarded to the private company NV Zetes. This company still takes care of the logistics (transport of the eID card request forms and of the eID cards), and of all the other practical issues: physical assembly of the eID card, printing of the front/back of the card, the electronic initialization of the cards (key pair generation, initialization of data files, etc.). All the eID card-related certificates are issued by the Certipost consortium, which is a joint venture of the Belgian Post Group and Belgium's largest telecommunications operator Belgacom.

The first municipality started issuing eID cards to its residents on May 9, 2003, the eleventh on July 25, 2003. An overview of the number of eID cards that have been produced, activated and revoked since the start of the pilot phase is available at [DC].

During the pilot phase, a few technical difficulties were discovered and fixed. In particular, the holder's address was removed from the visual part of the card and is now only present in the chip. Otherwise, it would have been necessary to re-issue cards as soon as holders change their address. For cost reasons, this option was discarded.

Nation-wide roll-out. The national roll-out started September 27, 2004. All citizens may now request an electronic identity card. All 589 Belgian municipalities are equiped to issue and process eID cards. Belgian citizens who wish to obtain their eID card, even before they are invited to do so, can initiate the eID card issuing process themselves.

By the end of 2009, the transition from paper based identity cards to electronic identity cards will be completed. Moreover, by that time, all non-Belgium residents who stay for more than 5 years in the country will also be issued an eID card. For cost reasons, non-Belgium residents who stay a shorter period of time (typically one year), will *not* be issued an eID card but a paper based version.

4 Cryptographic Details

In total, a Belgian eID card holds *three* different 1024-bit RSA private signing keys: one to authenticate the citizen, one for non-repudiation signatures, and one to identify the card itself towards the Belgian government. The eID card is able to compute digital signatures with all three private keys. For the citizen's authentication key and non-repudiation signature key, this is only done after the card holder entered a PIN. This PIN must be entered by the citizen, preferably using some trusted hardware, e.g., a smart card reader with stand-alone key pad.

Each of the first two key pairs is accompanied by a certificate. These certificates are issued to the citizen: one authentication certificate for use in client authentication, e.g., with SSL/TLS. The second

certificate is a qualified certificate that binds the non-repudiation key to the card holder and that can be used to produce electronic signatures that are equivalent with handwritten signatures. Neither of these certificates contains an email address of the citizen. The private key of the card's third key pair is used when the card communicates with the National Register (RRN) for mutual authentication, e.g., to update the card holder's details (typically the address), the national certificates, etc. The RRN keeps in its databases a copy of the public key to verify the signatures calculated with this third key.

It is the smart card initializer that starts the key pair generations during the initialisation phase of the eID card. The smart cards are produced by Infineon (chip type SLE66CX322P) and are equipped with the JavaCard operating system of Axalto. The cards use their on-board hardware random number generator to seed the key pair generation function of the card. The private part of the key pair never leaves the card. The public exponent of the 1024-bit RSA key pair has a fixed value and equals 65537.

The smart card in itself is not able to calculate the cryptographic hash value on which it produces a digital signature: an eID card digitally signs the 16 or 20 bytes that it receives from an external application. The card is instructed during the initialization of the signing session to expect 16 or 20 bytes, depending on the padding type (MD5withRSA or SHA1withRSA) that it needs to apply before calculating the actual signature. It is impossible to have the card calculate a signature on other information than these 16 or 20 bytes.

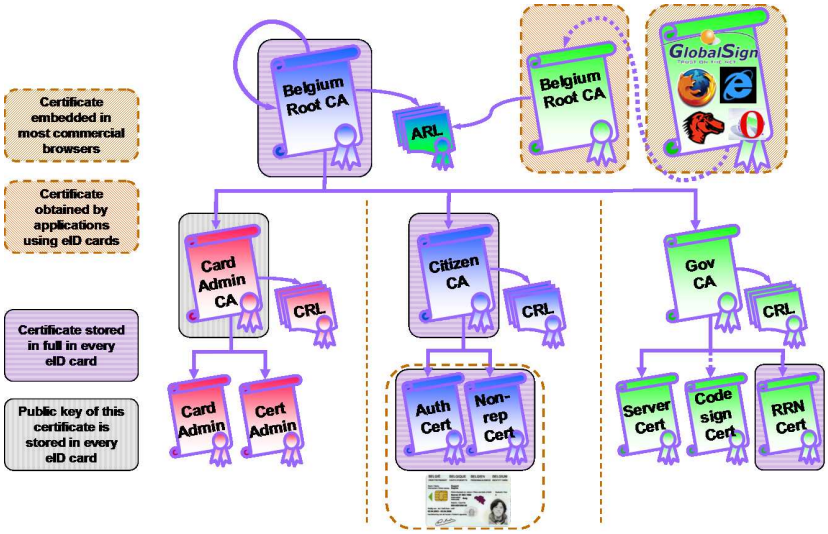

Fig. 2. Belpic eID CA structure

The card also holds, in addition to the two card holder certificates, three government-specific certificates: the Belgium Root CA certificate, the Citizen CA certificate, and the National Register (RRN) certificate. The overall certificate hierarchy is summarised in Fig. 2.

The Belgium government decided to use a 2048-bit RSA key for its CA certificates. Certificates for individual users (e.g., card holders, servers) and for the RRN include 1024-bit public keys. It was decided to issue 1024-bit RSA key pairs for use by the citizens during the first phase of the national roll-out. In the second part of the national roll-out, a gradual migration to 2048-bit moduli is envisaged.

Fig. 2 shows that the Root CA certifies other CA certificates, e.g., for the card administration and government-specific servers. The key pair used for the Self-signed Belgium Root CA certificate has also been certified by the commercial certification authority GlobalSign so that the certificate chain of, e.g., a citizen certificate → Citizen CA certificate → Belgian Root CA, can be validated by mainstream applications (email clients, browsers, etc.). The Citizen CA issues the two citizen certificates.

Carrying an identity card is a legal obligation in Belgium. Hence, the loss of such a card has to be reported swiftly, after which the corresponding certificate is suspended for up to 7 days. If the citizen

finds his/her eID card back before this 7-days period ends, then the card can be unsuspended. In the other case, the card becomes irreversibly revoked.

Each CA implements this functionality by issuing, next to certificates, also certificate revocation lists (CRLs) in which it enumerates all the certificates that have not yet been activated by the citizen (i.e., if the eID card has not yet been delivered to the citizen), that have been suspended (e.g., if the citizen lost his/her eID card), or that have been revoked (e.g., if a citizen's eID card has been stolen). All the CRLs that have been issued in the last year can be accessed through the Internet (CRLs that are older than one year can also be accessed, but this is not an online service). So far, no certification authorities have been revoked with the Authority Revocation Lists (ARLs). At present (November 2005), the overall revocation list has a size of 36 MB. To facilitate the handling of revoked keys, the CA provides delta CRLs, issued every three hours. Hence, individuals or organisations who wish to update their database with certificate status information only need to download these delta CRLs. Usually, they have a size of much less than 100 kBytes. To reduce the total size of an individual CRL, the CA has also started, since the beginning of 2005, to keep thirteen active CRLs. It issues certificates that point to a particular CRL in a Round-Robin scheme: the certificates issued for a batch of eID cards refer to one of the active CRL, the next batch to another active CRL, etc.

As each eID card has been initialized with a genuine copy of the Belgian Root CA certificate, the card can be used as a "trusted source:" each user can verify the chain of trust within the Belgian PKI system by loading the Belgium Root CA certificate from her/his smart card. Hence, the whole eID project can be seen as a nation-wide PKI – with strong user authentication during the issuing phase, as each citizen has to present her/himself at the municipality.

Apart from revoking the use of an eID card's keys when it is stolen, card holders also have the possibility to have the electronic signature capability of an eID card revoked, even before using a card ("opt-out"). This way, the card holder expresses that she/he is not interested in using the signature or authentication features of the card.

5 Comments

During the pilot phase, only very few (cryptographic) problems had to be fine-tuned, such as using RSA signatures by PKCS#1v2.1 instead of PKCS#1v1.5. Hence, from a technical point of view, the Belgian eID card relies on a sound architecture. For example, having two different private keys for each citizen prevents specific types of attacks, e.g., by asking to authenticate a "random number" during a session which could in fact result in a digital signature on a contract.

From a practical perspective, the lack of smart card readers installed in home computers performs a serious obstacle for the wider use of the eID card. However, by promoting government applications such as "tax on web," registered mail, social security registration of new personnel, online consultation of government data, together with the distribution to twelve-year olds of a free smart card reader when they get their eID card, the home penetration with readers is expected to increase in the short term. As soon as it is high enough, we also expect an increasing interest by companies using the eID card as a mean of authenticating their customers and entering legally binding electronic contracts with them.

The main concern with the Belgium eID card is privacy: a Belgian eID card can be used in citizen-citizen, citizen-business, and citizen-government communications. Currently, no privacy enhancing technologies have been implemented with the eID card. While technically possible, this has not yet been included in the specifications of the eID card. These improvements are expected in a later revision of the eID card system.

References

[dB] Stabsstelle IKT-Strategie des Bundes. Die Österreichische Bürgerkarte. http://www.buergerkarte.at.

[DC] Danny De Cock. Non-official information on the Belgian Electronic Personal Identification Card. https://www.cosic.esat.kuleuven.be/belpic/.

[Par00] European Parliament. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Januari 2000.