



SECRETARIAT GENERAL
DIRECTION de PROGRAMME
INES

Le programme INES

(identité nationale électronique sécurisée)

Le programme INES – identité nationale électronique sécurisée – est un projet global qui consistera à :

- Fusionner, simplifier et sécuriser les procédures de demande de passeport et de carte nationale d'identité (CNI) ;
- Améliorer la gestion de ces titres dans de nouvelles applications ;
- Délivrer des titres hautement sécurisés conformes aux exigences internationales ;
- Offrir aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique.

Pourquoi INES ?

Plusieurs raisons se conjuguent pour justifier le programme INES.

1. Les procédures actuelles de délivrance des CNI et des passeports ne sont pas suffisamment sécurisées. Des vols de titres vierges ont lieu chaque année. Des titres authentiques sont par ailleurs délivrés indûment sur la foi de faux certificats d'état civil ou à partir de vrais certificats usurpés. Cette fraude à l'identité sert à réaliser de multiples infractions : immigration illégale, fraude aux allocations ou aux droits sanitaires et sociaux, escroqueries, grand banditisme... dont le coût pour la collectivité, secteurs public et privé confondus¹, se chiffre en centaines de millions d'euros par an².
2. Afin de lutter contre le terrorisme, de nombreux pays, sous l'impulsion de l'Organisation de l'Aviation Civile Internationale et de l'Union européenne, introduisent des photographies et des empreintes digitales numérisées sur des puces insérées dans leurs cartes d'identité, leurs passeports et leurs visas. Par exemple le règlement européen du 13 décembre 2004 impose d'insérer dans une puce la photographie du titulaire d'ici à juin 2006, et ses empreintes dans un second temps.
3. Actuellement, le citoyen qui demande un passeport et une CNI doit en pratique remplir deux demandes distinctes, avec des justificatifs différents. En cas de changement ou de renouvellement d'un titre, il doit reconstituer tout son dossier. La nouvelle application INES vise à lui simplifier la vie : une seule procédure pour les deux titres, effectuée une fois pour toutes, et une accélération des renouvellements.
4. Le développement de l'administration électronique et la multiplication des données personnelles en ligne rendent patent le besoin de disposer d'outils permettant de garantir son identité sur Internet et de signer électroniquement ses transactions. Afin d'éviter que chaque administration mette en place ses propres modes de signature, ou achète au prix fort des certificats aux entreprises privées spécialisées, il est prévu de doter la carte INES de ces fonctionnalités qui seront valables pour toutes les administrations et tous les services financiers ou commerciaux sur Internet.

¹ Le secteur public est concerné par les fraudes aux droits et allocations, fraude aux impôts, amendes et cotisations impayées, etc, dont il répercute le coût sur les prélèvements obligatoires. Le secteur privé est victime des escroqueries, commandes impayées, etc, dont il répercute le coût sur les prix. Dans les deux cas, c'est le citoyen, à la fois contribuable et consommateur, qui se retrouve victime de cette fraude.

² Il n'existe pas d'étude sur le montant de la fraude en France. A titre de comparaison, le gouvernement britannique évalue le coût de la fraude à l'identité à 1,3 milliard de livres par an, plus 390 millions de livres de blanchiment. Aux Etats-Unis, la Federal Trade Commission a recensé 437 millions de dollars de fraudes commerciales liées à de fausses identités en 2003, et le Gartner Group évalue à 1,2 milliards de dollars le coût annuel pour les établissements financiers de la fraude sur internet par la technique de phishing.

Le contenu d'INES

1) la demande de titre

La procédure actuelle, avec production par le demandeur d'un certificat de naissance, sera remplacée par une procédure mettant directement en contact la mairie ou la sous-préfecture (service de dépôt de la demande) et la mairie de naissance. Lorsque le fichier central d'état civil sera opérationnel, le service de dépôt s'y raccordera et procédera directement aux consultations nécessaires: le demandeur n'aura plus de formalités préalables à remplir.

La gestion des titres étant centralisée, le demandeur pourra, à terme, demander sa carte d'identité ou son passeport, et les faire renouveler, dans n'importe quel point du territoire national, et non plus seulement à son lieu de résidence.

Le service de dépôt enregistrera numériquement la photo et les empreintes du demandeur³.

2) la gestion des titres

Un nouveau fichier remplacera les fichiers nationaux existants de cartes d'identité et de passeports. Ce fichier ne comportera pas les photos et les empreintes numérisées, qui seront stockées sous forme anonyme dans des fichiers séparés.

Seuls auront accès à ces fichiers de photos et d'empreintes, dans le cadre strict de leurs missions, les agents habilités à établir les titres, et les services publics de sécurité spécialement habilités pour des missions précises et encadrées par la loi (contrôles d'identité, enquêtes judiciaires).

3) les nouveaux titres

Le passeport INES comportera une puce sans contact insérée dans le livret. Il sera donc visuellement identique au passeport actuel. Ses fonctionnalités électroniques se limiteront à la présence d'une photo et des empreintes dans la puce, conformément au règlement européen. Ces données ne seront consultables que par les agents habilités pour le contrôle.

La carte d'identité électronique est décrite de manière détaillée ci-après.

³ Outre la facilitation des contrôles, la prise des empreintes a également pour but d'empêcher une même personne de demander des titres sous plusieurs identités, ou à plusieurs personnes d'user de la même identité.

La carte nationale d'identité électronique (CNIE)

La nouvelle carte aura le format d'une carte bancaire.

Les informations écrites sur la carte seront, comme actuellement, le nom, le prénom, la date et le lieu de naissance, le sexe, l'adresse, la signature manuscrite, la préfecture qui a délivré la carte, et le numéro de la carte.

Les informations contenues dans la puce seront divisées en blocs distincts et étanches (par le moyen de la cryptographie):

- Le bloc "identité" sera confidentiel (cryptographie de haut niveau) et accessible aux seules autorités habilitées (traçabilité des interrogations, habilitations nominatives des agents,...). Il reprendra les informations imprimées sur la carte, en particulier la photo numérisée et deux empreintes digitales numérisées.
- Le bloc "authentification de la carte" constituera le mécanisme permettant de prouver automatiquement l'authenticité de la carte (pour éviter les fausses cartes). Ce mécanisme sera bien entendu anonyme, afin de ne pas divulguer de donnée personnelle. Schématiquement, quand on demande à la puce si elle est authentique, elle répond « oui » (et, évidemment, le prouve), et c'est tout. Cette fonctionnalité est envisagée pour faciliter l'utilisation de la carte dans la vie courante (commerce, poste, etc). De nombreux usages peuvent aussi être imaginés par nos concitoyens.
- Le bloc "identification authentifiée du porteur " ou « identification certifiée » (par un code secret PIN) permettra d'accéder à des télé procédures publiques ou privées (par exemple accès à son compte en banque...).
- Le bloc " signature électronique" (voir le glossaire) permettra (par un code PIN secret) de signer électroniquement des documents authentiques, soit à l'intention d'une e-administration, soit pour toute transaction électronique privée.
- Le bloc "portfolio personnel": il est en outre envisagé de permettre aux titulaires, s'ils le souhaitent, de stocker, à titre personnel, des informations complémentaires dans la carte, soit pour faciliter leurs transactions électroniques (par exemple : stocker de manière « exportable » nom, prénom, adresse, pour remplir des formulaires), soit pour remplacer d'autres papiers (ex : numéro de permis de conduire, numéro fiscal, etc). L'imagination de nos concitoyens est là aussi sollicitée, dans le respect bien entendu de la protection due à chacun de ses données personnelles

Il sera remis au titulaire d'un passeport ou d'une carte d'identité numériques, un document papier indiquant toutes les informations contenues dans la puce. Bien entendu, chacun disposera du droit de rectification de ces informations.

La carte sera sans doute dans un premier temps bimode : la consultation des données d'identité (photo et empreintes) par les autorités habilitées se fera sans contact ; l'authentification automatique de la carte et la mise en œuvre des fonctions électroniques offertes au porteur se feront avec contact (et avec un code secret), grâce à un lecteur de cartes

externe (coût 5 à 10 €) en attendant que les ordinateurs privés soient équipés en série de lecteurs de cartes.

Depuis que la carte est gratuite, le nombre de « pertes » et de « vols » a été multiplié par dix, ce qui implique autant de renouvellements injustifiés aux frais du contribuable. La question de la fin de la gratuité est posée à chacun d'entre nous: elle permettrait de responsabiliser le porteur de la carte. En outre, elle correspondrait au prix d'un nouveau service bien réel, celui d'accéder aux fonctionnalités sécurisées d'administration et de commerce électronique.

Un centre d'appel sera mis en place pour recevoir 24h/24 les demandes d'opposition d'une carte suite à une perte ou à un vol.

Lors d'un usage de la carte sur internet, les interlocuteurs pourront vérifier, sur une liste tenue par le ministère de l'intérieur, que la carte n'est pas en opposition.

Le projet actuel ne prévoit pas de rendre la carte obligatoire. Mais là aussi toutes les opinions seront les bienvenues.

Les garanties

L'informatique fait peur, la création de fichiers électroniques inquiète, la numérisation des empreintes digitales et des photographies est redoutée. Chacun d'entre nous craint la mise en fiche par le Big Brother inventé par l'écrivain George Orwell. Toutes ces craintes seraient légitimes si un projet tel qu'INES n'était pas assorti d'un ensemble développé de garanties juridiques et technologiques contre toutes les utilisations (de source publique ou privée) et contre toutes les intrusions illégales dans la connaissance de nos données personnelles d'identité.

C'est pourquoi le programme INES comprendra un volet "garanties et sécurités" sur plusieurs plans :

- sécurité logique des composants du système (stations d'acquisition, serveurs, fichiers) et des connexions ; il s'agit d'éviter l'accès au système, que ce soit en production ou en consultation, par des personnes non habilitées ;
- sécurité physique des installations, indispensable pour éviter une tentative d'intrusion sur le système ;
- sécurité des titres : résistance du contenu aux attaques physiques et logiques pour éviter l'altération d'un titre authentique, et résistance du support à la falsification pour éviter la fabrication de faux ;
- sécurité des procédures : il s'agit de garantir, par des procédures exigeantes et par une répression pénale renforcée, un niveau de confiance le plus élevé possible dans les informations certifiées par les titres INES,.

C'est à la condition expresse que ces aspects soient parfaitement pris en compte que les enjeux suivants seront atteints :

- renforcement de la confiance dans les titres et mise aux normes européennes et internationales ;
- maintien de la confiance du citoyen envers l'Etat concernant l'informatisation des procédures et la centralisation des informations ;
- réussite de la modernisation des relations entre le citoyen et l'administration par la mise à disposition d'un outil électronique : la carte nationale d'identité électronique.

Le programme INES veut apporter la garantie au citoyen que les données à caractère personnel réunies dans les fichiers du système INES et dans les puces des titres seront exclusivement utilisées afin de produire les titres en augmentant le niveau de confiance dans l'identité, d'assurer la libre circulation des citoyens en leur permettant de justifier simplement de leur identité, et ne sont consultées que dans les cas expressément prévus dans la loi.

Aussi, chaque accès aux fichiers INES nécessitera une habilitation et sera "tracé" (repérage automatique de l'agent habilité qui aura consulté le dossier, date et heure de cette consultation, liste des données consultées). En cas d'abus, ce traçage fera foi comme preuve devant la justice pénale.

Glossaire technique des fonctionnalités électroniques

Authentification d'un titre : cela consiste à prouver l'authenticité du titre , c'est à dire qu'il a bien été émis par le ministère de l'Intérieur.

Pour le passeport, cette preuve est apportée aux autorités de contrôle par le déchiffrement des données personnelles de la puce (conformément aux normes UE).

Pour la carte d'identité, idem. De plus, pour permettre à d'autres intervenants que les autorités de contrôle de bénéficier de la même garantie d'authenticité sans dévoiler de données personnelles, il est prévu un mécanisme d' « authentification active » de la carte. Il consiste en un dispositif permettant à la carte de répondre en substance « je suis valide » (et, évidemment, de le prouver) lorsqu'elle est interrogée par un opérateur du type autre administration, guichet de la poste ... A contrario, une carte ne prouvant pas qu'elle est valide est soit défectueuse (puce cassée) soit fausse.

Identification : action de donner certains éléments constitutifs de son identité, par l'intermédiaire par exemple de sa carte d'identité, de son contenu électronique,

"identification authentifiée " du titulaire de la carte ou « identification certifiée » : action de prouver électroniquement son identité. L'identification authentifiée du titulaire recouvre deux étapes :

- l'identification du titulaire (cf supra)
- la preuve de l'identification ou « authentification » (elle est basée sur la frappe du code PIN du titulaire et un échange cryptographique),
 - Le titulaire d'une CNIE pourra utiliser cette fonction d' « identification authentifiée » afin d'accéder à des sites d'administration électronique gérant des données personnelles (fiscales, médicales, etc).

Signature électronique : action de signer des données, avec une validité équivalente à celle de la signature manuscrite (art 1316-4 du code civil). La signature électronique non seulement engage valablement le signataire, mais également garantit l'origine des données et leur intégrité: il convient de ce fait de bien distinguer ces deux fonctions là aussi recouvertes par la même expression "signature électronique".

- Le titulaire d'une CNIE pourra ainsi "signer" des documents d'administration électronique (déclaration de revenus, etc).

Intégrité des données: garantie que les données figurant sur un document électronique, une puce, une base de données, ... n'ont pas été corrompues ou modifiées frauduleusement ou par accident.

Certificats électroniques: L'identification authentifiée du porteur ou titulaire de la carte et la signature électronique sont réalisées par le recours à des **certificats** électroniques émis par l'Etat, garantissant l'identité du titulaire de la carte, et permettant à l'interlocuteur (commerce ou administration par exemple) de s'assurer électroniquement qu'il a affaire au bon usager, et que celui-ci est pleinement d'accord avec la transaction en cours.

Dans les autres pays

Pour les mêmes raisons que le gouvernement français, de nombreux autres pays dans le monde utilisent déjà ou étudient une carte d'identité électronique. Voici un échantillon en Europe :

Allemagne : carte traditionnelle actuellement obligatoire et facturée 8€. Projet de carte électronique avec photo et empreinte numérisées, fonctionnalités d'authentification et de signature électroniques.

Belgique : carte d'identité électronique en cours de distribution à la population. Elle est obligatoire à partir de 12 ans et payante (10€ environ). Elle ne comporte pas pour le moment d'éléments tels qu'empreintes ou iris de l'œil. Fonctionnalités d'authentification et de signature électroniques. Sites d'information : www.registrenational.fgov.be, www.eid-shop.be, www.belgium.be/eportal

Estonie : près de 700.000 cartes électroniques distribuées (sur une population de 1.4 million de personnes) avec authentification et signature électroniques. Carte payante (10€ environ), sert de ticket dans les transports, de carte de sécurité sociale et d'accès aux dossiers médicaux. Extensions prévues : inclusion du permis de conduire, de l'assurance automobile, du vote électronique. Site d'information : www.id.ee

Finlande : 45.000 cartes électroniques distribuées en 2004. Carte payante (40€ ; + prix du lecteur 21€), avec authentification et signature électroniques, et données d'assurance et de sécurité sociale. Site d'information : www.fineid.fi

Italie : 600.000 cartes électroniques distribuées mi-2004. L'enregistrement des empreintes est facultatif. Carte avec authentification électronique, groupe sanguin, numéro fiscal. Usages : identification au bureau de vote, paiement des impôts, taxes et amendes par internet, inscription aux services municipaux, rendez-vous hospitaliers, demandes d'aide sociale, notification de changement de domicile... Site d'information : www.cartaidentita.it

Royaume-Uni : pays traditionnellement opposé au concept de carte d'identité. La loi du 20 décembre 2004 instaure une carte d'identité électronique qui sera à terme obligatoire et devra être présentée pour accéder aux services publics (santé, chômage, éducation). Elle comprendra une photo numérisée, les empreintes digitales et l'iris de l'œil. Elle serait payante (35£ soit environ 50€ au tarif plein, tarifs réduits pour les jeunes, les personnes âgées, les personnes à faible revenu).

Foire aux Questions

Les indications ci-dessous correspondent à l'état du projet au 28 février.

➤ **La carte INES servira-t-elle de carte de paiement ?**

Réponse : non.

La carte INES pourra servir dans du commerce en ligne, par exemple pour s'authentifier si on est un client régulier ou si on souhaite initier une transaction. Mais elle ne servira pas à payer. La CNIe offrira donc la même garantie que la présentation, aujourd'hui, de l'actuelle carte d'identité, par exemple, à l'occasion d'un paiement par chèque, mais cela dans les transactions à distance. En cela elle constitue une grande nouveauté et une meilleure sécurité pour les internautes.

➤ **Contiendra-t-elle des données médicales (groupe sanguin, maladies) ? Pourquoi ne pas la fusionner avec la carte Vitale ?**

Réponse : les deux cartes Vitale et INES sont clairement distinctes et complémentaires.

Vitale est une carte émise et gérée par l'assurance-maladie, pour traiter des données médicales.

INES est une carte émise et gérée par le ministère de l'intérieur, pour prouver son identité. Elle n'a pas à contenir des données médicales.

➤ **Y a-t-il un risque de voir la puce sans contact lue à distance, à l'insu du porteur, par un intrus ou par l'Etat ?**

Réponse :

Il ne faut pas confondre les étiquettes RFID, faites, comme toute étiquette, pour être lues facilement, avec des puces sans contact comme celles prévues dans la carte INES.

Le projet de CNIe prévoit deux modes d'accès sans contact à la puce qui sont tous deux sécurisés par des mécanismes ne permettant pas d'accéder aux données personnelles contenues dans la puce à l'insu du porteur de carte.

Il s'agit :

1) d'un code qui permettra d'accéder à la partie de la puce contenant l'identité et la photo (c'est à dire les mêmes informations que celles imprimées sur la CNIe : accéder à la puce n'apporte aucune information supplémentaire). Ce code se déduit des éléments imprimés sur la carte et nécessite donc de présenter la carte lors du contrôle (pas d'action à distance possible). Il s'agit d'un mode d'accès identique à celui retenu pour les passeports des pays extra-européens (« contrôle d'accès basique »).

2) d'un autre code et d'un matériel spécifiques pour accéder aux empreintes. Ce code et ce matériel seront réservés aux seuls services de contrôle (police, gendarmerie, douanes) européens pour les contrôles d'identité et les passages aux frontières. Il s'agit d'un mode d'accès identique à celui retenu pour les passeports européens (« contrôle d'accès étendu », prévu par le règlement européen du 13 décembre 2004).

Aucun autre accès sans contact n'est prévu.

On ne peut donc ni « suivre quelqu'un à la trace » grâce à des bornes dans la rue (ces bornes ne connaissent pas les codes des cartes qui passent à proximité), ni, comme certains le craignent, connaître les noms des participants à une manifestation.

➤ **Les titres INES seront-ils réellement infalsifiables?**

Réponse : rien n'est infalsifiable à 100%. On pourrait remplacer le terme "infalsifiable" par:

"dont la falsification demanderait de tels moyens que cela devient hors de portée des fraudeurs actuels, et que cela ne serait de toute façon pas rentable pour eux".

➤ **Des faussaires peuvent-ils fabriquer des fausses cartes ?**

Réponse : on peut certes fabriquer une fausse carte contenant des fausses données, mais alors celles-ci ne porteront pas la signature électronique de l'Etat (rappel : cette signature contient aussi, de manière infalsifiable, les données signées, ce qui garantit à la fois l'émetteur et le contenu).

Cela la désignera automatiquement comme fausse.

En outre, un dispositif supplémentaire est prévu par lequel la vraie carte, avec des clefs secrètes (non recopiables), prouve son authenticité.

➤ **La puce est-elle sûre ? Les cartes bancaires ne le sont pas.**

Réponse : dans les cas de fraude à la carte bancaire, les fraudeurs ont porté leur attaque sur des actes ne mettant pas en jeu toutes les sécurités de la puce, soit en fabriquant des copies de vraies cartes (mais sans pouvoir copier la puce) pour servir à l'étranger (où la puce n'est pas contrôlée), soit en trompant en France des dispositifs ne pratiquant pas de contrôle de haut niveau.

Par contre, aucune attaque n'a réussi à ce jour contre des systèmes utilisant tous les dispositifs de sécurité de la puce.

La CNIE mettra en œuvre le niveau le plus élevé de sécurité conformément aux recommandations de la DCSSI ...