

# **LA CARTE D'IDENTITE ELECTRONIQUE**

**Un guide pour les utilisateurs et  
les développeurs d'applications**

SPF Intérieur



## Avant-propos

L'introduction de la carte d'identité électronique fait partie de la réalisation de l'e-gouvernement qui va de pair avec la simplification administrative et la modernisation des services publics fédéraux. Ces réformes ont pour but de mettre le mieux possible l'administration au service du citoyen.

La nouvelle carte d'identité remplit les fonctions qu'elle a toujours exercées, notamment l'identification du titulaire, mais elle permet aussi de le faire de manière électronique. De plus, chaque citoyen pourra générer une signature électronique valable en droit. Ainsi se crée une prestation de services plus rapide et respectueuse des clients, sans que la sécurité des données à caractère personnel ne soit compromise. En effet, le respect de la vie privée est garantie par la mise en place de toute une série de mesures de sécurité et par la création d'une commission chargée du contrôle de l'application stricte des règles donnant accès aux données à caractère personnel.

La délivrance des cartes d'identité se fera par l'intermédiaire des administrations communales avec lesquelles le citoyen est étroitement en contact. Les communes sont reliées par ordinateur à l'autorité fédérale, aux firmes agréées et aux autorités de certification qui, à des niveaux différents, prennent part au processus. Le Registre national des personnes physiques joue un rôle clé aussi bien dans la mise au point que dans le contrôle du système.

Le succès de l'utilisation de la carte électronique dépendra en grande partie des applications offertes aux citoyens, non seulement par les pouvoirs publics (consultation en ligne des données personnelles relatives à différents dossiers, accès à toutes sortes de services par un site portail), mais aussi par les instances privées. Les nouvelles applications qui seront créées constitueront une plus-value pour l'utilisateur et pour l'instance concernée. Cette brochure est dès lors destinée à tous ceux qui ont besoin d'informations générales et techniques. Les utilisateurs y apprendront comment fonctionne le système et de quel équipement ils ont besoin. Les développeurs d'applications y trouveront les informations indispensables pour utiliser la nouvelle carte de la meilleure façon possible conformément à leurs propres objectifs. Ainsi, grâce à l'utilisation de ce nouveau produit électronique, un pas important sera franchi dans l'ère digitale.





## TABLE DES MATIERES

<b>Avant-propos</b>	2
<b>Informations générales</b>	4
<b>Introduction de la carte d'identité électronique (en abrégé CIE)</b>	4
<b>A quoi ressemblera la nouvelle carte d'identité?</b>	4
• Informations visibles	4
• Informations invisibles, lisibles électroniquement	4
<b>Qui recevra une CIE?</b>	5
<b>Comment la CIE est-elle activée?</b>	5
<b>Qui sont les acteurs de ce processus?</b>	6
• Le producteur de la carte, le personnalisateur de la carte et l'initialisateur de la carte	6
• Le Registre national des personnes physiques (RN)	7
• Une autorité de certification agréée	7
<b>Quels sont les avantages et les applications de la carte d'identité électronique ?</b>	7
<b>Pourquoi la carte d'identité électronique est-elle sûre?</b>	9
<b>Matériel approprié</b>	10
<b>Explication technique</b>	10
➤ Note explicative pour les entreprises	10
• Web	10
⊙ Apache	10
⊙ Microsoft IIS – serveur web de Microsoft	10
⊙ Intégration medium and high end pour management d'accès web	10
⊙ Serveurs d'applications hauts de gamme	11
• Host access	11
⊙ Microsoft	11
⊙ Linux	11
⊙ Smartcard enabled secure web access	12
➤ Mode d'emploi pour les citoyens	12
• Netscape vs Internet explorer	12
⊙ Microsoft	12
⊙ Netscape	12
⊙ Plug-ins	12
Ⓛ Adobe Acrobat	12
<b>Doel van de EIK</b>	13
<b>Garanties relatives aux possibilités d'intégration de la carte CIE dans tout système informatique</b>	13
<b>Garanties relatives à la compatibilité logicielle avec les environnements Windows existants et futurs.</b>	14
<b>Liste des abréviations et des sigles utilisés</b>	14





## Informations générales

### Introduction de la carte d'identité électronique (en abrégé CIE)

Bientôt la carte d'identité électronique !

Si vous habitez dans une des onze communes pilotes suivantes, vous pourrez bientôt disposer d'une carte d'identité électronique et vous serez les premiers à entrer dans l'ère nouvelle de l'e-gouvernement :

11 communes pilotes	Province ou arrondissement administratif
Lasne	Brabant wallon
Marche-en-Famenne	Luxembourg
Rochefort	Namur
Seneffe	Hainaut
Seraing	Liège
Woluwe-Saint-Pierre	Arrondissement administratif Bruxelles-Capitale
Borsbeek	Anvers
Grammont	Flandre orientale
Jabbeke	Flandre occidentale
Louvain	Brabant flamand
Tongres	Limbourg

L'objectif est d'introduire progressivement la carte d'identité électronique. L'introduction dans les 11 communes sera suivie de très près et le Conseil des Ministres évaluera et adaptera le projet en temps utile.

### A quoi ressemblera la nouvelle carte d'identité?

La carte d'identité électronique aura le format d'une carte de banque et comportera une puce électronique.

#### Informations visibles

Comme la carte d'identité actuelle, la nouvelle carte reprendra des informations visibles à l'œil nu : le nom, les deux premiers prénoms, la première lettre du troisième prénom, la nationalité, le lieu et la date de naissance, le sexe, le lieu de délivrance de la carte, la date de début et de fin de validité de la carte, la dénomination et le numéro de la carte, le numéro d'identification du Registre national des personnes physiques, la photo du titulaire, la signature du titulaire et celle du fonctionnaire communal.

#### Informations invisibles, lisibles électroniquement

L'adresse du titulaire sera uniquement enregistrée de manière électronique, de sorte que la carte ne devra pas être remplacée à chaque déménagement. La carte contiendra en outre les données suivantes: les clefs d'identité et de signature, les certificats d'identité et de signature, le prestataire de service de certification accrédité, l'information nécessaire à l'authentification de la carte, à la protection des données visibles de manière



électronique figurant sur la carte et à l'utilisation des certificats qualifiés y afférents.

Le titulaire de la carte décidera lui-même s'il souhaite ou non 'initialiser' sa carte électronique (c.-à-d. s'il veut utiliser ou non ses certificats d'identité et de signature). S'il ne le souhaite pas, les données relatives aux clefs d'identité et de signature, les certificats d'identité et de signature et le prestataire de certificats auprès de l'autorité de certification sont maintenues en position « inactive » et le titulaire ne reçoit pas de code PIN.

## Qui recevra une CIE?

Dans 4 cas, le citoyen des 11 communes précitées peut obtenir une carte d'identité électronique:

1. l'ancienne carte d'un habitant d'une des communes pilotes vient à échéance. A ce moment-là, le citoyen reçoit automatiquement une convocation pour se rendre à la maison communale en vue de la demande d'une nouvelle carte d'identité digitale. Au plus tard une semaine après, il reçoit une nouvelle carte d'identité;
2. tous les jeunes âgés de douze ans reçoivent pour la date de leur anniversaire une convocation pour demander une carte d'identité électronique;
3. si l'ancienne carte d'identité est perdue ou volée ou si elle doit être remplacée parce qu'elle est abîmée, elle est remplacée par une nouvelle carte d'identité électronique;
4. en cas de demande volontaire, l'ancienne carte est remplacée par une nouvelle, électronique.

## Comment la CIE est-elle activée?

Dans les quatre cas, la carte est activée par le citoyen à la maison communale de la commune où il habite. Le citoyen décidera à ce moment-là d'utiliser sa carte comme simple preuve d'identité ou comme carte assurant non seulement son identité, mais contenant également sa signature électronique.

Qu'il utilise ou non la signature électronique, le citoyen se rendra à la maison communale muni de son formulaire de convocation et deux photos d'identité. La photo du titulaire est collée sur le formulaire de demande de la carte d'identité et le formulaire est signé tant par le futur titulaire de la carte que par le fonctionnaire de la commune.

Celui qui opte pour l'utilisation de la signature électronique devra signer un formulaire par lequel il atteste qu'il se déclare d'accord d'utiliser cette signature. Ce document est conservé à la commune. Le prix de revient de la carte sans signature électronique est le même que pour celle avec une signature électronique.

Dans un bref délai, le demandeur de la carte recevra une lettre l'invitant à aller chercher sa carte à la maison communale. Il recevra aussi une deuxième lettre contenant un code PIN et un code PUK.

Le code PIN (Private Identification Number) est le numéro d'identification privé. Le code PUK (Personal Unblocked Key) est la clé d'activation. Comme pour une carte bancaire, les codes sont protégés par une couche de protection qu'il faudra gratter pour que l'information soit lisible.

Muni des lettres reçues, le citoyen se rend à la maison communale où un fonctionnaire



introduit la carte dans un lecteur de cartes, afin de lancer le processus d'activation et de contrôler la signature digitale.

Si le titulaire de la carte n'utilise pas la signature électronique, il devra uniquement introduire son code PUK pour activer la carte. La carte est ainsi protégée et les données électroniques (telles que l'adresse et la photo digitale) peuvent être activées et lues par les services compétents.

Pour générer une signature électronique, le titulaire de la carte introduit lui-même son code PIN. Le système lui indique si tout s'est bien déroulé. Si la réponse est OK, c'est terminé. Sinon, une faute s'est présentée : un code erroné ? Le code peut être introduit jusqu'à trois reprises, après quoi, la carte est bloquée. Mais, à l'aide du code PUK, le fonctionnaire peut rétablir le processus jusqu'à six fois. Une dernière possibilité consiste à générer un nouveau code PIN en utilisant un code PUK 3. Le citoyen voit apparaître le nouveau code et en prend note.

Lors d'une faute de production, la carte est soit retirée, soit elle fonctionne comme carte d'identité sans que la signature soit activée. Une nouvelle carte est alors demandée.

Si des problèmes se manifestent au niveau du lecteur de cartes, le fonctionnaire en est averti par un signal d'erreur sur l'écran de son PC et, grâce à la formation reçue, il peut résoudre le problème. Dans le cas contraire, il peut faire appel à un helpdesk qui sera disponible 24 heures sur 24 au Ministère de l'Intérieur.

Une fois la carte activée, l'agent la remet au titulaire. A la fin de cette opération, le titulaire de la carte a toujours la possibilité, s'il le souhaite, de changer son code PIN et d'introduire un autre code personnel.

## Qui sont les acteurs de ce processus?

- [Le producteur de la carte, le personnalisateur de la carte et l'initialisateur de la carte.](#)

Le producteur de la carte appelé également CM (Card Manufacturer): s'occupe de la fabrication de la carte physique et du microprocesseur.

Le personnalisateur de la carte ou CP (Card Personalisator): imprime la carte avec les données personnelles et s'occupe des mesures de sécurité à ce sujet (éviter la fraude, ...).

L'initialisateur ou CI (Card Initialisator) s'occupe de l'aspect digital de l'opération.

Ces deux ou trois opérations peuvent être effectuées par la même firme ou par deux ou trois firmes différentes, à condition qu'elles soient agréées par une adjudication publique européenne. Ces opérations sont actuellement assurées par la firme ZETES, désignée dans le cadre d'une adjudication publique.

- [Le Registre national des personnes physiques](#) - (RN) est la plaque tournante du système. Ce service s'occupe de la coordination entre le demandeur de la CIE dans la commune et le contact avec le CM, le CP et le CI. Toutes les étapes du processus de production sont signalées au Registre.



Le Registre national demande également à l'autorité de certification les certificats d'authentification et de signature électronique. Le CI prépare les clés de sécurité. Le RN vérifie si la paire de clés attribuée est unique : la clé publique est contrôlée, la clé privée n'est pas connue. Le RN prépare les données pour demander un certificat pour la paire de clés contrôlée : le RN attribue le numéro du certificat et demande à une autorité de certification agréée de délivrer un certificat. L'agrément de l'autorité de certification satisfait aux conditions de la loi du 9 juillet 2001 du Ministère des Affaires Economiques et aux exigences européennes en la matière.

- **Une autorité de certification agréée:** attribue le certificat demandé par le RN.

Un certificat est un document électronique établissant entre autres une liaison entre les clés de sécurité et l'identité du titulaire de la carte. Il contient des informations sur le titulaire de la carte d'identité, une clé publique et l'adresse du site de l'autorité de certification. Le certificat est signé par l'autorité de certification à l'aide de sa clé privée. La carte connaît également la clé publique de l'autorité de certification. On peut ainsi vérifier si le certificat est valable et n'a pas subi de modifications.

La validité du certificat est contrôlée par une demande OCSP auprès de l'autorité de certification. Un message envoyé est protégé par l'adjonction d'une valeur hash. C'est la valeur alphanumérique (exprimée en lettres et en chiffres) du message envoyé de manière comprimée. Toute modification du document entraîne également une modification de cette valeur alphanumérique. Toute feuille hash est cryptée au moyen d'une clé privée. Cette feuille hash est déchiffrée à l'aide de la clé publique de l'expéditeur. Au moment de la réception d'un message, le système contrôlera si la valeur hash est restée identique à celle du texte original. Ainsi le destinataire aura la certitude que le document qu'il signera et approuvera n'aura pas été modifié.

## **Quels sont les avantages et les applications de la carte d'identité électronique ?**

La carte d'identité électronique permet à tout citoyen :

- d'accéder à ses dossiers auprès des autorités publiques, par exemple de consulter son propre dossier "population", de demander des documents pour lesquels on doit actuellement se déplacer et attendre parfois longtemps
- d'échanger des informations en ligne avec les autorités publiques, les sociétés privées ou les autres organisations par des messages électroniques sécurisés
- de prendre contact avec les autorités communales: de nombreuses communes disposent dès à présent d'un site web sur lequel on peut trouver toutes les informations utiles concernant les services qu'elles proposent: bibliothèque, sport, population, transports en commun, etc. Certaines communes sont d'ailleurs déjà équipées de guichets électroniques où une demande peut être introduite au moyen de formulaires électroniques. C'est par exemple le cas à Senefte et à Gand. Consultez <http://www.senefte.be> ou <http://www.gent.be>. Grâce à l'authentification au moyen de la carte d'identité électronique et de la signature électronique, les contacts avec l'administration communale seront à l'avenir encore plus faciles et plus efficaces

<sup>1</sup> On line certificate status protocol.



- de prendre contact avec les régions et l'autorité fédérale: les régions et l'autorité fédérale mettent également leur administration à la disposition du citoyen via Internet. FEDICT a pour mission d'élaborer une stratégie qui permettra à l'autorité fédérale belge d'être l'un des pionniers dans le domaine de l'e-gouvernement. Le website de Fedict à l'adresse <http://www.fedict.be> ou le portail fédéral à l'adresse <http://www.belgium.be/> vous permettra d'entrer en contact avec tous les autres départements. Le portail de la Région wallonne est disponible à l'adresse <http://www.wallonie.be/>; celui de la Région flamande à l'adresse <http://www.vlaanderen.be/>; celui de la Région de Bruxelles-Capitale à l'adresse <http://www.bruxelles.irisnet.be/>; celui de la Communauté germanophone à l'adresse <http://www.dglive.be/>; et celui de la Communauté française à l'adresse <http://www.cfwb.be/>.
- de réaliser de transactions commerciales sur Internet d'une manière sûre, tant pour l'acheteur que pour le vendeur (achat et vente en ligne)
- d'apposer sur des documents une signature électronique à laquelle est reconnue la même valeur juridique qu'à la signature manuscrite. Envoyer des messages signés valablement et même conclure des contrats avec des concitoyens, etc.
- de participer à toutes les applications qui seront mises à disposition à l'avenir, tant par le secteur public que par le secteur privé: réservation, inscription, commande, paiement, résiliation, etc. Toutes ces opérations seront possibles en toute sécurité. Autres applications éventuelles: badge d'entreprise, carte de paiement électronique, déclaration de TVA en ligne, etc.
- d'accéder, en tant que travailleur, au réseau de l'entreprise et éventuellement de réaliser un travail à domicile par le télétravail

Les entreprises déjà présentes sur le réseau auront la possibilité de passer d'une utilisation purement informative à des applications permettant des transactions. Des cartes test pourront être obtenues au Ministère de l'Intérieur, Registre national, Direction des Elections et de la Population, Boulevard Pacheco, 19 boîte 20 – 1010 Bruxelles. Tél. 02/200.21.21. Fax: 02/210.21.86 – 02/210.21.49 auprès de Mme I. BENS, tél. 02/210.21.85, e-mail: [info@rrn.fgov.be](mailto:info@rrn.fgov.be)

La carte pourra être testée sur le site du Registre national à l'adresse suivante: <http://www.rijksregister.fgov.be>

Grâce à l'authentification et à la signature CIE, les serveurs web seront beaucoup plus accessibles que ce n'était le cas jusqu'à présent ...

Les banques pourront également profiter de l'interopérabilité rendue possible par la CIE ...

Dans les universités, la CIE pourra également être utilisée comme carte d'étudiant.

## **Pourquoi la carte d'identité électronique est-elle sûre?**

Parce que les fonctionnalités d'identification et de signature électronique sont protégées par deux paires de clés : la clé d'identification et la clé de signature.

Grâce à la clé d'identification, le titulaire d'une carte fait connaître son identité, il fait savoir qui il est en introduisant son code PIN, comme lorsqu'on utilise un GSM.

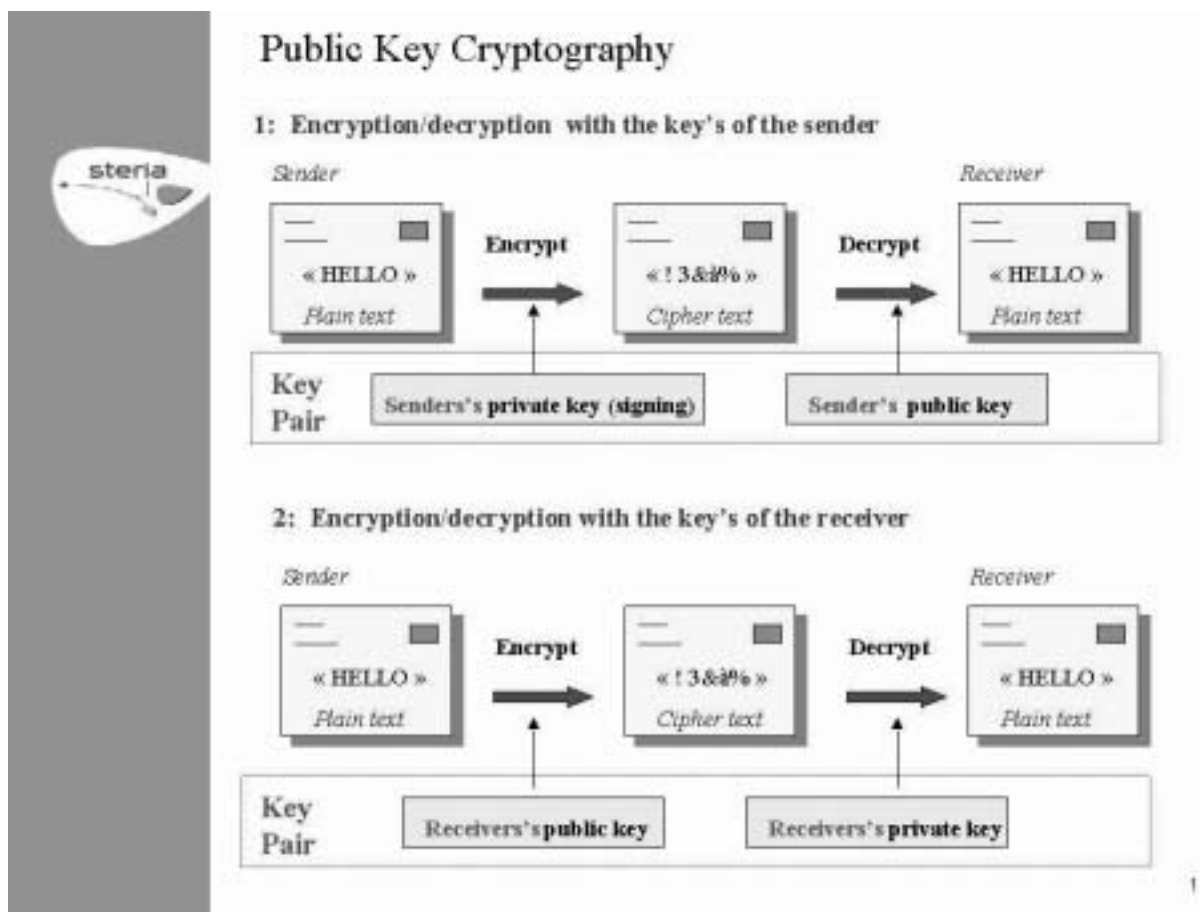


Grâce à la clé de signature, le titulaire d'une carte pourra apposer une signature électronique sur des formulaires au moyen de son code PIN. Cette signature aura la même valeur qu'une signature manuscrite.

Pourquoi ces clés sont-elles sûres? Parce qu'elles sont une combinaison de deux clés: une clé privée et une clé publique. La clé privée est secrète. Chaque clé est composée de 128 lettres et chiffres. Grâce à ces clés, le titulaire d'une carte dispose donc d'une signature unique.

L'utilisation des clés privées, des codes et des mots de passe permet de protéger la vie privée du titulaire de la carte. De plus, une protection spécifique garantit l'identité réelle de l'expéditeur et du destinataire. Aucun des deux ne pourra prétendre que le message n'a pas été envoyé ou reçu.

Pour une meilleure compréhension du système, voici les schémas rédigés par la firme Steria, chargée, dans le cadre d'une adjudication publique, de l'adaptation de l'infrastructure informatique du Registre national et des communes pilotes.



## Matériel approprié

Pour utiliser une signature électronique, on a besoin d'un lecteur de cartes connecté à un PC ordinaire. Les lecteurs de cartes compatibles avec la CIE sont mentionnés sur le site Internet <http://www.registrenational.fgov.be>.



## Explication technique

### Sous réserve d'un test avec la véritable CIE

La présente notice technique décrit un certain nombre d'adaptations à réaliser en vue de la reconnaissance de la CIE dans le cadre d'activités commerciales – e-commerce – et de la transformation d'applications existantes en une plate-forme sécurisée (secure platform) au moyen de la CIE.

De nombreux logiciels gratuits (freeware) et produits commerciaux sont actuellement développés en vue de l'utilisation d'une carte à puce.

Quelques produits existants seront cités à titre d'exemples.

#### ➤ Note explicative pour les entreprises

- Web

- ⊙ Apache

Actuellement 65% des logiciels de navigation (webbrowsers) disposent d'une version apache.

Il existe des modules plug-in destinés à augmenter la sécurité, appelés parfois des Pam –plugable authentication modules. Un de ces modules est le mod\_ssl, permettant d'utiliser le SSLv2 et le v3 tout comme le TLS. On peut ainsi protéger son site au moyen de https. Mod ssl utilise les bibliothèques logicielles de openssl.

Il existe également des plug-ins supplémentaires en version beta utilisant mod\_ssl plug-in. Ce projet est basé sur un plug-in fonctionnant avec une carte à puce pouvant être lue par un lecteur de cartes à puce. Ainsi se crée la possibilité d'effectuer une authentification renforcée (strong authentication) au moyen d'un certificat par l'intermédiaire d'un serveur web apache "étendu". Ce projet s'appelle smart card netlogin. Il existe un autre projet remplissant les mêmes fonctionnalités: le scas.

- ⊙ Microsoft IIS –serveur web de Microsoft

Le projet permettant au logiciel de navigation (webbrowser) de Microsoft de supporter les cartes à puce s'appelle Fortezza.

Uniquement applicable à IIS 5.0 ou plus.

Le PC client doit être compatible (compliant) avec Fortezza.



### ⊙ *Intégration medium and high end pour management d'accès web*

Momentanément, il existe des progiciels qui combinent l'authentification avec une gestion décentralisée du serveur (distributed server management), tout en protégeant les serveurs web.

Un tel progiciel peut fonctionner avec des combinaisons d'authentification et donner accès en fonction de l'autorisation de l'utilisateur. Ainsi, on peut par exemple obtenir un accès sur la base d'un certificat, vérifier si le certificat n'a pas été révoqué (revoked) et demander encore une authentification supplémentaire comme login /mot de passe, ...

De tels logiciels offrent beaucoup de possibilités, mais les progiciels standards doivent encore être développés afin de les adapter aux exigences des différentes applications ou entreprises. Ces produits supposent en général une connaissance approfondie et sont souvent relativement chers. La gestion centrale offre toutefois un excellent aperçu fonctionnel de l'ensemble du processus.

Certains progiciels comprennent des contrôles d'accès basés sur la fonction (role-based access control) (l'accès étant réservé à des individus sur la base de leur fonction), une personnalisation de l'environnement de l'utilisateur, un auto-enregistrement de l'utilisateur (user self-registration) et des liaisons avec d'autres produits de protection tels que firewalls, détections d'intrusion (intrusion detections),... combinés à des banques de données des utilisateurs (ldap, nt, racf, ...). Ces solutions plus onéreuses sont généralement accompagnées d'instruments de contrôle (auditing tools) pour la gestion de l'ensemble.

### ⊙ *Serveurs d'applications haut de gamme*

Les serveurs d'applications offrent la possibilité de créer un accès granulaire, souvent accompagné d'une bibliothèque et d'outils propres.

Un grand nombre de ces applications présentent l'avantage de permettre le développement "out of the box" d'applications directes. Beaucoup de produits présentent des problèmes de contrôle d'accès (access control) entre différents domaines: une fois connecté, on sera généralement obligé de s'identifier une nouvelle fois en passant à un autre serveur web.

Pour remédier à ce problème, des entreprises dirigeantes ont accepté le standard SAML afin d'assurer l'interopérabilité entre divers produits.

#### • Host access

### ⊙ *Microsoft*

Windows 2000 et Windows XP supportent l'utilisation d'une carte à puce pour entrer dans le système.

### ⊙ *Linux*

Dans Linux, on développe actuellement des plug-ins supportant une carte à puce pour un login permettant une authentification renforcée (strong authentication). Ces plug-ins continuent à se développer. Vous pouvez trouver de plus amples informations sur les projets de carte à puce actuels dans le projet MUSCLE. Vous trouverez des informations sur les projets Linux dans le site [www.linuxnet.com](http://www.linuxnet.com). Moyennant quelques légères adaptations, certains projets pourraient supporter la CIE.



### ⊙ Smartcard enabled secure web access.

Cela permet de signer un document avant de l'envoyer. Lors de la phase de démarrage, on ouvre une session SSL avec le serveur web. Dès que la ligne de chiffrement est établie, la page web à envoyer est hachée. Ensuite, ce hachage est signé ou chiffré via la clé privée sur la carte à puce. La page originale est renvoyée au serveur web où elle est vérifiée au moyen du hachage. Si la valeur hash est restée identique, la page n'a pas été modifiée pendant l'expédition.

### ➤ Mode d'emploi pour les citoyens

- Netscape vs Internet explorer

Netscape emploie par exemple pkcs-11, une bibliothèque de fonctions.

Microsoft emploie pc/sc et les crypto api correspondants, intégrés dans Internet Explorer et dans d'autres produits de Windows.

- Mail

### ⊙ Microsoft.

En installant MS office 2000 ou d'autres systèmes d'exploitation récents, on dispose d'un progiciel de messagerie (mail) permettant de supporter l'utilisation de certificats. A l'aide de ces logiciels, on peut donc travailler avec "smime", en d'autres termes, on peut envoyer en toute sécurité un courriel et le signer de manière électronique.

### ⊙ Netscape

Netscape dispose d'un plug-in permettant de supporter une carte à puce au moyen de netscape mail.

### ⊙ Plug-ins

#### ⌚ Adobe Acrobat

Adobe requiert un plug-in complémentaire pour protéger électroniquement des documents au moyen d'une signature digitale.

## Garanties relatives aux possibilités d'intégration de la carte CIE dans tout système informatique

La carte CIE répond aux normes suivantes :

01. ISO 7810 spécifiant les dimensions physiques de la carte ; en l'occurrence le format ID1.
02. ISO 7816-1 spécifiant les différences de niveau entre les contacts et la carte.
03. ISO 7816-2 spécifiant la localisation des contacts.
04. ISO 7816-3 spécifiant les signaux électroniques et protocoles de transmission.
05. ISO 7816-4 spécifiant les commandes intersectorielles pour les échanges.
06. ISO 7816-5 spécifiant les systèmes de numérotation et la procédure d'enregistrement d'identificateurs d'applications.
07. ISO 7816-8 spécifiant les commandes intersectorielles de sécurité.
08. ISO 7816-9 spécifiant les commandes intersectorielles additionnelles et attributs de sécurité.

<sup>2</sup> S/MIME: Secure/Multipurpose Internet Mail Extensions: een methode om veilige internet boodschappen te zenden en te ontvangen.



## Garanties relatives à la qualité technique de la carte CIE

La carte CIE répond aux normes suivantes :

- 01. MILSTD-883c réglementant l'électricité statique.
- 02. ISO 7811-1 spécifiant l'estampage.
- 03. ISO 7811-3 spécifiant la position des caractères estampés sur les cartes ID1.
- 04. ISO 10373 réglementant la torsion dynamique du support, le taux d'acceptation de vibrations, la résistance aux produits chimiques.
- CECC 90 000 Salt Atmosphere and chip assembly humidity.

## Garanties relatives à la compatibilité logicielle avec les environnements Windows existants et futurs

La compatibilité avec la norme 'CRYPTO API' de Microsoft ainsi qu'avec la norme PKCS11 de RSA Labs sera assurée.

L'architecture du fichier est conforme à la norme PKCS15 version 1.1 de RSA Labs.

Les certificats d'authentification et de signature électronique posséderont un profil conforme à la norme RFC 3039 (Qualified Certificate Profiles), elle-même basée sur la norme RFC2459 décrivant la structure et la sémantique des certificats X509 Version 3.

Dans le cadre de la fonction de 'signature électronique', les standards suivants seront également pris en compte, à savoir :

1. RFC 3161 Internet X509 Public Key Infrastructure, Time-Stamp Protocol (protocole d'horodatage sécurisé).
2. RFC 2044 UTF-8, a transformation format of Unicode and ISO 10646 (concerne l'information stockée dans la puce électronique de la carte CIE).
3. RFC 2527 Internet X509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework.
4. RFC 2560 Internet X509 Public Key Infrastructure, Online Certificate Status Protocol – OCSP.
5. Directive ETSI TS 101 456 : Policy Requirements for Certification Authorities Issuing Qualified Certificates.



## Liste des abréviations et des sigles utilisés

API	Application Programming Interface	Jeu de fonctions pour l'emploi d'une bibliothèque de programmes.
CA	Certificate Authority	Autorité de certification: instance qui émet le certificat.
CI	Card Initialisator	Initialisateur de la carte: prépare la carte sur le plan digital.
CIE		Carte d'identité électronique.
CM	Card Manufacturer	Producteur de la carte: s'occupe de la production de l'aspect matériel de la carte et du microprocesseur.
CP	Card Personalisator	Personnalisateur de la carte: imprime les données personnelles sur la carte et la protège contre les falsifications.
ETSI	European Telecommunications Standards Institute	Institut européen établissant des directives pour la standardisation de la télécom munication.
FEDICT		Service public fédéral Technologie de l'Information et de la Communication.
HTTP	Hypertext tranfer protocol	Protocole pour l'échange de documents hypertextes sur le World Wide Web.
ID	Indentity Card	Carte d'identité.
IETF	Internet Engineering Task Force	Un groupe Internet informel pour la standardisation.
ISO	International Standards Organisation	Normes internationales définies pour promouvoir la gestion de qualité.
LDAP	Lightweight Directory Access Protocol	Protocole utilisé pour donner accès aux "directory servers" (un directory est une sorte de banque de données où l'information est conservée en arborescence).
MUSCLE	Movement for the Use of Smart Cards in a Linux Environment	Un projet pour coordonner le développement de cartes à puce et d'applications Linux.
NT	New Technology	Programme d'exploitation de Windows.
OCSP	On line certificate status protocole	Protocole permettant de vérifier rapidement (en temps réel) la révocation d'un certificat.
PAM	Pluggable Authentication Modules	Une architecture flexible, ouverte pour l'authentification des utilisateurs sur des systèmes Linux.
PIN	Personal Identification Number	Le numéro d'identification privé de la carte à puce.
PKCS	Public Key Cryptography Standards	Une série de spécifications émanant de la protection des données de RSA.
PUK	Personal Unblocking Key	La clé d'activation de la carte à puce.
RACF	Resource Access Control Facility	Système de gestion relatif à la sécurité utilisé par IBM.
RFC	Request For Comments	Une série de spécifications émises par l'IETF.
RN		Registre national des personnes physiques.
RSA	Rivest, Shamir, Adleman	Système cryptographique asymétrique inventé par Rivest, Shamir et Adleman.



S/MIME	Secure/ Multipurpose Internet Mail Extensions	Une méthode permettant d'envoyer et de recevoir des messages internet en toute sécurité.
SAML	Security Assertion Markup Language	Un système basé sur XML pour l'échange sûr d'informations.
SSL	Secure Socket Layer	Un protocole de sécurité permettant l'authentification et la cryptographie sur l'internet.
TLS	Transport Layer Security	Une version de SSL
TS	Technical Specification	Spécification technique de l'ETSI
UCS	Universal Charter Set	Norme définissant un jeu de signes pour XML
UTF-8		Jeu de signes pour XML, selon la norme UCS
X.509	The Directory Authentication Framework	Une description détaillée de certificats digitaux ainsi que de leur emploi.
XML	eXtensible Markup Language	Une norme internet pour la construction flexible et logique de fichiers documents; le recours à XML rend les informations des fichiers accessibles d'une manière relativement aisée.



