Belgian e-government Application: the eID Card

Philip KEERSEBILCK, Bert DUFRAIMONT
University College KAHO St Lieven
Gebr. Desmetstraat 1, BE-9000 Ghent
Philip.Keersebilck@kahosl.be, *Bert.Dufraimont@kahosl.be*

Abstract—**The implementation of the electronic identity card (eID) is a part of the Belgian e-Gov project regarding the administrative simplification and the modernization of the public services. This concept of a citizen eID card is quite a breakthrough in different aspects: it offers the possibility to authenticate electronically and to make electronic signatures, which are the equivalent of traditional handwritten signatures. This paper presents the card's design issues, it's crypto functionality and outlines some practical consequences.**

Index Terms—**eID, identity management, electronic identity card, digital identity**

I. INTRODUCTION

Proving who we are is an all too common characteristic of modern life. Citizens travelling from their country to another are generally required to carry a passport to identify them and their country of origin~~;~~ to access welfare services, they present a social security card, and to vote a polling card. However, in an electronic communication environment where individuals and groups want to discourse, share and access content, and conduct transactions at a distance with confidence and security, these official papers are of little value. In this environment, an electronic identity (eID) token provides the answer.

There are a wide range of ambitious identity management initiatives around the globe. In Europe, Belgium has already started its own eID roll-out. The UK, the USA and many others are actively developing the legal framework for their own programmes. These projects range in scope and scale, from traditional PKI (Public Key Infrastructure) style projects using smartcards with embedded chips, through to those that will also include biometrics. In Europe, Directive 1999/93/EC of the European Union (EU, 1999) on electronic signature use, provides the baseline for many European eID initiatives. In this paper, I will consider the approach of my country Belgium to eID management [1] on a national scale.

The Belgian eID card program is already well advanced. It is an initiative from the Belgian government, to replace the current passport of every citizen by an eID card [2]. The Belgian Council of Ministers decided in July 2001 to introduce an electronic identity, to be issued to every Belgian citizen over the age of 12. The eID card is being deployed since the half of 2003, and at the time of writing nearly 5 million cards have been issued.

The eID card is a smartcard and contains certificates and identity data on its chip. Main functionalities are data capture, authentication and digital signature.

The eID card remains above all other features the official proof of one's identity, but makes remote control identification possible, with regular identification on the one hand, and authentication on the other hand. Another feature for the card holder is the possibility to sign electronic documents with a legally binding signature.

II. CARD COMPOSITION

The identity card consists of a secure physical section and an electronic section (chip). Counterfeit-proof details are engraved and printed on the plastic surface. The contact chip is embedded and glued into the plastic layer. The card is made of polycarbonate material and its size is identical to a credit card. Several security techniques are applied, some of them being used in banknotes.

The chip is a JavaCard with a crypto-processor that performs cryptographic operations (RSA and DES). You can compare this chip with a full-blown personal computer, allowing the storage of data and even applications.

The chip included on this eID card contains the citizen's identity information and address together with identity and signing certificates. This enables the chip to be used for authenticating information and generating digital signatures that are regarded as equivalent to handwritten signatures. The card is valid for 5 years; figure 1 shows an example of a Belgian eID card.

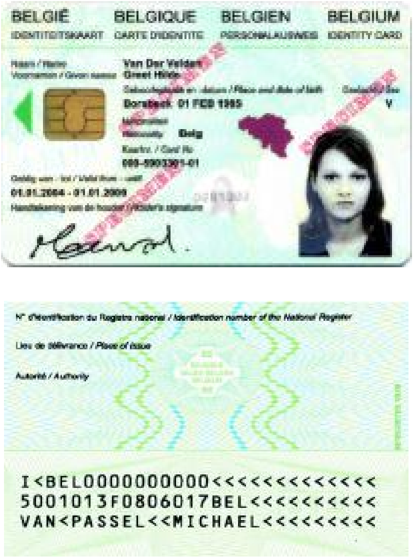
BELGIË BELGIQUE BELGIEN BELGIUM
IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD
Van Der Velden
Greet Hilde
Borsbeek 01 FEB 1995
Belg
01.01.2004 - 01.01.2009
I<BEL0000000000<<<<<<<<<<<<
5001013F0806017BEL<<<<<<<<<<
VAN<PASSEL<<MICHAEL<<<<<<<<<

Figure 1. eID card physical layout.

Data on the electronic identity card [3] are of two types: *information readable with the eye and electronically* (such as name, two first names, nationality, birth date and place, sex, place of card delivery, date of start and end of card validity, holder's photography, signature of the holder and local employee and the identification number in the national register for physical persons) and *invisible information only readable in an electronic way* (such as identity keys and signature, identity certificates and signature, accredited certification authority, the necessary information to the card identification as well as the protection of electronically readable data stated on the card as well as the use of linked certificates and the holder's main residence).

III. CRYPTO FUNCTIONALITY OF THE CHIP

The eID government application is largely a traditional PKI style deployment, based on a smartcard system that incorporates keys and digital certificates [4][12]. On the eID file system of the card, there are two main directories. One contains the specific user data in a proprietary format and the other one is PIN protected and contains the certificates.

The cardholder's *key pair* (consists of public and private key) is generated on-chip and only the public key is accessible. The use of the private key is protected with a pin code. In the personalisation phase, the public key is entered into two certificates signed by a government-approved "certificate authority".

The public key can be used by everyone. It can be retrieved, together with the digital signature, by every one who wants to check the validity of a signature. The private key is only accessible if the card holder enters his PIN code (that's rather obvious: otherwise malicious software could sign any document as soon as you put your eID card into a smartcard reader).

The certificates have a standard format and in addition to the public key, contain the name and national registry number (unique personal identifier) of the cardholder. The eID contains a minimal set of personal data so that the individual's privacy is protected in the event of theft or loss. Each certificate is linked to a private and a public key.

The Belgian eID holds three different private keys: one to authenticate the citizen, one for non-repudiation signatures and one to identify the card towards the Belgian government for mutual authentication [5]. The first key is accompanied by a certificate that can be used for authentication *(authentication certificate*); you'll need it for instance when you fill in your tax form online. The second one is accompanied by a certificate that can be used to produce an electronic signature that is equivalent with a handwritten signature (the *qualified signing certificate).* The third private key is used when the card communicates with the National Register (RRN). There is no corresponding certificate on the card; the National Registry keeps the public key in its databases. It is evident that these keys never leave the smart card: they are private.

Furthermore, the card contains, besides the 2 card holder certificates, 3 government-specific certificates: the Citizen Certification Authority (CA), which itself is signed by the Belgian Root CA certificate. Finally there is also the National Registry (RRN) Certificate (corresponding with a private key used by the National Registry). A certificate has always to be validated, meaning the validity period has to be checked and the serial number of the certificate has to be checked with an OCSP (Online Certificate Status Protocol) or against a CRL (Certificate Revocation List).

These key elements allow three types of use of the eID card: data capture and standard cryptographic operations such as authentication and e-signing of documents.

First of all, the card's *data capture* is used in applications to read identity data (name, address, gender, …) from the card. Inserting the eID card in a smart card reader which is compatible with the published technical specifications, allows someone to read the personal data mentioned above. So this stored data can be used in any circumstance where citizens want to "show" their eID card, but then in an electronic equivalent way avoiding that human errors are made because the files can now be electronically read from the chip. This gives an advantage to business applications which use this data, because it takes less time to enter the data, and no more typing errors can occur.

Every citizen above twelve can *authenticate electronically* with a card issued by the government. In the next example (figure 2) [11], Alice visits a website which asks client authentication e.g. with SSL. The web server will learn Alice's official name, here national number and that here card was used for authentication to the server.

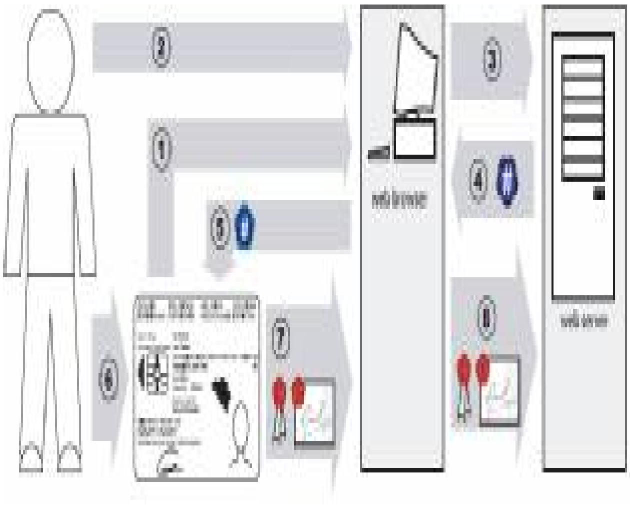

Figure 2. Authentication to a server.

Alice connects (1) the eID card reader with here computer en puts here eID card in the reader. Next, she visits (2) the website (who is secured with eID technology). The web browser sends (3) a request to log in to the web server. The web server sends (4) a random challenge to Alice's browser. Alice's browser sends (5) this hashed challenge tot the eID-chip in order to sign it. Alice confirms she wants to log in on the website, by presenting here PIN-code (6) to the eID card and authorizes the signature generation. The eID card sends (7) the signature and the corresponding certificate to the browser. Finally, the web server receives (8) Alice's signature and certificate. So, Alice's eID card allows her to authenticate herself in this secured on-line application.

The signature key pair (with certificate) on card, allows people *to digitally sign documents.* A digital signature can be used to proof that some content originates from a certain user and has not been modified along the way. Through the use of the PIN in combination with the digital signature certificate on the eID card, citizens can now sign e-mails, documents and forms in Word, Acrobat, etc. with the same legal value as their handwritten signature. This is only possible for citizens above 18 years old, not for minors.

In figure 3 [11], Alice will use here eID card to sign a document. Bob will learn Alice's official name, her national number and that here eID card was used to produce a digital signature.

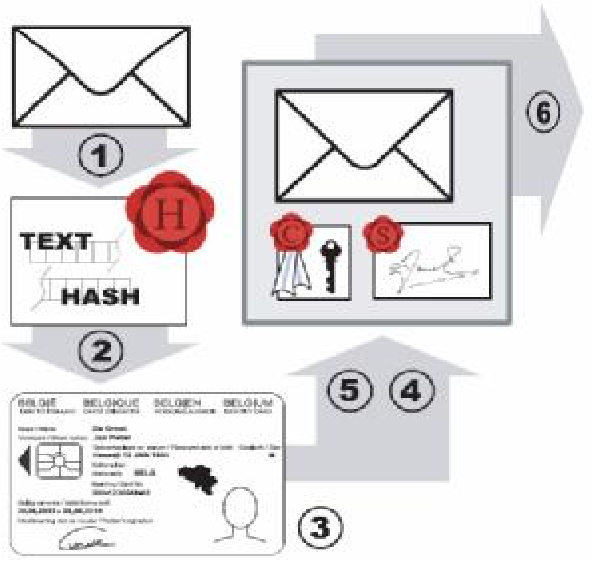

Figure 3. e-signing of a document.

Alice writes (1) some text for Bob. She puts her eID card into the reader and the eID chip computes (2) the cryptographic hash on the message to be signed. She also presents (3) her PIN code. The eID card generates (4) a signature on the hash and the application collects (5) the digital signature from her eID card. This package (containing the digitally signed message and the certificate) is send (6) to Bob.
Figure 4 [11] shows now how the digital signature will be verified.

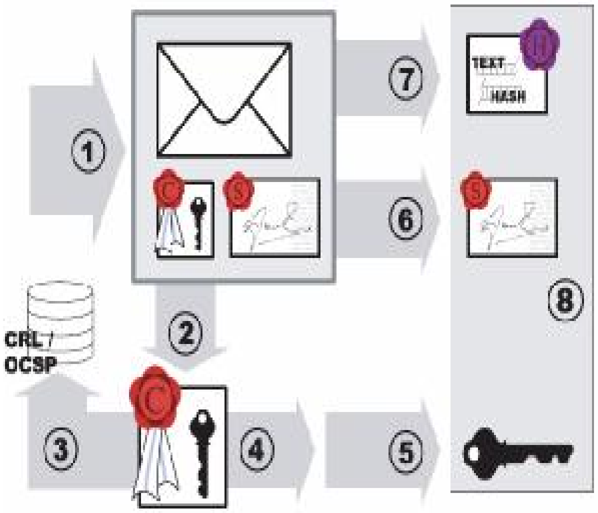

Figure 4. Verifying digital signature.

Bob receives (1) an "envelope" with the digitally signed message and the certificate from Alice. The sender's certificate is retrieved (2) from this information package and its revocation status is checked (3) by consulting a CRL/OCSP-server. At this point, the certificate is declared valid or invalid. If the declaration is invalid, then the signature is considered as invalid. The checking process stops here. In the case of a valid certificate (4), Alice's public key is extracted from the certificate (5) and the signature is retrieved (6) from the message. As result of the valid declared certificate, a new hash on the received message is calculated (7). Finally, the signature is declared valid/invalid (8) , based on the computation of hash, digital signature and the certificate. If the verification succeeds, Bob knows that the eID card of Alice was used to produce the digital signature.

IV. ISSUING PROCEDURE

During the pilot phase, about 4.500 eID cards were issued each month. Once up to full national production, some 1.500 eID cards are provided and activated each working day.

By 2009, all Belgian citizens over the age of 12 will have their own eID card, making a total of over 8 million cardholders. The Belgian government has not only developed middleware [6] to enable the large-scale deployment of low-cost eID-compatible smart card readers, but has distributed more than 125 000 readers to youngsters receiving their first eID card at the age of 12.

The identity card is to be replaced in the municipalities in the following cases:

- at the validity term of the identity card
- when the holder wants an identity card in a language different than the one it has been established
- when the holder's photo is no more compatible
- when the identity card has been damaged
- when the holder changes his first or second name
- after loss, destruction or robbery of his e-card
- on request of the holder.

When a citizen has to receive an eID card, a complex process [7] is started. The citizen first attends a government office to request the eID card, using their existing paper-based card to prove their identity. Their photo is captured. A few weeks later, the citizen will receive a letter with a PIN and a card activation code in the post. The citizen returns to the government office to collect the card, taking that letter with them. The information in the letter is used to activate the eID card, which will be exchanged for their current paper-based passport. The citizen will generate two test digital signatures: one identity and one qualified signature to prove the proper functioning of the eID card. The cost to the citizen is about 12,5 Euros.

V. APPLICATIONS

In conjunction with the private sector, the Belgian federal government has supported developer road shows to promote the integration of the eID card in e-government applications. This has resulted in an eID-compatible application [8] portfolio range: both the public and the private sectors have already developed a significant number of applications [9] and services compatible with the Belgian e-ID card.

Here are *some actual applications:*

- Online consultation of your National Register file
- Online income tax declaration
- Access control to container parks, library, …
- Electronic declaration of birth and death
- Online car license plate request
- Electronic submission of conclusions in court cases
- Access to patient files (e-Health)

The federal government is not yet considering the integration of the social security card or the citizen's driving license, because of incompatibilities with the Belgian legislation [5] [10].

The lack of smartcard readers installed in computers, is an obstacle for the wider use of eID cards. Therefore, an initiative is started between the government, the banks, Zetes (eID manufacturer) and the PC manufacturers to come to one reader standard and to integrate those readers in the keyboards of all computers delivered in the Belgian market in the next few years. These readers will then be compatible with eID and other cards in the mid term.

VI. CONCLUSION AND COMMENTS

This short paper cannot do justice to a rich and complex topic such as eID, but it has highlighted some of the main current issues in the use and adoption of eID cards.

The Belgian eID card programme is already well advanced. It offers the prospect of improved reliability and security and provides a framework where identities can be exchanged safely between the mix of identity providers, providing a good fit legally and to the nature of identity itself. . It is clear that the applications availability (concerning both government and private sector applications) will be the key element for success of this type of government project.

REFERENCES

[1] J. Deprest, F. Robben, "E-government: the approach of the Belgian federal administration", Brussels, http://www.law.kuleuven.ac.be/icri/frobben

[2] R. Depoortere, "10 million Belgian electronic ID cards", Zetes Corporate Division, 2005

[3] D. De Cock, "The Belgium National eID Card Program", 2007, http://homes.esat.kuleuven.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf

[4] Zetes nv and Certipost (Oct 2003), "eID usage in Belgium"

[5] D. De Cock, "Introduction to the Belgian eID card BELPIC", 2004

[6] Belgium's eID portal, http://eid.belgium.be/

[7] J. Fischenden, "Identity management in an online world", ntouk.com/papers/eID.doc, 2005

[8] iLoket 2007, Available: http://www.iloket.be/

[9] E-government Vlaanderen, http://www3.vlaanderen.be/e-government/

[10] ESC TB1 Public Identity, "Open Smart Card Infrastructure for Europe", http://www.ebusinessforum.gr/old/content/downloads/e-ID%20White%20Paper.pdf

[11] Alexander Goossens, "eID Wat is het?", thesis KHL, 2004.

[12] Belgian Official Journal, "Belgian law on the introduction of the use of telecommunications methods and of the electronic signatures in legal and non-legal procedures", 2000.