Legal aspects of the introduction of the electronic identity card in Belgian law by the Act of 25 March 2003[1]

OLIVIER GOFFARD AND EMMANUEL ROGER FRANCE

Introduction[2]

Traditionally, the identity card is regarded as a document *"certifying registration in the population register"*,[3] proving certain aspects of the civil status of its bearer. While the population register was instituted in Belgium by the French occupying authority in 1792,[4] it was not until the end of the First World War that the well-known obligation was imposed on the municipal authorities to issue an identity card to every person aged 15.[5] The identity card is currently issued by the population section of the municipal authority to Belgians and foreigners who are admitted or authorized to settle in Belgium.[6] From then on, like in most countries in the world, this document has been issued in paper format.[7]

This practice, which is soon to become a century old, was however, to witness a small revolution with the introduction in Belgian law of the electronic identity card by the Act of 25 March 2003.[8] By doing so, the Belgian legislator has added a stone to the construction of what is sometimes already called e-government, which is defined as the *"basically new, integrated and continuous way of providing services by making maximum use of the possibilities of the new information and communication technologies"*.[9] This Belgian initiative is in line with a wider European trend, aimed at the development of information technology infrastructures allowing the use of information and communication technology for easier, more accessible and more transparent communication between citizens and government.[10]

This trend is aimed, first of all, at making life easier for the citizens by giving them a "tool" enabling them to gain access in an easy and user-friendly manner to most public services,[11] through the use of new technologies and more particularly

[1] The present contribution is a completed and adapted version of an article that has previously appeared in *"Aspects juridiques du paiement électronique"*, collective work, T.2, (Kluwer, 2004), p.123.

[2] The present article only reflects the personal views of its authors. The authors wish to thank V. Musin, P. Collette and B. Lempkowicz for their contributions.

[3] See www.registrenational.fgov.be.

[4] Obliging each municipality for the first time to keep *"a register of inhabitants with their names, forenames, place of birth, last domicile, occupation, trade and other means of subsistence"* in order to facilitate the ten-yearly census. Those registers, however, fell into disuse under the Dutch occupation. The Act of 2 June 1856 concerning the general census and the population registers once again linked with the ten-yearly census the obligation to keep municipal population registers in order to allow the calculation of the annual population figure and the establishment of certain figures between two censuses (cf. http://rijksregister.fgov.be/bev_fr/voorstelling/bev_f_voorstelling_d.htm).

[5] See Royal Decree of 6 February 1919, adopted on the basis of the aforesaid Act of 2 June 1856 (footnote above).

[6] Article 6 of the Act of 19 July 1991 concerning the population registers and identity cards, amending the Act of 8 August 1983 organizing a national Register of natural persons, *Moniteur Belge* of 3 September 1991, p. 19075.

[7] For an analysis of the traditional identity card, see WARRANT, F., *"La réglementation belge en matière de carte d'identité"*, *Dr. inform.* 1987, p. 115.

[8] Act of 25 March 2003 amending the Act of 8 August 1983 organizing a national Register of natural persons and the Act of 19 July 1991 concerning the population registers and identity cards, amending the Act of 8 August 1983 organizing a national Register of natural persons, *Moniteur Belge*, 28 March 2003, p. 15921.

[9] See http://www.belgium.be/eportal/index.jsp and Wall-on-line, "Le projet wallon d'E-Gouvernement", p.5 , which also gives the following definition: *"E-government is the gradual transformation of the internal and external relations of the public sector through the information and communication technologies"*.

[10] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p. 23.

[11] Such services include application for a license plate, reporting accidents at work, VAT returns, granting access to a waste sorting park, library or swimming pool, etc.

the internet. In doing so, it is hoped that long queues and inconvenient opening hours will become a thing of the past by making it possible to perform the necessary formalities through the use of the new electronic identity card from a personal computer, at any time of day or night. In this connection, we should also draw attention to the initiatives aimed at standardizing the procedure so that data concerning a particular citizen only needs to be entered once and subsequently made accessible to all public officials who need to consult them, without the citizen each time having to repeat the procedure.[12]

The additional benefit that the new electronic identity card is expected to offer is also sought to make government administration run more smoothly. The card should be able to speed up the process of transmitting administrative documents and avoid the accumulation of an excessive backlog. It is for these reasons that many European countries have begun creating and using electronic identity cards. Italy,[13] Finland,[14] and Sweden[15] have already reached the stage of large-scale use. France[16] and Spain are going to launch their national electronic identity card in the coming years so that a mass rollout of the former identity cards could be achieved for 2008.

In Belgium, a step towards electronic administration has already been taken in industry with initiatives such as DIMONA[17] and on-line VAT returns.[18] A further step was taken in April 2003 when the electronic identity card was issued to citizens in eleven pilot municipalities.[19] The card was also issued to certain specific target groups such as certain public officials and liberal professions so that they should set an example in terms of the social benefits of the new electronic identity card.[20] The actual decision to proceed with the general introduction of the electronic identity card was taken by Royal Decree in 2004,[21] in accordance with the provisions of the law,[22] with a view to achieving the entire replacement of all existing identity cards with electronic identity cards by the end of 2009.[23]

The present study will examine in more detail certain legal questions connected with the introduction of the electronic identity card.

We will first consider the new legal functions that are presented by the electronic identity card, namely "authentication" and "electronic signature". We will also address the question of the modalities for reporting loss or theft of the card as well as the implications, notably in terms of the responsibilities linked to any fraudulent use that may result. The issue of the information contained on the card, and more particularly information that is not legible to the naked eye, such as the address, will also be discussed, notably

The additional benefit that the new electronic identity card is expected to offer is also sought to make government administration run more smoothly

[12] The FEDMAN network (Federal Metropolitan Area Network) has thus been set up in order to link up all government bodies electronically. This initiative is also aimed at reducing the number of forms used and consequently at substantially cutting costs. For more information about FEDMAN, see http://www.belgium.be/eportal/index.jsp.

[13] For more information, see: http://www.itworld.com/Man/2681/itwnews010319italy/; http://dgrc.org/dgo2004/disc/posters/tuesposters/rp_arcieri.pdf; http://www.infosec.co.uk/ExhibitorLibrary/168/ItalianID_CaseStudy.pdf.

[14] For more information, see: http://europa.eu.int/idabc/en/document/2649/334; http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/fineidcase/case.html.

[15] For more information, see: http://interop-esa05.unige.ch/INTEROP/Proceedings/eGovScientific/papers/42.pdf.

[16] For more information, see: http://www.infoworld.com/article/05/04/12/HNfrenchbiometriccards_1.html; http://www.electronic-identity.org/porvoo/2/france.ppt.

[17] DIMONA (Déclaration IMmédiate – Immediate Declaration) is an electronic social security declaration system, which is compulsory for all employers in the private sector. Every commencement or termination of employment must be communicated immediately to the Department of Social Security (ONSS), Circular N°522, 6 June 2002, *Moniteur Belge* 26 July 2002, p. 33314.

[18] See http://www.belgium.be/taxonweb/app/citizen/public/taxbox/home: facility introduced by the Royal Decree of 27 March 2003 establishing an electronic declaration system, *Moniteur Belge*, 4 April 2003, p. 17197.

[19] Borsbeek, Geraardsbergen, Jabbeke, Lasne, Louvain, Marche-en-Famenne, Rochefort, Seneffe, Seraing, Tongres, Woluwé-Saint-Pierre (Article 1 of the Royal Decree of 25 March 2003 establishing transitional measures in connection with the electronic identity card, Moniteur Belge, 28 March 2003, p.15942), i.e. around 330,000 inhabitants. 65,000 electronic identity cards had to be issued per year during the trial period.

[20] For more details we refer to the Royal Decree of 30 November 2003 amending the Royal Decree of 25 March 2003 establishing transitional measures in connection with the electronic identity card, Moniteur Belge, 12 December 2003, p. 58956.

[21] Royal Decree of 1 September 2004 concerning the decision to proceed with the general introduction of the electronic identity card, Moniteur Belge, 15 September 2004, p. 67527. This Royal Decree is accompanied by a Royal Decree amending the Royal Decree of 25 March 2003 establishing transitional measures in connection with the electronic identity card, Moniteur Belge, 15 September 2004, p. 67528.

[22] Article 19§1 of the Act of 25 March 2003, o.c.

[23] At the information meeting of FEBELFIN on 10 March 2004, the date announced for the general introduction was 2007 (WYNANT, P., "De elektronische identiteitskaart in de financiële praktijk. Inleiding"). Meanwhile, the Council of Ministers had decided in May 2004 to delay the general introduction of the electronic identity card by two years until the end of 2009. This decision was based on an evaluation report of the House of Representatives on the introduction of the electronic identity card (Parliamentary documents, House of Representatives, Session 2003-2004, 51, 1094/001, p. 3).

in terms of its compatibility with other laws and regulations imposing the legibility of this address. Other questions connected with security will also be dealt with. Finally, this analysis concludes with a description of the procedure for issuing the card as well as a brief enumeration of the applications currently available and the outlook for the future.

The new legal functions presented by the card: authentication and electronic signature

■ The identification function

Unlike the present identity card, whose sole purpose is to identify its bearer, the new electronic identity card also presents two additional functions: in addition to the identification, in its strict meaning, of its bearer (by reading the data on the card that are legible to the naked eye), the new card contains authentication and electronic signature functions that enable the bearer to legally commit himself towards the public authorities or in the context of business relations.

The conventional identification function of the identity card is that where the data identifying the bearer are read from the card on which they are printed in such a manner that they are visible to the naked eye (name, forename, photograph, etc).

Generally speaking, any identification function can take place in a passive manner from the point of view of the person concerned, that is to say, without his consent, and even without his knowledge (consider for example the mechanism for controlling access to certain buildings where entry is authorized simply by camera control allowing the guard to check the identity of visitors).[24]

As is already the case with the conventional identity card, the identification function of the new electronic identity card does not involve any special handling operation if it merely concerns the physical presentation of the card for the purpose of verifying the identity of its bearer.

We should remember in this connection that the cases in which a bearer can be obliged to show his identity card are restrictively enumerated by law.[25] Thus it is specified that the card must be shown whenever the police so requests, as well as with any notification, request for certificates and in general for the purpose of establishing the identity of the bearer. It must also be shown to a bailiff serving a writ. If the electronic identity card is to fully play its part as standardization tool, we may ask ourselves whether it would not be a good idea to revise these regulations in order to enlarge the scope of cases where identification is required, taking into account the new possibilities opened up by the electronic identity card.

Moreover, still on the subject of identification, it should be pointed out that Article 6§4 of the Act concerning the electronic identity card imposes a prohibition on automatically verifying the identity of a citizen by means of the electronic identity card without his consent. This provision stipulates that the electronic identity card cannot be used without special authorization as an authorization badge to enter a building. The law also specifies that any automated verification of the card by means of optical or other reading processes must be ratified by Royal Decree. This provision, however, only applies to automated verification, namely verification without human intervention, and does not seek in any way to limit the contractual freedom of two opposite parties. It therefore seems permitted to provide in a contract that the electronic identity card may be used for verification purposes insofar as the citizen has given his consent beforehand.

Nevertheless, this physical presentation of the card does not in itself prove the true identity of the bearer; it simply furnishes certain elements of proof in this respect. Indeed, apart from the photograph which currently constitutes the principal identifying element, how can one be certain that the written data actually relate to the bearer of the card and that they have not been falsified, for instance?

Moreover, this identification function alone does not in itself offer an adequate solution to allow remote communication with government authorities, for example over the internet. These are probably some of the reasons why the legislator considered it expedient to incorporate the electronic authentication function in the identity card. The conventional identification by physical presentation of the card by the bearer, for reasons of inadequate security, is thus meant to play a less important role in the future and only to apply to legal acts with a lower level of importance.

■ The electronic authentication function

The electronic authentication function is

[24] SYX, D., "Vers de nouvelles formes de signature? Le problème de la signature dans les rapports juridiques électroniques", *Droit de l'informatique,* 1986, p. 134.
[25] Article 1, Royal Decree of 25 March 2003 on identity cards, *Moniteur Belge*, 28 March 2003, p. 15935.

intended to enable the bearer of the identity card to prove with "certainty" that he is indeed the person he claims to be. This is the "active" process where the bearer identifies himself electronically and voluntarily.[26]

This function calls for a specific handling operation. The bearer of the electronic identity card has to insert it into an appropriate reader (terminal) and enter a secret code (PIN code), which he alone is deemed to know (similarly to the way in which bank debit cards are used today). If this secret code is correct, the terminal sends a message to the recipient (for example government services) authenticating the bearer's identity. From a purely technical point of view, the entry of the PIN code actually unlocks a private electronic key contained in the microchip of the electronic identity card, which in turn generates a cryptogram (i.e. a message composed by means of a coded system).

This cryptogram is created in a "dynamic" way by the card each time the PIN code is entered. It will therefore be randomly different each time the card is used, and thus constitutes an additional security measure.[27] This technique is one of the many security elements of the electronic identity card that are designed to prevent the card from being counterfeited all too easily.

This new function is meant to offer several advantages. The use of this electronic authentication may be considered in the future for the purposes of secure connection to any internet site. The use of the authentication certificate will thus suffice to prove one's identity in order to obtain access to a particular website. To this end, the creation of a standardized access platform may be contemplated, which could introduce a certain degree of standardization in the current diversity existing in this area.

■ The electronic signature function

The electronic signature function will also be contained in the new card. This will allow the bearer to electronically sign a message and thus mark his approval of its contents. Similarly, the card may of course be used to sign e-mail messages or mark one's approval of certain documents, either over the internet or at the counter of a bank, hotel or car rental firm. But what is the legal value of the electronic signature of an electronic identity card?

■ Principles applicable in this area

The Acts of 20 October 2000[28] and 9 July 2001[29] are concerned with introducing and defining the concepts of electronic signature.[30] Furthermore, they regulate the probative and legal value of certain types of electronic signature. In principle, those acts only apply in the case of "open" networks, where the parties to this network are not linked to each other beforehand by private law contracts (generally on paper) that legally regulate beforehand between the parties the implications of operating in that network (notably the question of the probative value between the parties of the use of the PIN code or the electronic signature).[31]

Given that the internet – the open network *par excellence* – is to be the means of communication in the area of e-government, the Acts of 20 October 2000 and 9 July 2001 should in principle apply to the relations between citizens and government services and, in particular, to the electronic signature generated by the electronic identity card. It is worth noting that the Act of 9 July 2001 on electronic signatures makes a distinction between 'simple' electronic signature and 'advanced' electronic signature.

From a purely technical point of view, the entry of the PIN code actually unlocks a private electronic key contained in the microchip of the electronic identity card, which in turn generates a cryptogram

[26] SYX, D., "Vers de nouvelles formes de signature? Le problème de la signature dans les rapports juridiques électroniques", *o.c.,* p. 134.

[27] This mechanism therefore differs from cards with a "static" authentication mechanism, where the cryptogram is loaded once and for all on the card when it is created (called personalization) and remains unchanged thereafter.

[28] Act of 20 October 2000 introducing the use of telecommunication media and electronic signature in judicial and extrajudicial procedure, *Moniteur Belge*, 22 December 2000, p. 42698.

[29] Act of 9 July 2001 establishing certain rules governing the legal framework for electronic signatures and certification services, *Moniteur Belge*, p.33070.

[30] For a more thoroughgoing analysis of those texts, we refer to STORME, M., "De invoering van de elektronische handtekening in ons bewijsrecht-een inkadering van en commentaar bij de nieuwe wetsbepalingen", *R.W.*,2000-2001, p.1505; DE CLIPPELE, F., "Wettelijke regeling voor de elektronische handel", *R.D.C.* ,2001, p.329; GOBERT, D. and MONTERO, E.., "La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle", *D.A.O.R.*, 2000, p.17; GOBERT, D. and MONTERO, E., "L'ouverture de la preuve littérale aux écrits sous forme électronique", *J.T.* , 2001, p.113; ROGER FRANCE, E. and DE GROOTE, E., "La valeur probante des signatures électroniques –Réseaux fermés, réseaux ouverts et opérations effectuées au moyen d'instruments de transfert électronique de fonds", *R.D.C.* 2002, p. 185; VAN EECKE, P., "Bewijsrecht en digitale handtekeningen: nieuwe perspectieven", *in* le droit des affaires en évolution. Le commerce électronique, *A.B.J.E.*, n°10, Bruylant-Kluwer, 1999, p.233.

[31] A typical example of a closed network is that constituted by the environment in which bank cards are used, where the secret banking code is contractually equated with a handwritten signature.

A 'simple' electronic signature is defined as *"a data element in electronic form which is logically joined or linked to other electronic data and which serves as authentication method"*.[32] This may, for example, be a PIN code.

An 'advanced' electronic signature is defined as a 'simple' electronic signature which in addition satisfies other supplementary requirements, namely:

- the ability to identify the signatory (identification);
- the fact of being linked exclusively to the signatory (authentication);
- being created by means of which the signatory can keep under his exclusive control (security);
- being linked to data to which it is connected in such a way that any subsequent changes in the data are detectable (integrity).[33]

The Act of 9 July 2001 establishes the *"principle of assimilation"*[34] assigning to (1) an 'advanced' electronic signature the same probative value as a handwritten signature, on condition that this signature was (2) produced on the basis of a "qualified certificate"[35] and that it was (3) created "by means of a secure device for creating electronic signatures".[36] This type of electronic signature is sometimes called "qualified electronic signature"[37] or "strong signature".

The term advanced electronic signature testifies to the choice of the Belgian legislator in favour of technological neutrality. At present, technically speaking, only the digital signature using asymmetric cryptography, such as the RSA[38] type signature, answers this definition. If, in addition, this electronic signature technology is based on a PKI[39] type infrastructure of electronic certificates, the end result, termed secure signature, will ensure that the electronic signature thus created satisfies the conditions for being equated with a handwritten signature.

With the RSA technique, a secure signature is created through a correlation between a pair of asymmetric electronic keys, constituted by a private[40] key on the one hand and a public[41] key on the other. Unlike with symmetric cryptography mechanisms, there is no shared secret between the two parties since the private key remains incorporated in the card held by the bearer and the public key is freely accessible. The PKI technology is the infrastructure surrounding the RSA technique which, through the use of certificates[42] issued by certification service providers (CSP), offers certainty that the signature can be considered trustworthy by ensuring proper agreement between the public key and the identity of the holder. This link will be confirmed by the various data contained in the certificate and which ensure that this certificate can be called a qualified certificate.[43] As we will see, this certificate always has a limited period of validity and may even be revoked in certain cases.[44]

[32] Act of 9 July 2001, Article 2, o.c.
[33] Act of 9 July 2001, Article 2, o.c.
[34] Article 4§4 of the Act of 9 July 2001.
[35] A qualified certificate is a certificate bearing certain references listed in Annex 1 to the Act of 9 July 2001 and issued by a certification service provider satisfying the conditions established in Annex 2.
[36] The requirements imposed on those secure electronic signature creation devices are listed in Annex 3 to the Act of 9 July 2001. It should also be noted that, besides the principle of assimilation, Belgian law has also established the principle of non-discrimination against electronic signatures that do not satisfy the three conditions laid down by the principle of assimilation. It is expressly provided that, besides the conventional handwritten signature directly affixed to a document, an electronic alternative is now admissible in court. In practice this means that a 'simple' electronic signature can no longer be refused as evidence in court on the sole ground that it is in electronic form or that it is not based on a qualified certificate issued by an accredited certification service provider (Article 4§5 of the Act of 9 July 2001).
[37] JACOBS, E. "Authenticatie en elektronische handtekening in elektronisch bankieren", in *Juridische aspecten van de elektronische betaling T.1.*, Kluwer 2004, p. 179.
[38] Named after the founders Rivet, Shamir and Adleman.
[39] Public Key Infrastructure.
[40] This can be defined as a mathematical key, which is kept secret by its holder, and is used to create an electronic signature and, depending on the algorithm, to decrypt messages or files encrypted with the corresponding public key (http://www.signatureelectronique.be/glossary.cfm). See also the reading list in MASON, S., *Electronic Signatures in Law*, pp 101 –102.
[41] This can be defined as a mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files, which can then be decrypted with the corresponding private key.
[42] I.e. "an electronic certificate that links the data connected with signature verification to a natural or legal person and corroborates the identity of that person", see Article 2, 3° of the Act of 9 July 2001, *o.c.*
[43] Those data are: specification that the certificate has been issued as a qualified certificate; identification of the CSP as well as the country where it is established; the name of the signatory or a pseudonym which is identified as such; the possibility to include, where appropriate, the specific capacity of the signatory for which purposes the certificate is intended; data connected with signature verification which correspond to the data for signature creation under the control of the signatory; starting date and expiry date of the certificate; identity code of the certificate; the advanced electronic signature of the CSP issuing the certificate; restrictions on the use of the certificate and, where appropriate, the maximum value of the transactions for which the certificate may be used.
[44] Articles 12 and 13 of the Act of 9 July 2001, *o.c.*: if the holder requests it in a discretionary manner, if the identification of the holder has changed, when the accredited CSP so requires and, finally, for obvious security reasons.

In its concern to achieve the highest level of security, the law requires that the CSPs be accredited within the meaning of the Act of 9 July 2001. This accreditation is subject to a double basic obligation. First of all, the CSP must comply with certain qualitative obligations[45] and must issue qualified certificates.[46] Secondly, the CSP must use secure signature creation devices.[47]

The CSP may be obliged to suspend or revoke a certificate. It must notify all users thereof by means of a revocation list, called Certificate Revocation List (CRL). This list will be published periodically on the website of the CSP,[48] containing the electronic signature of a CSP and the references of the certificates that are marked as suspended or revoked before their expiry date. The list will generally mention the name of the issuer, the date of issue, the next issue date, and the serial number of the certificates that have been suspended or revoked, along with the exact moment and reason for the suspension or revocation. The list of suspended or revoked certificates will be accessible on-line so as to enable the government to keep its database up to date, even if it seems that keeping a database accessible and up-to-date is not so evident.[49]

■ Application to electronic identity cards

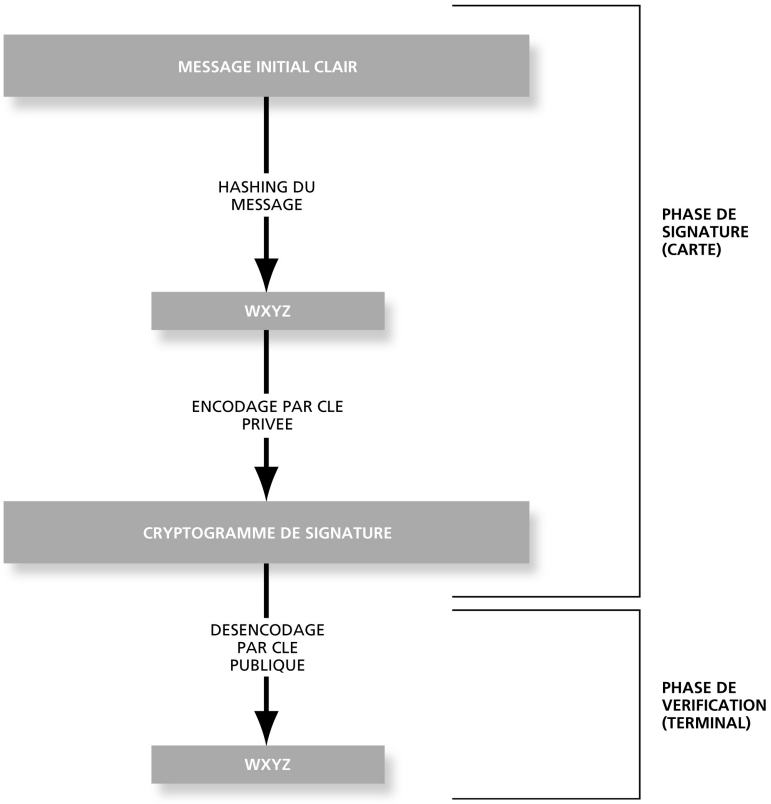
The government has naturally opted for the use of RSA technology and the PKI infrastructure to supply the new electronic identity cards with the electronic signature function, thus allowing their bearers to benefit from the principles of assimilation[50] and non-repudiation. Consequently, a person who electronically signs a document using his identity card should be entitled to the same protection as that offered to handwritten signatures.

To sign a message using an electronic identity card, it will nevertheless be necessary to have a PIN code and to have a card on which the electronic keys have been activated, with the private key remaining secret on the electronic identity card and the public key being known to everyone by means of a publication list.[51]

In practice, the signature function of the electronic identity card can be divided into two stages, the signature stage and the verification stage. The signature stage unfolds as follows: the bearer inserts his card into a terminal[52] and enters his secret code. The content of the message to be signed is transformed[53] into a sequence of symbols, for example WXYZ. The private key, which from the start is contained on the card (insofar as such a request has been made to the accredited certification service provider), then comes into action and encrypts the symbols WXYZ to create a signature cryptogram. The signature stage, which unfolds entirely on the card, is then completed and verification of the signature cryptogram begins. This stage unfolds entirely inside the terminal. The message that has been signed with the private key is read by means of the public key. This public key, which the terminal will have to obtain from the accredited certification service provider, interacts with the signature cryptogram and transforms it into a sequence of symbols. The terminal then verifies whether the symbols thus obtained are identical to those reproduced by the terminal itself, namely WXYZ. If the answer to this question is affirmative, the signature will be considered verified and valid.[54]

This signature function can be graphically represented as follows:

[45] Namely the conditions of Annex II to the Act of 9 July 2001.
[46] The various conditions necessary to be able to speak of qualified certificates are specified in Annex I to the Act of 9 July 2001.
[47] Namely those of Annex III to the Act of 9 July 2001.
[48] By way of example, we refer the reader to http://status.eid.belgium.be/crl/.
[49] For further comments on this subject, see MASON, S., *Electronic Signatures in Law* (LexisNexis Butterworths, 2003) paragraphs 5.32 – 5.33; 8.24 – 8.29.
[50] The Internet Rights Observatory advocates a sparing use of the "advanced" electronic signature in order to prevent it from becoming commonplace. It is indeed pointless to require an 'advanced' electronic signature in all cases where assigning a user name together with a password or using a PIN code would suffice. We believe that the 'advanced' electronic signature should be reserved for acts of high legal importance (for example to identify a holder wishing to use his on-line banking application). On the other hand, the PIN code of a bank card, which can be characterized only as a 'simple' electronic signature, retains its entire raison d'être for a series of legal acts of a lesser legal importance, such as cash withdrawals from cash dispensers (ATMs) (see Internet Rights Observatory, Success factors of e-government, Opinion no. 2 of the Internet Rights Observatory, p.11, available at http://www.internet-observatory.be/internet_observatory/pdf/advices/advice_fr_002.pdf.
[51] For users who have chosen the firm ISABEL as certification authority, a list of public keys called list X500 can be consulted on the internet site of that firm by using a proprietary application.
[52] We take the example here of a terminal, though this is equally applicable to a secure internet site.
[53] Using what is called a one-way function, which is an irreversible scrambling mechanism designed to transform a message into a sequence of symbols but without being able to reverse the process.
[53] This entire procedure is exactly transposable to the authentication mechanism, except that in the latter case, instead of encrypting a message that makes sense, the message to be encrypted makes no sense whatsoever (it is a number that is chosen *at random* by the card), so that the sole purpose of entering one's PIN code and the unfolding of the entire process is to authenticate the holder.



There is always a risk, in the absence of verification of the bearer's identity, that a dishonest third party who has obtained knowledge of the secret code of the bearer may use the card for fraudulent purposes

If the use of RSA technology tends to provide a technical certainty that the signature is correct, there still however remains the question who has signed. Was it indeed the person holding the public key that was used? It is in this respect that confidence in the PKI infrastructure acquires its full significance. To illustrate this, let us take the following example:

When Mr Y tries to get in touch with Mr Z for important information, the stages are structured in a similar way to our purposes. If Mr Y only has the name and address of Mr Z, how will Mr Y proceed to get in touch with him? By consulting the telephone directory, which will provide Mr Y with a telephone number. He will then dial that number and he will hear a voice. The question is: how can he be sure that this voice is indeed that of Mr Z? In our society, we assume that this will be the case, since a telephone directory generally offers a proper guarantee of reliability since it has been published by a trustworthy authority.[55]

When we replace the telephone number obtained from the telephone directory with the public key, the voice with the secret key, and the directory with the certificate[56] supplied by the CSP, it becomes clear that trust in the origin and reliability of the public key is essential.

What remains is to ascertain the contents of this certificate. Roughly speaking, the certificate contained in the card holds the information that a public key belongs to Mr Z. It also contains the signature of the certification authority, which has been placed there by the person obtaining the card. Nevertheless, how do we ascertain that this certificate is trustworthy? To this end, the terminal will use the public key of the CSP, which it trusts since it had been placed in the terminal right from the start. It will then apply the same structure of the RSA mechanism as that described above, but this time with the keys of the authority.

In accordance with the principle of non-repudiation of a signature, the holder who signed by means of his private key contained on his identity card will not be able to contest his signature, since he is presumed to be the only person to "know" it and able to use it.[57]

At present, the firm Certipost has been chosen in this connection as accredited CSP.[58] Besides its role as producer of certificates, its job will also be to verify that the public key belongs to the holder. To this end, it will issue a qualified electronic certificate, which will make it possible to link the identity of the bearer of the electronic identity card to his public key.

This being the case, even if from a technological viewpoint, the digital signature based on the RSA and PKI technologies is the only one that can be equated with a handwritten signature, the fact remains that a necessary precondition must always be required in order to be sure of the authenticity of the signature, namely that the person entering the PIN code during the signature stage is indeed the bearer of the card. There is always a risk, in the absence of verification of the bearer's identity, that a dishonest third party who has obtained knowledge of the secret code of the bearer may use the card for fraudulent purposes. Nevertheless, at the moment, entry of the PIN code is, in our opinion, the safest way to initiate the electronic

[55] This is already less the case if this number is obtained from an internet site, which is, by definition, more easy to falsify than a telephone directory.
[56] This certificate contains several references: the name of the accredited certification service provider, the name of the holder of the certificate, the unique identification of the certificate holder, the period of validity of the certificate, the serial number of the certificate, the signature of the certification service provider confirming that this information is correct.
[57] Editors note: this is not a legal presumption, it is a technical presumption, as the authors illustrate further on in this article.
[58] This accreditation is subject to a twofold obligation: firstly, the CSP must comply with certain qualitative obligations and must issue qualified certificates, and, secondly, the CSP must use secure signature creation devices.

signature mechanism. It seems to us that this risk can only be avoided from the moment that biometric type signatures are introduced, allowing identification and authentication of the card bearer by verifying one or several of his own physical features (generally by taking fingerprints or verifying the retina of the eye). It should also be noted that only half the memory of the electronic chip of the identity card will be used for the functions described above, thus leaving room for other applications.

One such application might be the payment function and electronic funds transfer function, even if this solution seems unlikely in the short term,[59] which we will discuss in more detail below, namely in connection with the consequences of fraudulent use following loss or theft. However, other functions may be considered too. Certain initiatives have already been taken in other countries to add biometric functions, electronic driving licence, system of direct payment by Social Security fund (replacing social security (SIS) card), amongst other uses.[60]

The major risks associated with concentrating, on one single electronic chip, all personal details and all the functions offered by cards in general (banking functions, social security card, badge for access to buildings, fan card, rail season ticket, etc) will undoubtedly become manifest in the future.

■ Length of storage of electronic certificates

The law stipulates that the electronic identity card is valid for five years. As has already been mentioned, these cards are provided with electronic certificates for authentication and electronic signature. The length of the encryption keys used is currently fixed at 1024 bits, at least until 2013. Thus it can happen that, from one moment to the next, a citizen can no longer use the certificates contained on the electronic cards, either because he has died, or because his card has expired, or because the length of the encryption key has changed, thus necessitating a renewal of the certificates. The question that comes up is how to prove in the future that an instrument has indeed been signed with an electronic signature, given that the certificates contained on the card at the moment when the question arises may be different from those used for signing the instrument in question? The legislation on electronic signatures[61] and the Act governing electronic identity cards[62] precisely answer this question by stipulating that the certification service providers and the National Register are obliged to keep a list of certificates used by each citizen for a period of 30 years. The parliamentary documents[63] show that this choice is in fact based on Article 2262 of the Civil Code, which provides for a thirty-year period.

A second unresolved question immediately springs to mind: what happens if an instrument or contract signed with an electronic identity card is contested more than 30 years after the signature certificates have been filed? Is this limitation to 30 years not likely to create a certain legal uncertainty, which the legislator should remedy?

Legal consequences of loss or theft of the card: notification and misuse

■ Notification of loss or theft of an electronic identity card

Unlike the Act of 17 July 2002 on electronic funds transfer,[64] which only provides for a general obligation for the issuers of bank cards to supply the holder with *"the appropriate means to enable him at any time to notify loss or theft of his or her bank card"*, without any further specification, the Act of 25 March 2003 distinguishes notifications made *"during or after office hours"*.[65] During office hours, notifications must be made *"to the municipal authority"*, which will issue a certificate of loss, theft or destruction of the electronic identity card. The municipal authority will in turn instruct the accredited CSP, through the National Register, to immediately suspend or withdraw the

[59] In our opinion, this public/private synergy will not be realized in the short or medium term, since every bank uses and knows its own security technique. Furthermore, how should the issue of branding of the cards be addressed? Will we find ourselves with an electronic identity card that is sponsored by a banking institution? Moreover, the target group of the electronic identity card and that of the bank card do not correspond. In any case, what interest do credit institutions have in investing in expensive RSA and PKI technologies whereas an electronic signature initiated by a bank PIN code is contractually equated with a handwritten signature, and therefore acquires the same legal value as the secure signature of an electronic identity card, without however complying with the legal stipulation which is solely applicable in an open network?

[60] Certipost, "White Paper. EID usage in Belgium", p. 6, available in electronic format at www.certipost.be/eID.

[61] Annex II, subparagraph i of the Act of 9 July 2001 establishing certain rules governing the legal framework for electronic signatures and certification services.

[62] Article 3, Act of 25 March 2003, *o.c.*

[63] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p. 10.

[64] Act of 17 July 2002 governing transactions carried out using electronic funds transfer instruments, *Moniteur Belge,* 17 August 2002, p. 35337.

[65] Article 16 of the Act of 25 March 2003, *o.c.*

electronic function of the card.

The term 'electronic function' is ambiguous to say the least. According to the preamble, it corresponds to *"the identity and/or signature certificates contained on the card"*.[66] After office hours, a helpdesk has to be set up at the National Register. This helpdesk will receive all notifications of loss or theft of the electronic identity card and will, where appropriate, suspend or withdraw the 'electronic function' of the card. The bearer must subsequently ask the municipal authority for a certificate of loss or theft.

If the card is retrieved within seven days following the notification, the municipal authority will instruct the accredited CSP to reactivate the electronic function. If the card is not retrieved within that time, the bearer must apply to the municipal authority for a new card. The municipal authority will cancel the lost, stolen or destroyed electronic identity card and ask the CSP to withdraw the 'electronic function' of that card, and will then launch the procedure for the production of a new card.[67]

According to the preliminary documents,[68] it has been maintained that this helpdesk is not comparable with "Card Stop" (helpdesk shared by all banks in case of loss or theft of a bank card) and that it is advisable that the municipal authority should remain the general point of contact in case of loss, theft or destruction of the electronic identity card. The helpdesk would have to be used only sparingly. From this point of view, *"a very elaborate helpdesk would be difficult to run and hard to justify financially"*.[69]

One may wonder about the practicality of this distinction as regards the moment when a loss or theft is notified. Would it not be likely to cause pointless confusion in the minds of the citizens? It should be noted that at present Card Stop already receives thousands of notifications of loss or theft of identity cards per year, without however being able to take action since this call centre is not designed for this! In those circumstances, it might be a good idea to consider setting up a permanent helpdesk, all the more so since the new identity card will be able to be used as a tool for authentication or signature, and thus liable to be used for fraudulent purposes. The texts that were subsequently adopted eventually brushed aside the financial misgivings that were raised during the debates and ultimately insisted on the permanence of the service to be set up.

The Act therefore now provides that the helpdesk must be *"permanently operational"* [70] without making any distinction between working hours and non-working hours. The implementing Royal Decree specifies in this connection that the helpdesk should be able to be reached *"seven days a week, twenty-four hours a day"*, after the example of Card Stop, by the bearer as well as by the municipal authorities, the police, the manufacturer, the initializer and the personalizer of the card.[71] It seems, however, that unfortunately the opposite message has been given to the municipal staff. In a document addressed to the municipalities entitled "General instructions concerning the electronic identity card", we read: *"In other words, the helpdesk will, on the direct request of a citizen, only take a notification of loss, theft or destruction of an electronic identity card if no such notification can be made to the municipal authority of the principal residence or the nearest police station (after working hours, public holidays, weekends, or other instances where the appropriate services cannot be reached)"*.[72]

■ Liability in case of fraudulent use

As was mentioned above, it is up to the bearer of the identity card to notify loss or theft. Following this notification, the electronic function of the card will either be suspended or withdrawn. What is the liability of a bearer who fails to notify such loss or theft, and whose card is then used for fraudulent purposes?

In this respect, it should be pointed out that in the area of *"electronic funds transfer instruments"* the legislator introduced a special liability arrangement,[73] under which the holder of this instrument (generally a bank card) is, in principle (i.e. apart from cases of fraud or serious negligence), liable up to an upper limit of one hundred and fifty euros until such time as he has notified the loss or theft of his card. The issuer of the card (generally the bank) is liable for all sums above that limit. After being notified, the issuer of

[66] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p.32.
[67] Article 6§2 of the Royal Decree of 25 March 2003 on identity cards, *o.c.*
[68] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p.32.
[69] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p. 32.
[70] Article 16 of the Act of 25 March 2003, *o.c.*
[71] Article 7 of the Royal Decree of 25 March 2003 on identity cards, *o.c.* The telephone number of this government helpdesk is +32(2)518.21.16 (French) or 518.21.17 (Dutch).
[72] See http://www.rijksregister.fgov.be/rrn_fr/cccie/circulaire/9mai/INSTRUCTIONS GENERALES CID MAI 2003.pdf.
[73] Article 8§2 of the Act of 17 July 2002, *o.c.*

the electronic funds transfer instrument will be liable for all financial consequences connected with the fraudulent use of this instrument.

So far, no such liability arrangement has been put in place by the legislator with respect to the electronic identity card. All fraudulent use will therefore be governed by common law. The utmost caution is therefore recommended, since the electronic identity card will in principle comprise the new electronic authentication and signature functions, fraudulent use of which is liable to cause considerable financial prejudice. An advanced electronic signature produced in the context of a transaction using a lost or stolen card will be legally equated with a handwritten signature produced by its bearer, with all the implications that this entails.

Assuming that, in the future, it will also be possible to activate a payment function on the identity card, we believe this will fall directly within the scope of the Act of 17 July 2002 on electronic funds transfers, which applies to *"any instrument allowing the performance, wholly or partly by electronic means, of one or several of the following transactions: funds transfers, withdrawal and depositing of cash, remote access to a bank account, charging and discharging of a rechargeable instrument"*.[74]

Less straightforward, however, is the task of determining the person who has to be considered as the issuer (who will in principle be liable for the financial consequences of any fraudulent use of the said funds transfer function, following notification). According to the Act of 17 July 2002, an issuer is considered to be *"any person who, as part of his business activity, puts an electronic funds transfer instrument at the disposal of another person in accordance with a contract concluded with that person"*.[75] Who would be concerned with respect to electronic identity cards? Should the liability of the State be involved or only that of the banks? We cannot avoid the conclusion that, at the current stage of technology, there is no clear legal solution that can be offered yet.

We can, however, try to extrapolate on the basis of certain funds transfer applications that are already operational in the field of m-commerce (or mobile commerce, generally using techniques provided by a mobile telephone). For example, one facility that already exists consists in recharging the prepaid card of a mobile telephone by means of the mobile telephone itself or, as is already the case in Finland, making payments directly with a mobile telephone. In the latter case, it would seem that the banks should at first sight be regarded as the issuers of the transfer instrument (rather than the mobile telephone operators), insofar as the legal rules governing the use of the payment function in m-commerce are contractually defined in the general banking conditions, which the cardholder has agreed to observe.

In this hypothesis, given a closed network, we may ask ourselves what benefit the banks would derive from choosing the digital signature of the identity card as a means of signature or authentication while the applicable liability arrangement is identical to that of a banking card.

Data appearing on the card: legal implications

■ Obligatory data and absence of address legible with the naked eye

Besides the signature of the bearer, the electronic identity card must bear the signature of the municipal official issuing the card, or, where appropriate, the signature of the post office clerk charged with issuing it. The signature of this official confirms that the identity of the bearer was verified when he presented himself at the town hall. In addition, there are a number of data that must appear on the card. Some of this information can both be read with the naked eye and be consulted by means of an electronic device, whereas other data can only be consulted electronically.

■ Data that are visible to the naked eye and electronically readable

Article 14 of the Act of 25 March 2003 specifies which information is visible to the naked eye as well as electronically readable:[76] name, first two forenames, first letter of the third forename, nationality, place and date of birth, sex, place of issue of the card, starting date and expiry date of the card, name and number of the card, photograph of the bearer and his identification number in the National Register.[77]

The utmost caution is therefore recommended, since the electronic identity card will in principle comprise the new electronic authentication and signature functions, fraudulent use of which is liable to cause considerable financial prejudice

[74] Article 2,1° of the Act of 17 July 2002 governing transactions carried out using electronic funds transfer instruments, *o.c.*

[75] Article 2,3° of the Act of 17 July 2002 governing transactions carried out using electronic funds transfer instruments, Article 2, *o.c*

[76] Other information may also appear on the card: certification of prolonged minority status (Article 487f, par. 4 of the Civil Code), indication of 'white stick' or 'yellow stick' for the blind or partially sighted (Royal Decrees of 25 August 1954 and 9 March 1992).

[77] As regards the identification number in the National Register, we should mention that while with the conventional identity card the citizen could choose whether or not this number should appear on the card, this option has now been withdrawn for no specific reason.

■ Information that is electronically readable only

There are various kinds of data that are electronically readable only through the use of an electronic reading device that can read the electronic chip on the card. The data concerned are first of all those that are necessary for the authentication of the card as well as for the protection of the electronic data and the use of qualified certificates.

Three other categories of data may also appear on the card in electronic form insofar as the bearer has activated them,[78] such as the electronic keys and identity and signature certificates, as well as the identity of the accredited CSP. Finally, the card will also bear various data required by law, as well as the address of the bearer's principal residence.

■ Absence of the principal residence from the data that are visible to the naked eye

Unlike with the paper identity card, the bearer's address no longer appears on the electronic identity card in a format visible to the naked eye. It will now only be available electronically. According to the parliamentary documents,[79] this decision was motivated by various arguments:

- First, the legislator wanted to leave out a data element which tends to fluctuate too much. It considered in this respect that 10 per cent of the population changes address every year, and that it therefore has become too difficult to ascertain the accuracy of the address appearing on the card.
- Furthermore, it wanted to avoid the procedure of changing the electronic identity card in case of change of address, a constraining procedure which would have necessitated a too frequent renewal of the card. The Council of Europe is in full agreement with this, since it considers that the address should not be regarded an identity element of a person. [80]
- Finally, if the card is lost or stolen, it is preferable, for security reasons, that the address should not be directly readable, so as to make the link between a card and the contents of a stolen handbag more difficult to establish (for example house or car keys). This is one of the reasons why the Federal Department of the Interior has addressed a circular[81] to the pilot municipalities, specifying the modalities whereby a citizen can prove his address in accordance with Article 3 of the Royal Decree of 25 March 2003.[82]

Although the reasons given above do indeed justify the omission of the address from the data that are legible with the naked eye, it seems nevertheless that the fact that the address is not directly readable in turn creates new legal problems that need to be resolved. Thus, in the area of banking, a series of legal rules require credit institutions to know the address of their customers in accordance with the compliance principle know your customer. This is particularly the case with the Act of 11 January 1993 on combating money laundering, which requires the banks to verify the address of their customers by means of probative documents of which they must make a copy.[83] In this connection, the Banking, Finance and Insurance Commission (BFIC) requires credit institutions, investment companies, investment consulting firms and exchange offices to identify the customer's address by making a photocopy of the identity card and the address that appears on it.[84]

How is this requirement to be satisfied if the address no longer appears on the card? The solution that is currently being considered, is to equip those financial institutions with the necessary technical infrastructure to consult the data contained on the electronic chip. It would then suffice to print out the information appearing

[78] We may ask ourselves how those elements are to be activated once the electronic identity card has been issued. In our opinion, the card would have to be renewed.
[79] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p. 25.
[80] Resolution (77) 26 of the Council of Europe on the establishment and harmonization of national identity cards, adopted on 28 September 1977. Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p. 26.
[81] Circular available in electronic format at http://www.rijksregister.fgov.be/rrn_fr/cccie/circulaire/mentionadresse/OB-VermAdres281103-FR-v121203.pdf.
[82] A document called "Proof of Address" will be issued by the municipal authority together with the card. This document may be used as proof of principal residence in pursuance of Article 3 of the Royal Decree of 25 March 2003.
[83] Article 4 of the Act of 11 January 1993 on prevention of the use of the financial system for the purposes of money laundering, *Moniteur Belge*, 9 February 1993, p.2828.
[84] Circular D1/WB 99/1, Circular D4/EB/2000/2, Circular D1/WB 99/1, and to a lesser extent Circular PPB 2003/5 of the Banking and Finance Commission to credit institutions, investment companies, investment consulting firms and exchange offices concerning the identification of customers bearing electronic identity cards.

on the computer screen in order to comply with the legal obligation to make a photocopy.

In a circular of 22 December 2003,[85] the BFIC points out that the financial institutions are obliged to make sure that they furnish themselves adequately and as soon as possible with appropriate appliances to read and record the necessary data that are stored on the microprocessor with which the new electronic identity cards are fitted. This circular stipulates that a copy must be made of the identification details that are electronically signed by the National Register and thus verify the validity of this signature. This verification takes place by ascertaining the validity of the certificate of the National Register that is introduced along with the last modification of the data on the chip. This certificate will be useful for tracing the origin of the information obtained during printing. Furthermore, the certificate of the National Register will be altered in case of an attempt to modify the information contained on the chip by any person other than an employee of the National Register who has been duly authorized to do so. In this way, a degree of certainty can be had as to the validity of those data. Finally, in order to guarantee the integrity of the recorded data, the circular provides that the identification details and their electronic signature by the National Register should be kept together so as to allow subsequent verification of the signature.[86]

In so doing, the BFIC implicitly admitted the absence of a visible address on the electronic identity card, while urging the credit institutions to furnish themselves with the necessary infrastructure.

It should also be pointed out that the anti-laundering legislation is not the only legislation requiring verification of the address of the bearer of an electronic identity card. Other law texts also provide for this, such as in the area of inheritance[87] or consumer credit[88] law, where in both cases verification of the identity of the customer is required. In the area of consumer credit, it is also provided that certain data must be recorded in the Central Consumer Credit Register, such as the domicile of the borrower or, if this is non-existent or unknown, his residence, identified by the name of the street, number of the building, the letterbox number where appropriate, the name of the town and the postcode. According to this law, the name and address of the lender must be recorded as well.[89]

This absence of the bearer's address in visible form from the electronic identity card will therefore require the banks and any other body that is legally obliged to verify this information[90] to furnish themselves with the necessary technology to electronically read the card, whether directly by means of a compatible card reader or by asking for an exception granting a limited access to the National Register.

The Act of 25 March 2003 provides in this connection that the appliances and applications that must allow consultation of the data that are electronically stored on the electronic identity card must satisfy certain technical and functional standards established by the King. The conditions of sale, rental and transmission of those appliances will also be regulated by the King.[91] Those terminals must also be compatible with the specifications established by the firm ZETES[92] and must satisfy the conditions laid down in the specifications for the manufacture, personalization, initialization and distribution of the digital identity cards and for the provision of certification services.[93] There are even plans to create a special label for the electronic identity card, with which the terminals will be provided that are designed to read them, and must satisfy certain predefined technical and security conditions.

■ Right of access and rectification of the electronically recorded data

In accordance with the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data,[94] which outlines a set of general rules governing the right of access and rectification of files containing automated data (including the National Register), the bearer of an

[85] Circular PPB 2003/5.
[86] BIENFAIT, B., "La carte d'identité électronique. La circulaire PPB 2003/5 du 22 décembre 2003 de la Commission Bancaire et Financière" in "La carte d'identité électronique dans la pratique financière", FEBELFIN Information Meeting, 10 March 2004.
[87] Article 218 of the Civil Code.
[88] Article 17 of the Act of 24 March 2003 amending the Act of 12 June 1991 on consumer credit, *Moniteur Belge*, 2 May 2003, p. 23749.
[89] Article 2 of the Royal Decree of 7 July 2002 regulating the Central Consumer Credit Register, *Moniteur Belge*, 19 July 2002, p. 32542.
[90] For example the Belgian National Bank, investment consulting firms, insurance companies.
[91] Article 18 of the Act of 25 March 2003, o.c.
[92] Specifications available in electronic format at http://www.rijksregister.fgov.be
[93] Specifications available in electronic format at http://www.rijksregister.fgov.be/bev_fr/bev_f_dispatcher.htm
[94] Act on the protection of privacy with regard to the processing of personal data, *Moniteur Belge,* 18 March 1993, p. 5801.

electronic identity card is granted directly, or via a computer that is placed at his disposal at a municipal institution, a right of access to the electronic data recorded on his card, as well as the right to rectify those data if they turn out to be incomplete, inaccurate or incorrect.[95] It is also perfectly possible for the bearer to carry out this verification at home by means of his computer and an internet connection.[96]

The bearer will even be able to know the identity of all the authorities, organizations and persons who over the past six months have consulted or updated his details in the population register or in the National Register of natural persons, with the exception of the administrative and judicial authorities charged with investigating and combating crime. The modalities of those rights of access and rectification that are granted to the bearer will be established by the King.

■ Identity Cards Register[97]

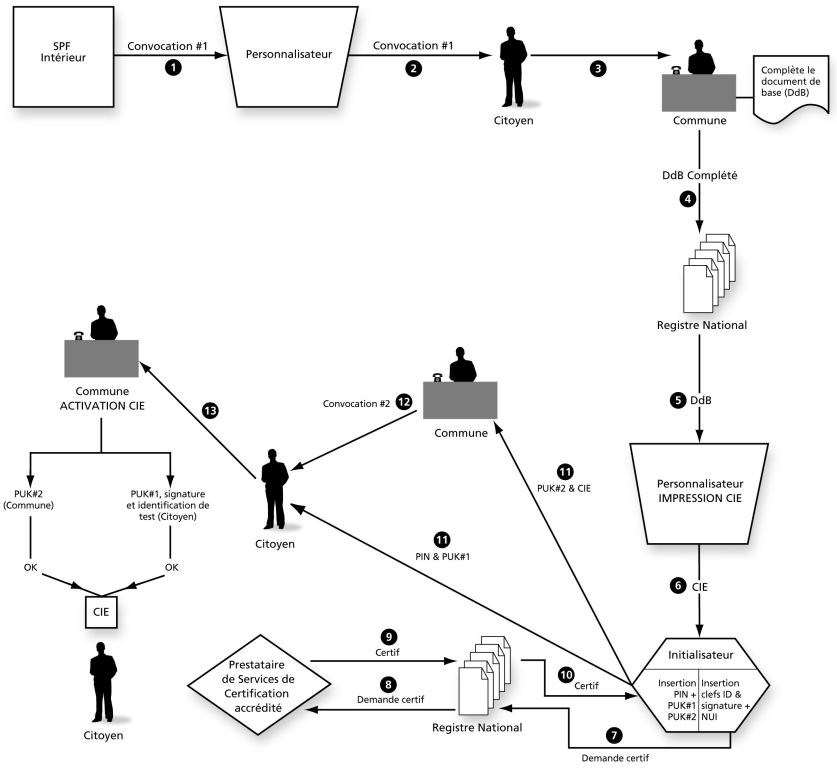
The Identity Cards Register, set up by law within the National Register of natural persons, is an essential tool to monitor the lifecycle of electronic identity cards. This register makes it possible to centralize all information about the identity cards and to follow each particular card during its production process. It contains information about the bearer of the card[98] as well as about the card itself.[99] The conditions by which a person may obtain access to this file will be established by Royal Decree.

The Identity Cards Register will be updated regularly with the necessary information which the municipal authorities, the initializer and the accredited CSP will to this end send to the Federal Department of the Interior.

Delivery procedure

■ Delivery procedure in the strict sense[100]

The delivery procedure for the electronic identity card is fairly complex and can be subdivided into various main stages, as shown in the diagram below:



[95] Article 6§3 of the Act of 25 March 2003, *o.c.*
[96] This right of access may be exercised via https://mondossier.rrn.fgov.be.
[97] Article 15 of the Act of 25 March 2003, *o.c.*
[98] For the bearer, the identification number in the National Register, the language of the electronic identity card and the serial number of the card are mentioned.
[99] For the card, the date of application, expiry and destruction of the card are specified, as well as the date of issue of the basic document, the date of delivery and the municipality charged with this delivery. Also available are the serial number of the card, information showing that the card is valid or expired, the type of identity card, where appropriate, the availability of the electronic signature function and the dates of the latest general update and the latest update of the principal residence.
[100] Article 3§4 of the Royal Decree of 25 March 2003 on identity cards, *Moniteur Belge*, 28 March 2003, p.15929.

■ First stage: physical contact between the bearer and the registrar

The Federal Department of the Interior first sends a notification (1) to each municipality through the personalizer (2). The municipal authority is instructed to transmit this notification to the citizen referred to therein. The citizen must present himself with a sum of money and a recent photograph to the registrar of his municipality in order to complete the "basic document" (3). On this document all the data needed to produce the electronic identity card are brought together.[101] When he arrives at the town hall, the citizen must first identify himself to the registrar. This identification will be corroborated by the current identity card. The registrar and the bearer then jointly sign the basic document containing all the appropriate information of the electronic identity card. This document is then sent to the Registration Centre of the National Register (4) where the data will be recorded in the Identity Cards Register and then retransmitted to the card personalizer (5).

■ Second stage: production and personalization of the plastic card

In Belgium, the role of manufacturer and initializer of the electronic identity card has been entrusted to Zetes following a procurement contract procedure. As manufacturer, Zetes attends to the production of the plastic card and the microprocessor. As personalizer, its job is to print on the card the personal details contained in the basic document (i.e. the information intended for the card bearer as well as the data on the card that are visible to the naked eye). It also places the bearer's photograph on the electronic identity card. Finally, it also takes care of the appropriate security measures in order, for example, to prevent all possible fraud. Once the card has been personalized, Zetes transfers it to the initializer (6).

■ Third stage: initialization of the card

Request for initialization

The initializer, which is again the firm Zetes, first generates a pair of basic technical keys which have but a limited usefulness during the initialization process, and subsequently stores the unique card number (identifying the card) on the card along with the identity details of the requester as required by the Act of 25 March 2003.[102] Next, it generates two pairs of keys on the card, namely the identification key, which allows the bearer to identify himself by means of a PIN code, and the signature key, which enables him to produce his digital signature by means of the PIN code.

It is for the bearer to decide whether or not he wishes to initialize' his electronic identity card (that is to say, whether or not he wishes to use his identity and signature certificates). If he does not wish to do so, the data relating to the identity and signature keys, the identity and signature certificates and the CSP held by the certification authority remain in "inactive" status and the bearer does not receive a PIN code. If on the other hand the bearer wishes to make use of the authentication or digital signature functions, the initalizer[103] will at the same time transmit, through the National Register, the requests for qualified certificates to the accredited CSP (also called certification authority), namely the firm Certipost (7) (8).[104]

Default activation of the authentication and electronic signature functions

Since the law remains fairly vague about the way in which those authentication and electronic signature functions are assigned, the government services have chosen the "opt-out" technique, according to which those functions will be automatically available and activated on the bearer's card unless the latter expressly refuses. To do so, the government services based themselves on the new Article 6§2 *in fine* of the Act, which stipulates that the card bearer may, if he so wishes, waive the activation of the identity and signature keys and certificates. This choice goes against the European practice, which prefers the opt-in technique to the opt-out technique.[105] Moreover, does it really make sense to automatically activate those functions on the electronic identity card

[101] I.e. card number, National Register number, issuing municipality, type of card, language of the card, date of delivery, expiry date, date of birth, nationality, address, name, forename, signature of the bearer, signature of the official delivering the card, photograph of the bearer.

[102] I.e. National Register number, principal residence, qualified certificates, name of the accredited certification service provider, necessary information for the authentication of the card and the protection of the electronic data.

[103] In this specific context, the initializer will play the part of registration authority, since it is to the initializer that the bearer must apply for a certificate and it is the initializer who will verify the bearer's identity. After this verification, the initializer transmits this request to the personalizer, who in turn plays the part of certification authority. The personalizer produces the certificate and links it to a pair of keys.

[104] This is currently Certipost, a joint division of Belgacom and the Post Office, while the creation *sensu stricto* of the certificates is taken care of by Ubizen.

[105] Thus, for example, on the subject of advertising on the internet, Article 14 of the Act of 11 March 2003 on certain legal aspects of information society services stipulates that the use of electronic mail for advertising purposes is prohibited without the prior, free, specific and informed consent of the addressee of the messages.

whereas certain bearers have no use for them whatsoever on account of their legal incapacity or their age? Will this not give an extra incentive to fraud? Such an opt-out technique should unquestionably be accompanied by strict and formal safeguards so that the citizen is effectively informed about this option that is offered by the law to waive the activation of those functions.

Security questions linked to the authentication and electronic signature PIN codes

The few lines that follow are concerned more with security than with legal considerations. It appears that the secret codes used to initiate the authentication and electronic signature functions can be the same. Does this not devalue the signature PIN code which up to now has been used as a concrete manifestation of a bankcard holder's undertaking to carry out an electronic funds transfer? Should we not more fully differentiate the authentication and signature functions in order to make citizens aware of the importance attached to entering the signature PIN code? Moreover, given that those two PIN codes are made up of four figures, is there not a major risk that the citizen, through negligence or through ignorance of the risks, will use the same PIN code for the two functions? There is a considerable likelihood that a citizen will eventually use the same code for his debit card, credit card, mobile phone and electronic identity card. In this respect, we would strongly recommend that the government and the FEDICT take appropriate action in order to minimize such risks, for example by prescribing that the authentication PIN code consists of four figures while the signature PIN code numbers five or more figures.

Creation of electronic certificates

The certificates generated by the accredited CSP are transmitted to the National Register (9) which, in its role as original and authentic source, verifies the information on the first certificate as well as the digital signature on the second certificate before transferring them to the initializer (10) who then stores the PIN, PUK1 (Personal Unblocked Key enabling the bearer to activate his card) and PUK2 (enabling the authorized agent to activate the card) codes on the card. These codes are to be distinguished from the signature and identification keys that are contained in electronic form on the electronic identity card. The finished electronic identity card is then sent to the municipality (11) in a secure case. The PIN and PUK1 codes are transmitted to the card bearer (11) by the initializer, while the PUK2 code is sent to the municipality by the National Register.

■ Fourth stage: activation of the card

The municipal authority[106] invites the citizen (12), insofar as the latter has received his personal codes by post, to come and collect his electronic identity card. On the spot (13) it first needs to be verified whether the first stages have been completed correctly and whether the different certificates and secret codes work properly. At that moment, the bearer will decide whether to use his electronic identity card simply as an identity document or as an authentication document containing an electronic signature. If the bearer does not use the electronic signature, he only needs to enter his PUK1 code to activate the card. If he wants to be able to use the authentication and electronic signature functions, he will activate the card jointly with the competent official by entering the PUK1 and PUK2 codes respectively. He must then produce a test signature by means of his PIN code in order to test the qualified certificate. Finally, he must perform a test identification on a website of the authority that is specially intended for that purpose by again using his PIN code. Only once these final stages have been successfully completed will the electronic identity card be effectively activated and handed over to the bearer.[107] The activation of the card will naturally be registered at the Central Identity Cards Register.[108]

The entire process of manufacture and delivery of the electronic identity card as well as of the qualified certificates of identity and electronic signature will be overseen by a sectorial committee of the National Register that has been specially set up by law.[109]

■ Centralizing role of the National Register

The National Register acts as an intermediary

[106] It should be pointed out that the Programme Act of 5 August 2003 (Programme Act of 5 August 2003, Article 37, *Moniteur Belge*, 7 August 2003, p 40498) provides that the municipal authority can delegate the delivery of the electronic identity cards to the Post Office in its capacity as a public corporation. In that case, the signature of the Post Office employee delivering the card must also appear on the card.
[107] Article 9 of the Act of 25 March 2003 and its Preamble, Parliamentary documents, Session 2002-2003, 2226/001, p. 16.
[108] This activation procedure takes about 15 minutes.
[109] Article 13 of the Act of 25 March 2003, *o.c.*

between the different organizations in this delivery procedure. It takes care of the coordination between the request to the municipality for a card by the bearer and the transfer of this request to the manufacturer, the personalizer and the initializer of the card. The National Register is informed of the different stages in the manufacturing process of the card. It also requests the authentication and electronic signature certificates from the CSP. It verifies whether the assigned set of keys is indeed unique and prepares the details for requesting a certificate for the verified set of keys. It then assigns the number of the certificate and asks an accredited CSP to deliver a certificate.

■ 3) Conditions of delivery[110]

An electronic identity card can only be issued to Belgians and to foreigners who are admitted or authorized to stay in Belgium. The references on the back of the card will vary according to the status of the card bearer. Next to the word "Belgium" there must respectively appear the words "identity card" for Belgians, "aliens residence card" for nationals of the European Union or of the European Economic Area, and "aliens identity card" in all other cases.

Under the prerogatives that have been granted to him by law,[111] the King has decided that, as is already the case with the present identity cards, the card (or the certificate of theft, loss or destruction of the card which is only valid for a renewable period of maximum one year) will be distributed by the municipal authority to every Belgian citizen from the age of 12. Carrying the card will become compulsory from the age of 15.[112]

The maximum period of validity of the card is reduced to five years (instead of 10 years as is currently the case for every citizen from the age of 22). The reason set out in the Preamble is twofold: first to avoid that the photograph on the card loses its true likeness and second to allow the security technology contained in the electronic identity card to be fairly regularly adapted in order to keep up with the incessantly accelerating development of computer fraud techniques.[113] There are several cases where the bearer must return his electronic identity card to the municipal authority for renewal: expiry of the legal period of validity, if the bearer wants a card in a language other than that in which his card was made, if the photograph is no longer a true likeness, if the card is damaged, or if the bearer changes name, forename or sex. If the bearer dies or loses his Belgian nationality, the card will naturally not be renewed.[114]

Use of the identity card and outlook for the future

Although, at the time of writing, the applications available for the use of the electronic identity card are still fairly limited, it is certain that both the public sector and the private sector will make use of this new practical opportunity to carry out more dematerialized and secure transactions with the citizens. The applications currently available include on-line consultation of the National Register over the internet site 'My file',[115] validation of electronic registered mail transmitted by Certipost, access to the secure internet site of Keytradebank, on-line filing of tax returns via Tax On Web, access to waste sorting parks, request for a license plate, and requests for parking passes.

In the future, the card may also be used to consult the progress in the processing of a planning application, take part in a poll, book seats at a cultural centre, make use of the ISABEL services, as a library card, allow lawyers to transmit their pleadings to the courts and tribunals electronically: in short, the applications are as diverse as they are boundless.

Conclusion

The introduction of the new electronic identity card demonstrates the wish, both at the national and the European level, to facilitate access and communication between citizens and government, while at the same time simplifying certain cumbersome bureaucratic procedures. The recent emergence of numerous initiatives aimed at stimulating the use of the electronic identity card seems to confirm that this objective can eventually become reality. In addition, the new "authentication" and "electronic signature" functions available on the card provide new standardized techniques allowing each individual to gain access to legal tools which as yet are not all that widespread.

The additional benefits offered by the electronic identity card will not however be limited to the administrative sector alone. On the contrary, the

[110] Article 14 of the Act of 25 March 2003, *o.c.*
[111] Article 6§7 of the Act of 25 March 2003, *o.c.*
[112] Articles 1 and 2 of the Royal Decree of 25 March 2003 on identity cards, *o.c.*
[113] Parliamentary documents, House of Representatives, Session 2002-2003, 2226/001, p. 30.
[114] Article 5 of the Royal Decree of 25 March 2003 on identity cards, *o.c.*
[115] See footnote no. 89.

card is capable of being used on a daily basis in private and business relations. Examples include cards and codes giving access to a series of functions such as e-banking or access to the internet. It may even become a suitable instrument for introducing a certain degree of uniformity in this area. However, numerous legal and technical questions are bound to come up in the meantime. We have, for example, looked into the problem of the bearer's address, which no longer appears on the card in a visible form, as well as the issue of the helpdesk and the question of liability in case of loss or theft of the card.

Other questions may arise in the future too, however, such as that of branding (will we see electronic identity cards sponsored by a financial institution?), or the involvement of third parties in the validity of the authentication and signature certificates (management of the CRL).

The Act of 25 March 2003 is a first major step towards e-government. There is no doubt, however, that there still remains a long way to go.[116] It should be noted, however, that the various parties involved in the production, management and use of the electronic identity card are in constant touch with each other in order to find a pragmatic and reliable solution for the citizen with a view to strictly minimizing the legal risks attached to the use of the electronic identity card in the future. ■

Emmanuel Roger France is a partner at Verhaegen Walravens and specializes in informatics/IT-law. He advises, drafts and litigates about e-commerce, informatics, software and licence agreements. He is a member of a number of international Informatics and IT associations and has published several scientific commitments in this field.

erogerfrance@verwal.net
http://www.verwal.net

Olivier Goffard took his law degree at the University of Liège, has a Master in company law from Ghent University and a license in company management from ICHEC Brussels Business School. He is a company lawyer at Banksys, specialising in the processing of electronic data regarding payment orders generated on specific payment terminals.

olivier.goffard@banksys.be
http://www.banksys.com

[116] For more general information on the electronic identity card, we refer the reader to the following internet sites: www.eid.belgium.be and www.esat.kuleuven.ac.be/~decockd/belpic/.