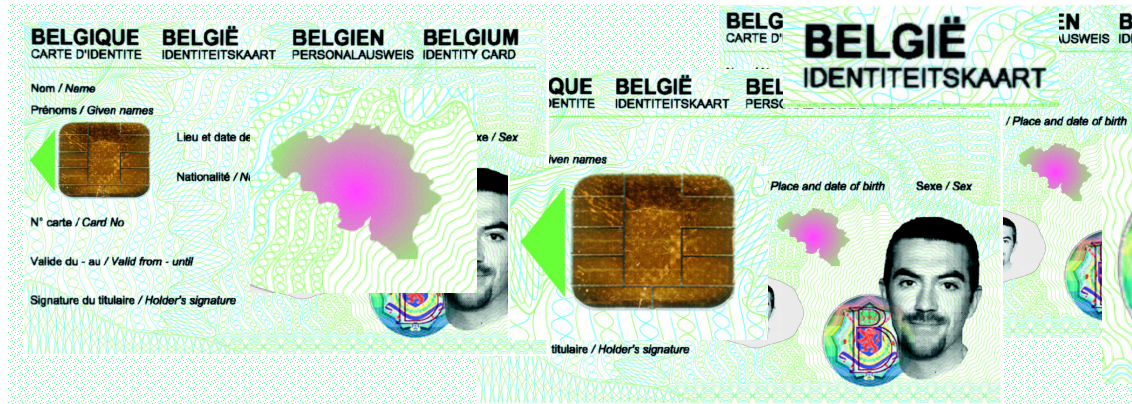


## Electronic Identity Cards and Electronic Signatures



## BELPIC (Belgian Personal Identity Card) What is an electronic identity card?

Introducing electronic identity cards is part of the Belgian e-government project, which aims to simplify and update administrative services. Electronic identity cards are next generation identity cards. They are even slightly smaller than the current Belgian identity card, about the same size as a credit card. The main difference from the old system lies in the microchip embedded in the front of the card. This chip contains the same information found on a standard Belgian identity card: surname, first name, date of birth, place of birth, sex, nationality, National Register number and a photo of the card holder. However, in the future other information pertaining to the card holder, which will not be visible on the actual card surface, will also be stored in the chip. This information will initially be limited to the holder's place of residence but, thanks to this information, he/she will no longer need to apply for a new card every time he/she changes address. Later the card will contain identity and signature keys and certificates, for which official certificates will be issued. The card will also include data required to authenticate itself, protect electronic data and use authorised certificates.

### What are electronic identity cards used for?

Initially, the new card's primary function will be the same as that of the old card: identifying and authenticating the holder. The advantage of the new card, however, is that this process will no longer need to be visual, via the physical presence of card and holder: thanks to a certificate stored in the card's chip, Belgians will be able to identify themselves remotely. Holders may even use personal digital signatures to certify the authenticity of data transmitted via the card.

In the future, the card's remote identification capabilities will enable users to access dedicated Internet applications. These will initially be e-government services.



However, private companies would also eventually be able to offer their customers services that may be accessed using electronic identification, via the new identity card. A later stage of the project aims to enable card holders to certify legal documents using digital signatures applied with their electronic identity card. The new card will therefore serve to further the development of e-business and e-government. Indeed, documents signed electronically using the card would have the same legal value as those that are nowadays signed by hand, from tax return forms to international business contracts. Once digital signatures are recognised everywhere in the world, this process will be more secure, thereby contributing to the definitive breakthrough of e-business of all types.

## How does the application process work? How will electronic identity cards be issued and activated?

The system will work as follows:

The citizen takes his/her invitation form and a passport photo to his/her local town hall. The photo is attached to the application form, which must be signed by the applicant and the attending town hall employee.

Applicants may decide if they want to use electronic signatures or not. Should they opt for this service, they must sign a second form to authorise the inclusion of the signature on the card. This form is kept by the municipality. The price of the card stays the same, whether it contains the electronic signature or not.

About two weeks later, the applicant will receive a letter informing him/her that the card is available for collection at the town hall. The letter will also indicate the user's PIN and PUK codes, protected by a scratch-off panel. The PIN (Private Identification Number) is a four-digit security code, similar to those issued with bank cards. The PUK (Personal Unblocked Key) is an activation key. This code is entered once to activate the card and the data it contains.

The applicant then takes the letter to the town hall where an employee will activate the card and check its digital signature, if the latter has been requested. Cards without digital signatures are secured via the activation of the PUK code.

In order to create an electronic signature, the card holder must enter his/her PIN code. The system will then verify that the correct code has been entered. If this is the case, the card is available for use; if not, the code must be re-entered. If the card holder enters an incorrect code four times, the card will be blocked.

If the card is defective, it will either be retained by the municipality or the holder will continue to use it without the digital signature until a new card is issued. The town hall employee will be informed of any problem with the card reader via an error message on the screen. If the employee is unable to resolve the problem using predefined procedures, he/she may contact the 24-hour helpdesk at the Federal Public Service Home Affairs.

Once the card is activated and the town hall employee has presented it to its owner, the latter may then opt to change his/her PIN code.

## What happens on the other side of the screen?

The request for a new electronic identity card is sent by the municipality to the National Register, which coordinates the different players involved in producing the card, making it secure, etc.

• The National Register then requests the authentication certificate and digital signature (if necessary) for the card from the certification authority. The card manufacturer delivers the security keys, which are then checked by the National Register to ensure they are unique (using the public key, since the private key cannot be read). Next, the National Register collates all the data in order to compile the certification request for the key pair that has just been validated. This request functions via a certificate number sent to the certification authority. This certificate will feature directly on the electronic identity card.

## FAQ

### • What is a certificate?

A certificate is an electronic document that enables a link to be established between the security keys and the card holder, amongst other things. It contains information about the card holder, the public key and the address of the certification authority. Certificates are signed with a private key issued by the same certification authority. The card also contains the certification authority's public key, which enables the validity of the certificate to be gauged.

### • From a technical point of view:

The electronic identity card uses a PKI system to secure the identification process and exchanges made via the card.

### • What is PKI?

PKI (Public Key Infrastructure) is a secure method for sending and receiving data. It uses a key pair that has been guaranteed as being fully functional by an independent certificate authority. Two key pairs are issued with the electronic identity card: one for identification and the other for the electronic signature.

### • How does a key pair work?

A key pair works according to the principle of asymmetric encryption. The private key is encoded onto the card but its value remains secret. The public key is used by third parties when data has been encoded with the private key. The two keys are of course completely different. Data encrypted with one key is then decrypted with the other. The private key therefore remains hidden from third parties, enabling only its owner to encode or decode messages and is also protected by a PIN code. If the card holder wants to send a message to a specific person, the opposite procedure can be used. He/she would request the recipient's public key and use it to encode the message to be sent to said recipient. As a result, only the owner of the corresponding private key would be able to decrypt the message.

### • What is an electronic signature?

Electronic signatures take this process one step further: not only are messages encrypted but they are also transformed into code using an algorithm. The code and the message are encrypted using the private key and sent to the recipient. The latter decrypts said code and message using the public key. The recipient then encodes the message using the same algorithm, which should produce the same code. The two codes are compared; if they are identical, the recipient knows that the message comes from the sender and that the transmission has been successful.

## STERIA and the Belpic Project

The Belgian government contracted Steria to implement the following measures:

- to adapt the National Register database in order to prepare for the introduction of electronic identity cards
- to open access to data stored on the National Register mainframe via the Internet and application servers
- to implement a new network infrastructure in order to establish secure links between municipal departments and the National Register servers
- to provide card readers and other hard- and software for the Population Departments of the municipal administrations (around 600 in Belgium) enabling cards to be requested, activated and distributed and, in the future, for reading and modifying individual card holder data.
- and, at the same time, to train the employees of the National Register and the various municipalities. As the project advances, Steria is also to provide any further training that is required.
- to set up a helpdesk to provide support for the National Register in the event of any problems that may occur.



[www.steria.be](http://www.steria.be)  
Boulevard du Souveain 36  
1170 Bruxelles  
+32 2 566 66 66