Fonctionnalités des cartes d'identité électroniques européennes concernant la protection des données privées

enisa
European Network and Information Security Agency

www.enisa.europa.eu

Ce document de synthèse a été écrit en Anglais. Le document que vous lisez est une traduction en français. L'ENISA c'est assuré que la traduction était de qualité, mais dû aux difficultés de la traduction, des différences mineures entre la traduction et l'original peuvent exister ainsi que des imprécisions ou erreurs de traduction dans l'ensemble ou dans des parties. Les traductions des documents de l'ENISA sont disponibles uniquement dans un but d'information et de diffusion.

Version: 1.0.1fr

Date de publication : 27/01/2009 (version originale), 18/06/2009 (traduction française)

Les documents de synthèse de l'ENISA présentent des opinions d'experts sur des questions importantes liées à la sécurité des réseaux et de l'information. Ils sont produits par un groupe de personnes sélectionnées pour leur expertise dans le domaine. Le contenu de ce document a été débattu entre juillet 2008 et janvier 2009 à la faveur d'échanges de courriers électroniques et de communications personnelles. Les données présentées dans les tableaux se fondent sur les informations fournies par les experts et sur les références citées dans la dernière section. Le contenu de ce document a été préparé par l'ENISA et la version finale a été révisée par les personnes citées ci-dessous.

Auteurs: **Ingo Naumann, Giles Hogben**
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)
Courriel: eid@enisa.europa.eu

Collaborateurs:

Herbert Leitold	**Zentrum für sichere Informationstechnologie (A-SIT), *Autriche***
Frank Leyman, Marc Stern	**Fedict, *Belgique***
Tarvi Martens	**AS Sertifitseerimiskeskus (SK), *Estonie***
Jens Bender, Dennis Kügler	**Bundesamt für Sicherheit in der Informationstechnik (BSI), *Allemagne***
Andrea de Maria	**Istituto Poligrafico e Zecca dello Stato (IPZS), *Italie***
André Vasconcelos	**Agence pour la réforme des services publics (AMA), *Portugal***
Roberth Lundin	**CEN TC 224 WG 15 (Carte d'identité européenne)**

Les membres de ce groupe participent en leur nom propre. Ce document ne doit donc pas être considéré comme reflétant les opinions de l'une ou l'autre entreprise ou organisation, et n'engage les membres du groupe en aucune manière lorsqu'ils traitent de ces questions dans d'autres contextes.

Avis juridique

Table des matières

Résumé

Jeton d'authentification et source de données à caractère personnel, une carte d'identité électronique nationale est une voie d'accès aux informations personnelles. Toute divulgation non souhaitée d'informations personnelles découlant de la délivrance ou de l'utilisation de la carte constitue une violation des droits du citoyen en matière de vie privée. Indépendamment des considérations relatives à ces droits fondamentaux, cette divulgation constitue également une sérieuse entrave à l'adoption de systèmes de carte d'identité électronique et à leur interopérabilité transfrontalière.

Ce document a pour objet de comparer les fonctions de protection de la vie privée intégrées dans les spécifications des cartes d'identité électroniques européennes en vue de faciliter l'identification des meilleures pratiques. Le public cible est constitué des décideurs du monde de l'entreprise et de la scène politique. Le document tend à leur faire prendre conscience des implications juridiques et sociales des dernières évolutions dans les technologies des cartes d'identité électroniques. Plus particulièrement, les conclusions devraient avoir de fortes implications pour les politiques de protection des données et de sécurité. Dresser l'état des lieux est une première étape essentielle vers la réalisation des objectifs importants que sont l'identification des meilleures pratiques, l'amélioration du niveau de base de protection de la vie privée des citoyens en matière de cartes d'identité électroniques à travers toute l'Europe et enfin l'amélioration de l'interopérabilité et de l'adoption par les citoyens.

Nous analysons les risques pour la vie privée découlant de l'utilisation de systèmes nationaux de carte d'identité électronique et présentons toutes les techniques réalisables disponibles pour les aborder. La majeure partie du document est ensuite consacrée à une enquête sur les modalités d'application des technologies d'amélioration du respect de la vie privée dans les systèmes européens existants et planifiés de carte d'identité électronique, dans la carte d'identité européenne et dans les spécifications techniques de l'OACI pour le passeport électronique. Les informations se fondent sur les spécifications publiques les plus récentes, s'accompagnent de références exhaustives et sont présentées sous la forme de tableaux pour faciliter la comparaison. Les informations présentées dans les tableaux illustrent la diversité du paysage européen en matière de carte d'identité électronique. Bien que ce document ne compare que les fonctions de protection de la vie privée, les autres aspects des cartes présentent la même diversité.

1. Introduction

Jeton d'authentification et source de données à caractère personnel, une carte d'identité électronique est une voie d'accès aux informations personnelles. Cela implique un ensemble de risques pour la vie privée des citoyens, liés à une éventuelle divulgation non souhaitée d'informations personnelles et à leur utilisation abusive. Il est fondamental de s'attaquer à ces risques, principalement parce qu'ils constituent une menace envers les droits humains fondamentaux du citoyen garantis par l'article 8 de la Convention européenne des droits de l'homme [23], en particulier lorsque la détention de la carte est obligatoire ou fortement encouragée par le fait qu'elle permet d'accéder

à des services importants voire essentiels. Un autre élément dont les gouvernements doivent tenir compte est que les menaces pour la vie privée démotivent fortement les citoyens à utiliser ces systèmes. La protection adéquate de la vie privée est donc une condition *sine qua non* dans les pays où la carte d'identité est facultative. Mais même lorsqu'elle est obligatoire, les risques pour la vie privée influenceront le taux d'utilisation de la carte et nuiront à sa popularité, ce qui compliquera la mise en application d'obligations, quelles qu'elles soient.

C'est pourquoi tous les systèmes existants et planifiés comportent déjà au moins quelques *fonctions de protection de la vie privée* pour protéger le titulaire de la carte contre toute divulgation non souhaitée et toute utilisation abusive de ses informations personnelles.

Ce document a pour objectif de comparer les fonctions de protection de la vie privée intégrées dans les fonctionnalités des cartes d'identité électroniques européennes en vue de faciliter l'identification des meilleures pratiques. Dresser l'état des lieux est une première étape essentielle vers la réalisation des objectifs importants que sont l'identification des meilleures pratiques, l'amélioration du niveau de base de protection de la vie privée des citoyens en matière de cartes d'identité électroniques à travers toute l'Europe et enfin l'amélioration de l'interopérabilité et de l'adoption par les citoyens.

Aux fins du présent document, on entend par *fonctionnalité de protection de la vie privée*:

toute fonctionnalité d'une carte d'identité électronique qui permet à son titulaire de mieux maîtriser la nature des données divulguées à son propos ainsi que leur destinataire

Ceci comprend la maîtrise de la divulgation d'informations à des personnes malveillantes ou détenant illégitimement la carte, sur l'identifiabilité involontaire du titulaire de la carte par la possibilité de liaison entre les actions d'authentification, sur la fuite de données vers des observateurs fortuits et sur la divulgation légitime des données du titulaire avec un *niveau de garantie inutilement élevé,* due à l'utilisation de la signature numérique en guise d'authentification (voir 4.3.2 Comparaison Authentification/Signature numérique). Il existe une grande variété de fonctions de protection de la vie privée: de la simple protection par code PIN à des mécanismes sophistiqués de contrôle d'accès basé sur des certificats ou des identifiants spécifiques à un domaine.

Dix États membres de l'Union européenne ont déjà mis en place des cartes d'identité électroniques et treize autres se sont engagés à le faire et en sont à des stades divers de planification (voir Tableau 1). La multiplication des systèmes en place crée des perspectives pour des initiatives paneuropéennes exploitant la nouvelle infrastructure. Des initiatives politiques européennes telles que la directive sur les services [25] supposent déjà l'existence d'une infrastructure interopérable transfrontalière et des initiatives telles que STORK [48] explorent des applications transfrontalières ambitieuses.

À l'instar de la plupart des autres aspects des cartes d'identité électroniques, les fonctions de protection de la vie privée ont été développées, mises en œuvre et testées au niveau national. Aucune stratégie coordonnée au niveau européen ne précise la nature des fonctionnalités à déployer et les modalités de cette mise en œuvre. L'absence de coordination est une entrave substantielle à toute interopérabilité transfrontalière éventuelle des systèmes de carte d'identité électronique. Cette coordination est essentielle pour garantir l'interopérabilité technique (des fonctionnalités attendues dans un système pourraient être absentes dans un autre, ce qui empêcherait l'interopérabilité). Toutefois, cet aspect est des plus importants à si l'on veut que les utilisateurs aient confiance dans ces systèmes – tout système transfrontalier ne garantit que le niveau de protection offert par son élément le plus faible: si un seul pays participant propose une protection de la vie privée communément considérée comme inadéquate, il est peu probable que les citoyens des autres pays acceptent un quelconque système transfrontalier qui constitue un risque plus important pour leurs données que leur système national.

Ce document donne un bref aperçu de la gamme de fonctions de protection de la vie privée disponibles, mais nous renvoyons à un article précédent [44] pour une description plus détaillée de ces fonctions. L'objet principal de ce document est de dresser l'état des lieux de la mise en œuvre de ces fonctions dans les divers systèmes nationaux de carte d'identité électronique. Il s'agit d'un point de départ essentiel, gage d'une mise en œuvre uniforme et interopérable des meilleures pratiques pour protéger les données privées des citoyens, et d'un élément essentiel de toute initiative d'interopérabilité plus vaste. Les données présentées facilitent également la comparaison des fonctions entre les systèmes des États membres et, nous l'espérons, pourront ainsi également déboucher sur une amélioration générale du niveau des fonctions de protection de la vie privée.

Tableau 1 – Systèmes de carte d'identité dans l'Espace économique européen (EEE) – Aperçu

Pays	Carte d'iden-tité?	Carte d'identité obligatoire (i)/principale	Carte d'identité électro-nique? (ii)	Carte d'identité électro-nique planifiée?	Références
Autriche	oui	non	oui	--	[1][38][51]
Belgique	oui	oui	oui	--	[5][38] [50][51]
Bulgarie	oui	oui	(non)	(non)	[38][50][51]
Chypre	oui	oui	non	non	[38][40] [50][51]
République tchèque	oui	oui	non	non	[38][50][51]
Danemark	non	--	--	non	[38][50][51]
Estonie	oui	(oui)	oui	--	[6][38][50]
Finlande	oui	non	oui	--	[7][38] [50][51]
France	oui	oui	non	oui	[38][50][51]
Allemagne	oui	(oui)	non	oui (spec.)	[10][38] [50][51]
Grèce	oui	oui	non	non	[38][50][51]
Hongrie	oui	non	non	oui	[38][50][51]
Irlande	non	--	--	non	[38][50][51]
Italie	oui	(oui)	oui (partiel)	--	[11][38] [50][51]
Lettonie	non	--	--	oui	[38]
Lituanie	oui	oui	non	non	[38][51]
Luxembourg	oui	oui	non	oui	[38][51]
Malte	oui	oui	non	oui	[38][51]
Pays-Bas	oui	(oui)	oui	--	[13][24] [38][51]
Pologne	oui	oui	non	oui	[14][38] [50][51]
Portugal	oui	oui	oui	--	[15][38] [50][51]
Roumanie	oui	oui	non	oui	[38][50][51]
Slovaquie	oui	oui	non	oui	[38][50][51]
Slovénie	oui	(oui)	non	oui	[33][38][40]
Espagne	oui	oui	oui	--	[16][38] [50][51]
Suède	oui	non	oui	--	[17][38] [51][52]
Royaume-Uni	oui (partiel)	inconnu	oui (partiel)	--	[20][21][27] [38][50][51]
Islande	oui	oui	non	oui	[38][51]
Liechtenstein	oui	non	non	oui	[38]
Norvège	non	--	--	non	[50][51]
Total	25	20	10	13	

Commentaires:

i. Dans certains pays, la détention d'une carte d'identité ou d'un passeport est obligatoire. Toutefois, l'adjectif «obligatoire» revêt des significations et des implications différentes selon les pays. Par exemple, l'obligation d'avoir une carte d'identité peut s'appliquer uniquement après un certain âge; dans certains cas, la carte d'identité est obligatoire pour les nationaux et les étrangers résidant dans le pays; souvent, la carte d'identité n'est obligatoire que pour les nationaux résidant à l'intérieur du pays. Un «oui» entre parenthèses dans cette colonne indique que la carte d'identité est la pièce d'identité principale au sens plus large.

ii. Les entrées «oui»/ «spec.» dans ces colonnes sont surlignées en rouge pour référer aux applications/ spécifications prises en compte.

2. Menaces pour la vie privée

Avant de décrire les fonctions de protection de la vie privée, nous présentons un aperçu des catégories de menaces (exploitation d'une vulnérabilité) contre lesquelles elles tentent d'apporter une protection. Notez qu'en définissant un risque comme la potentialité qu'une menace donnée exploite les vulnérabilités d'un système donné, nous n'essayons pas d'évaluer le niveau de risque général posé par ces menaces, car nous ne disposons pas d'informations sur la probabilité de leur survenance.

2.1. Actifs

Les actifs sont la cible de la protection dans une analyse des risques. Les principaux actifs en danger dans les scénarios de carte d'identité électronique sont généralement les informations personnelles et l'anonymat du citoyen. La perte de ces actifs peut mettre en péril des actifs secondaires tels que la propriété physique, des actifs financiers, la réputation (p. ex. si la carte est utilisée pour usurper l'identité de son titulaire) et le droit à ne pas être importuné (par du spam, etc.).

2.2. Menaces

Nous présentons ci-dessous les classes de menaces (impact négatif potentiel dû aux vulnérabilités d'un système) pour les actifs de données à caractère personnel dans les systèmes utilisant des cartes d'identité électroniques. L'objet de ce document est de faire l'état des lieux des mesures utilisées pour faire face à ces menaces dans les systèmes de carte d'identité électronique existants ou planifiés. Nous n'en donnons donc ici qu'une brève description et renvoyons à des explications plus détaillées dans des documents connexes tels que [32]. Notez que, suivant notre définition d'un risque pour la vie privée, toute vulnérabilité qui expose les données présentes sur la carte crée un risque pour la vie privée:

1. *Falsification du contenu:* la falsification du contenu due à l'écriture non autorisée dans le système de fichiers de la carte constitue une menace. Un identifiant unique modifié pourrait, par exemple, être accepté comme authentique si aucune mesure de sécurité appropriée n'était mise en place.

2. *Espionnage électronique:* un attaquant intercepte la communication entre la carte et le lecteur, et lit les données. Cet aspect revêt toute son importance pour les interfaces de carte sans contact mais il s'applique également aux interfaces avec contact utilisant des lecteurs et câbles non protégés (voir [52]).
3. *Attaques «man in the middle»:* similaire à la menace «espionnage électronique» mais l'attaquant se trouve entre la carte et le serveur/l'intergiciel et communique avec les deux côtés.
4. *L'utilisateur signe un faux document:* cela peut arriver par exemple si ce que l'utilisateur voit n'est pas ce qu'il signe vraiment. Cette situation peut constituer une menace pour la vie privée car elle pourrait dénaturer les données de l'utilisateur, ce qui compromettrait le principe du droit à la rectification, essentiel à la protection de la vie privée.
5. *L'utilisateur s'authentifie sur un faux serveur* parce qu'il accorde à tort sa confiance à un serveur. Ceci constitue une menace pour la vie privée car le faux serveur peut alors accéder aux informations de l'utilisateur.
6. *Délégation inappropriée de l'usage de la carte:* l'usage de la carte peut parfois être délégué volontairement à un tiers. Dans certains cas, lorsque des mesures appropriées sont prises contre les abus, cette délégation peut constituer une utilisation légitime de la carte. Dans d'autres cas, toutefois, les titulaires se mettent en danger en déléguant l'usage de leur carte.
7. *Perte ou vol de la carte:* si la carte est pourvue de mécanismes de preuve de possession et/ou de contrôle d'accès inadéquats, les données à caractère personnel sont mises en péril.
8. *Attaques physiques:* attaques invasives impliquant par exemple le recâblage d'un circuit sur la puce ou l'utilisation de broches de sondage pour observer les flux de données. Le but de ces attaques est généralement le vol de clés privées pour accéder aux données privées.
9. *Attaques par canaux auxiliaires:* ces attaques tirent profit des informations transparaissant de ce qu'on appelle les canaux auxiliaires pour accéder aux données privées. Ces informations complémentaires pourraient être le rythme des signaux, la consommation électrique ou le rayonnement.
10. *Attaques cryptoanalytiques:* ces attaques ciblent directement les algorithmes cryptographiques dans le but de percer la confidentialité des informations transmises (p. ex. entre la carte et le lecteur).
11. *Attaques par «skimming» (écrémage):* un attaquant ouvre une connexion clandestine vers la carte et accède aux données. Cette menace pour la vie privée ne s'applique pas aux cartes avec contact puisque la carte doit dans ce cas être insérée manuellement dans le lecteur. La distance maximale depuis laquelle une carte d'identité électronique peut être lue est généralement relativement limitée (environ 25 cm pour les cartes compatibles ISO14443, voir [34][35]), mais l'écrémage reste théoriquement possible. Même ainsi, il existe une incitation considérable à installer un dispositif de lecture caché, suffisamment proche des cartes d'identité électroniques portées dans les poches arrière ou les sacs à main, qui écrème les informations personnelles des cartes d'identité électronique.
12. *Pistage de la localisation:* un attaquant génère des profils de mouvement spécifiques à la personne ou à la carte en se basant sur la localisation des lecteurs. Cette manœuvre est

plus probable et plus puissante en combinaison avec une attaque d'écrémage, bien qu'elle puisse s'intégrer dans le cadre d'une application légitime (p. ex. la billetterie pour le transport).

13. *Profilage comportemental:* similaire au pistage de la localisation mais au lieu de contenir (simplement) la localisation, le profil contient des informations sur le type d'authentification, l'argent dépensé, les endroits visités, etc.
14. *Preuve de la véracité des informations personnelles à un tiers:* un autre détail intéressant est de savoir si les informations personnelles sont signées numériquement par le producteur du document, p. ex. parce qu'elles sont incluses dans un certificat de clé publique. C'est le cas avec les passeports électroniques. Lorsque la signature n'est pas réellement nécessaire pour effectuer l'opération requise, cela constitue une menace pour la vie privée puisque des données sont fournies avec un niveau de garantie non requis (voir 4.3.2. Comparaison Authentification/Signature numérique), ce qui permet au prestataire de services qui lit les données de prouver leur véracité à un tiers lors de toute transaction ultérieure. Cet aspect est souvent oublié étant donné que le problème n'est pas que l'on divulgue davantage de données à caractère personnel, mais que l'on expose davantage ces données divulguées à un abus potentiel.

3. Lutte contre les menaces pour la vie privée

3.1. Fonctions de protection de la vie privée disponibles sur les cartes d'identité électroniques

Voici une description générale des classes de fonctions des cartes d'identité électroniques conçues pour lutter contre les risques présentés ci-dessus.

1. *Blocs de données chiffrés:* les données présentes sur la carte sont chiffrées avec une clé secrète. Tout lecteur peut lire le bloc de données brut mais il faut connaître cette clé secrète pour obtenir les informations qu'il contient. Le seul avantage supplémentaire qu'offre cette fonction lorsqu'un contrôle d'accès adéquat est garanti est que les données peuvent rester confidentielles lorsqu'elles sont transmises à des tiers après avoir quitté la carte (pour autant que les clés secrètes ne soient pas transmises elles aussi). N.B.: les blocs de données chiffrés ne sont utilisés dans *aucun* système européen de carte d'identité électronique.
2. *Mécanismes de contrôle d'accès:* les données se trouvent sur la carte en texte clair mais le prestataire de services/lecteur de carte ne peut y accéder qu'après l'authentification réussie du prestataire de services/titulaire de la carte (preuve de possession). L'authentification réussie consiste habituellement à prouver la connaissance d'un code PIN ou d'une clé secrète/privée. L'authentification est dite «mutuelle» si, simultanément, la carte s'authentifie au service et le lecteur prouve sa fiabilité à la carte et à son titulaire.
3. *Utilisation d'identifiants uniques (UID) respectueuse de la vie privée:* les identifiants uniques sont des chaînes qui permettent aux applications de distinguer les citoyens (UID spécifique

au citoyen) ou leurs cartes d'identité (UID spécifique à la carte). Un UID spécifique à la carte change lorsqu'une nouvelle carte est donnée au citoyen. Il convient d'utiliser les identifiants avec la plus grande prudence pour prévenir les risques en matière de vie privée. Un système UID bien conçu pourrait mieux préserver la vie privée que, par exemple, l'utilisation d'un numéro de sécurité sociale ou la combinaison du nom et de la date de naissance en guise d'UID. En règle générale, plus un UID peut être relié à une utilisation dans d'autres transactions (utilisant la carte ou autres), moins il permet de préserver la vie privée. Il est important de noter que toutes les informations individuelles statiques présentes sur la carte, telles qu'une clé publique ou même un bloc de données chiffré, présentent toutes les caractéristiques d'un UID si elles sont uniques.

4. *UID spécifique à un domaine* (ou UID spécifique à un secteur ou identifiants personnels spécifiques à un secteur): l'utilisation de différents identifiants dans différents domaines d'application contribue à éviter la fusion de bases de données. Les identifiants spécifiques à un domaine peuvent être dérivés d'identifiants (secrets) détenus par un émetteur central fiable.
5. *Divulgation sélective:* un principe communément admis en matière de protection de la vie privée est que le volume de données divulguées devrait être le minimum requis pour l'application concernée. C'est par exemple un principe de la législation européenne en matière de protection des données ([23], article 7). Pour respecter ce principe, la carte ne devrait pas divulguer davantage d'informations que celles demandées par l'application effectuant la requête. Par exemple, si l'application de requête demande uniquement le nom du titulaire de la carte, celle-ci ne devrait pas donner accès à son adresse.
6. *Mode simple vérification:* constitue un cas simple de divulgation sélective où , au lieu de divulguer la valeur d'un champ, une réponse oui-non est donnée quant à savoir si une requête est satisfaite – p. ex. est-ce que l'âge est plus élevé qu'une certaine valeur ou est-ce qu'un élément biométrique correspond (selon une certaine probabilité) à un gabarit donné. Ou, par exemple si le serveur demandeur demande à la carte de certifier que le titulaire est âgé de 18 à 30 ans (une valeur booléenne), la carte ne devrait pas divulguer sa date de naissance. L'interprétation complète de ce principe et du précédent nécessiterait l'intégration d'un module de requête sur la carte, appliquant une chaîne d'interrogation aux données contenues. Cela requiert un traitement trop important et est dans une large mesure inutile puisque les cas où une requête ne peut être satisfaite exactement par les champs existants sont assez limités pour la plupart des applications de la carte d'identité électronique. Au lieu de cela, pour la plupart des applications, il suffit de pouvoir divulguer certains champs sélectionnés (plutôt que l'ensemble des données) et de certifier si la date de naissance de l'utilisateur est comprise ou non dans une certaine tranche (généralement pour prouver qu'il a plus de 18 ans). Autre caractéristique connexe importante: une fonction «match on card» pour les informations relatives aux empreintes digitales. Il existe plusieurs autres cas utiles, tels que la preuve des aptitudes de conduite ou de la citoyenneté européenne.
7. *Gabarits biométriques:* un gabarit biométrique est un ensemble de données tirées d'informations biométriques (p. ex. une photographie numérique d'une empreinte digitale) qui permet une comparaison avec les données biométriques réelles. L'utilisation de

gabarits biométriques, au lieu de photographies, peut être considérée comme une mesure de protection de la vie privée étant donné que les informations biométriques proprement dites ne sont pas stockées sur la carte, ce qui diminue la quantité d'informations stockées à propos de son titulaire.

8. *Communication sûre entre la carte, l'intergiciel et le serveur:* une fois les données divulguées par la carte, elles sont vulnérables à un éventuel espionnage électronique lors de leur transfert entre la carte et l'intergiciel qui interagit avec la carte ainsi que plus loin dans la chaîne, lors de leur transfert entre l'intergiciel et le service de destination. Afin de respecter la vie privée du titulaire de la carte, les données devraient dès lors être chiffrées entre ces trois entités, idéalement sous la forme d'un chiffrement de bout en bout entre la carte et le serveur, ce qui diminuerait le risque de compromettre l'intergiciel/ordinateur du titulaire de la carte.

Vous trouverez des explications plus détaillées sur certains de ces mécanismes dans le document [44].

3.2. Exemples dans les spécifications existantes

La littérature donne quelques exemples d'application de technologies de protection de la vie privée (PET) dans les cartes d'identité (et les passeports) électroniques:

- Le *Basic Access Control* (BAC), tel que défini dans les specifications de l'OACI pour les documents de voyage lisibles par machine (*Machine Readable Travel Documents*) [37] afin d'éviter l'écrémage et, dans une moindre mesure, l'espionnage électronique.
- Le *Extended Access Control*(EAC) (européen) [8][9], tel que spécifié par l'Office fédéral allemand pour la sécurité de l'information et adopté par l'Union européenne, s'attaque à certaines faiblesses mineures du BAC et empêche les dispositifs non autorisés de lire les informations d'empreintes digitales stockées sur les passeports de l'UE. Il est également proposé d'inclure ce mécanisme, en tant qu'«EAC modulaire» dans le standard pour la carte d'identité européenne (ECC, *European Citizen Card*) [29][30].
- Le PACE [9] et des protocoles similaires, dont certains ont été adoptés par le standard ECC [29][30], ont à l'origine été mis au point pour la carte d'identité électronique allemande. Il remplace le BAC et complète l'EAC afin de permettre une authentification sur des serveurs distants par Internet.
- Des UID aléatoires pour l'établissement des canaux de communication sans contact ([37] Doc 9303 partie 3 volume II section III A1.16, ou dans les versions antérieures, supplément au doc 9303 de l'OACI, E11).

Les identifiants spécifiques à un domaine (ou UID), également appelés identifiants spécifiques à un secteur [1][3] ou identité restreinte [9], comme expliqué plus haut (voir le point 4 sous 3.1 Fonctions de protection de la vie privée disponibles sur les cartes d'identité électroniques) sont intégrés dans les systèmes de carte d'identité électronique autrichien [3] et allemand [9].

3.3. ICP à confidentialité améliorée

Les «jetons ICP à confidentialité améliorée» installés dans les produits tels que l'ancien U-Prove (récemment acquis par Microsoft) [31] et Idemix (IBM) [36] offrent des techniques cryptographiques qui peuvent:

- empêcher la possibilité de liaison entre les identifiants présentés à différents services, même si ces fournisseurs de services et l'émetteur des pièces d'identité partagent les données ou s'associent d'une autre manière par la suite. En recourant à ces technologies, l'utilisateur peut être connu sous un pseudonyme différent auprès de chaque fournisseur de services. Cela lui permet de produire une affirmation garantie à son propos sans révéler la moindre information inutile (par un lien avec d'autres transactions). Plus particulièrement, le vérificateur ne peut découvrir le pseudonyme sous lequel l'utilisateur est connu auprès de l'émetteur;
- apporter une fonctionnalité de divulgation sélective plus étendue;
- appliquer des protocoles limités (p. ex. pour l'argent électronique) par lesquels l'utilisateur ne peut prouver une affirmation qu'un nombre limité de fois;
- apporter une révocation globale de plusieurs certificats détenus par un utilisateur tout en maintenant l'impossibilité de les relier pour l'émetteur et les vérificateurs (voir [28]). Notez que l'on part ici de l'hypothèse raisonnable que ni l'émetteur ni le vérificateur ne peuvent ajouter d'entrées arbitraires à la LRC. S'ils pouvaient le faire, cela leur permettrait d'effectuer des attaques en force en révoquant temporairement des combinaisons de certificats et en essayant ensuite d'en vérifier d'autres. Il s'agit toutefois d'une hypothèse raisonnable, puisque la plupart des LRC sont contrôlées par des procédures strictes qui rendraient cette attaque impossible.

De la sorte, les technologies ICP à confidentialité améliorée présentent un potentiel significatif d'amélioration des fonctions de protection de la vie privée actuelles des cartes d'identité électroniques. Bien que ces technologies soient disponibles depuis longtemps, on ne constate qu'une faible adoption[1] dans les applications dominantes et dans les déploiements des cartes d'identité électroniques.

4. Aperçu des caractéristiques des cartes d'identité électroniques européennes

Les passeports électroniques contiennent uniquement une «application OACI», nom habituellement donné aux fonctionnalités conformes aux caractéristiques de l'OACI [37][2]. Les cartes d'identité électroniques peuvent également être pourvues d'applications supplémentaires. Les cartes avec contact sont généralement pourvues d'une application de signature électronique qui peut être utilisée pour signer

[1] *L'Autriche et l'Allemagne ont entrepris des démarches importantes vers l'impossibilité de liaison et la divulgation sélective (voir le chapitre 3.2).*

[2] *Les différents ensembles de fonctionnalités des cartes intelligentes sont appelés «applications»[46].*

électroniquement des documents. En général, l'utilisateur doit saisir un code PIN pour signer le document et ne peut récupérer la clé privée de la carte. Une troisième application, que l'on appelle aujourd'hui généralement «application eID», permet à l'utilisateur de s'authentifier et de se connecter par Internet à des services de commerce ou d'administration en ligne. Dans certains cas, cette application n'est pas différente d'une application de signature électronique à l'exception de la désignation des certificats à des fins d'authentification (voir également 4.3.2 Comparaison Authentification/Signature numérique).

À des fins comparatives, nous avons inclus dans les tableaux les données des caractéristiques des passeports électroniques, selon l'OACI et l'Union européenne (OACI/UE[3]).

4.1. Interfaces et fonctionnalité

Le tableau suivant donne un aperçu des cartes d'identité électroniques européennes existantes (ou spécifiées), de leurs interfaces et de leurs applications.

Tableau 2 – Interfaces et fonctionnalité

Caractéristique	Interface	Signature électronique (facultative) (i)	Application eID	Références
AT	**contact**	**oui**	**oui**	**[1]**
BE	**contact**	**oui**	**oui**	**[5]**
EE	**contact**	**oui**	**oui**	**[6]**
FI	**contact**	**oui**	**oui**	**[7]**
DE	**sans contact**	**oui**	**oui**	**[9][10]**
IT	**contact**	**oui**	**oui**	**[11]**
NL	**sans contact**	**non**	**non**	**[13]**
PT	**contact**	**oui**	**oui**	**[15]**
ES	**contact**	**oui**	**oui**	**[16]**
SE	**contact et sans contact (deux puces)**	**oui**	**oui**	**[17][38]**
UK	**contact et sans contact**	**inconnu**	**inconnu**	**[27]**

[3] *Les spécifications du passeport électronique européen modifient les spécifications de l'OACI en apportant une définition et l'exigence du contrôle d'accès étendu (EAC). Il existe au moins une autre définition du contrôle d'accès étendu, formulée par le gouvernement de Singapour. Dans ce document, nous nous référons uniquement à la spécification européenne de l'EAC.*

ECC	**contact optionnel, sans contact ou les deux**	**oui**	**oui**	**[29][30]**
OACI	**sans contact**	**non**	**non**	**[37]**
OACI/UE	**sans contact**	**non**	**non**	**[37][22]**

Commentaires:

i. L'application de signature électronique est facultative dans toutes les caractéristiques, à l'exception de l'Estonie. Dans le cas de l'Autriche, l'activation de la fonctionnalité de signature électronique de la carte est obligatoire, mais la carte n'est pas obligatoire et ne constitue pas essentiellement un document de voyage.

4.2. Écriture de données sur une carte

La caractéristique de savoir s'il existe un accès en écriture aux données d'une carte après la personnalisation est un facteur essentiel en matière de sécurité et de vie privée. Cela étant, cet accès permet bien sûr de nombreuses applications utiles. Dans le tableau suivant, nous présentons les caractéristiques qui permettent l'accès en écriture aux données d'une carte.

Nous distinguons trois catégories de données acceptant l'écriture ou la mise à jour sur la carte:

les données primaires: les informations personnelles ou les UID du citoyen, également intégrés dans les certificats, ou l'adresse;

les données supplémentaires: les données spécifiques à des applications telles des lettres, des reçus, l'état de la déclaration fiscale ou même des fichiers personnels;

les données de fonctionnement: les informations minimales dont a besoin le système d'exploitation de la carte, telles que le nombre restant d'essais pour le mot de passe/code PIN, les horodateurs, les certificats vérifiables à partir de la carte actualisés.

Tableau 3 - Accès en écriture

Caractéristique	Les données primaires (p. ex. l'adresse) sur la carte peuvent-elles être modifiées?	Écriture possible sur les données supplémentaires	Écriture possible uniquement sur les données de fonctionnement	Références
AT	**oui (i)**	**oui**	**oui**	**[1]**
BE	**oui**	**oui**	**--**	**[5]**
EE	**oui (ii)**	**non**	**--**	**[6]**

FI	**oui**	**oui**	**--**	**[7]**
DE	**oui**	**non**	**oui**	**[9][10]**
IT	**non**	**oui**	**--**	**[11]**
NL	**non**	**non**	**non**	**[37]**
PT	**oui**	**oui**	**--**	**[15]**
ES	**inconnu**	**inconnu**	**inconnu**	
SE ct (contact)	**non**	**oui**	**oui**	**[18]**
SE cl (sans contact)	**non**	**non**	**non**	**[37]**
UK	**inconnu**	**inconnu**	**inconnu**	**[27]**
ECC	**facultatif**	**facultatif**	**facultatif**	**[29][30]**
OACI	**non**	**non**	**non**	**[37]**
OACI/UE	**non**	**non**	**oui**	**[22][37]**

Commentaires:

i. Techniquement faisable mais non utilisé puisque la modification des données primaires (p. ex. le nom du titulaire) conduirait à la révocation du certificat et au remplacement de la carte.

ii. EE: un utilisateur ne peut modifier les données présentes sur la carte. Toutefois, il est possible de renouveler les clés privées et les certificats sur la carte (par une procédure spéciale) depuis n'importe quel ordinateur connecté à Internet.

4.3. Fonctions de protection de la vie privée déployées

4.3.1. Contrôle d'accès

Différents mécanismes de contrôle d'accès sont intégrés dans les systèmes européens de carte d'identité électronique. La méthode la plus simple consiste à demander à l'utilisateur de saisir un code PIN (stocké sur la carte) avant de permettre l'accès à certains groupes de données. Pour utiliser la/les clé(s) privée(s) conçue(s) pour la signature (autorisée) ou l'authentification, l'utilisateur doit toujours saisir un code PIN secret.

Des clés secrètes peuvent également être utilisées en guise de justificatif d'identité pour accéder à la carte. Utilisant des algorithmes symétriques, la clé secrète doit être connue de la carte et du lecteur/serveur et est très souvent dérivée du numéro de série de la carte. Dans ce cas, la gestion des clés pour de grands systèmes est généralement assez complexe, car elle requiert l'échange sécurisé de nombreuses clés secrètes entre différentes entités.

Les algorithmes asymétriques peuvent aussi être utilisés pour authentifier le serveur au moyen d'une clé privée stockée sur le serveur. Dans le tableau, nous distinguons le contrôle d'accès basé sur une clé symétrique et le contrôle d'accès basé sur un certificat[4].

[4] *Bien que le contrôle d'accès de base et les mécanismes similaires qui empêchent l'écrémage soient en principe des mécanismes de contrôle d'accès basés sur une clé symétrique, nous ne les citons pas ici puisque la clé n'est pas secrète mais imprimée sur la carte. Nous ne considérons*

Tableau 4 – Fonctions de protection de la vie privée: contrôle d'accès et chiffrement

Caracté-ristique	Contrôle d'accès basé sur un PIN	Contrôle d'accès basé sur une clé symétrique	Contrôle d'accès basé sur un certificat	Stockage chiffré des données	Trans-mission chiffrée des données	Référence
AT	**oui**	**non**	**non**	**non**	**oui**	**[1]**
BE	**oui**	**non**	**oui (i)**	**non**	**oui**	**[5]**
EE	**oui**	**oui**	**non**	**non**	**oui**	**[6]**
FI	**oui**	**non**	**non**	**non**	**oui**	**[7]**
DE	**oui**	**non**	**oui**	**non**	**oui**	**[9][10]**
IT	**oui**	**non**	**non**	**non (iii)**	**oui**	**[11]**
NL	**non**	**non**	**non**	**non**	**oui**	**[13][24] [37]**
PT	**oui**	**non**	**oui**	**non**	**oui**	**[15][49]**
ES	**oui**	**oui**	**non**	**inconnu**	**oui**	**[16][53]**
SE ct	**oui**	**non**	**non**	**non**	**oui**	**[18]**
SE cl	**non**	**non**	**non**	**non**	**oui**	**[37]**
UK	**inconnu**	**inconnu**	**inconnu**		**inconnu**	
ECC	**facultatif**	**facultatif**	**facultatif**	**facultatif**	**facultatif**	**[29][30]**
OACI	**non**	**non**	**non**	**non**	**facultatif**	**[37]**
OACI/UE	**non**	**non**	**oui**	**non**	**oui**	**[22][37]**

Commentaires:

i. Uniquement pour un accès en écriture.
ii. Dépend du déploiement.
iii. Des données supplémentaires chiffrées sont stockées sur la piste laser de la carte d'identité italienne.

4.3.2. Comparaison Authentification/Signature numérique

Pour l'authentification et la signature numérique (autorisée), de nombreuses cartes d'identité électroniques européennes utilisent le même mécanisme mais des certificats et clés publiques différents. Cette pluralité de certificats réside généralement dans le fait que l'authentification et la signature numérique ont des implications juridiques différentes. Toutefois, l'utilisation d'une signature numérique pour des actions de simple authentification constitue une atteinte à la vie privée.

Une signature numérique laisse en effet toujours une preuve non récusable de l'acte de signature et permet à la partie utilisatrice de montrer les mêmes pièces (une simple réponse à un procédé d'identification ou des affirmations à propos du signataire), *avec*

toutefois pas la communication BAC comme chiffrée, puisque l'hypothèse est qu'un espion électronique n'a pas connaissance des données imprimées sur la carte. Voir plus bas.

le même niveau de garantie, à une autre partie. L'utilisation d'une signature électronique pour une authentification (p. ex. un procédé d'identification signé) constitue une plus grande menace pour la vie privée qu'une action de simple authentification, qui prouve seulement que la partie a été authentifiée. On peut comparer cette différence dans le monde réel au fait de *laisser* une *copie* avec signature certifiée d'une photo par opposition à simplement la *montrer* à quelqu'un pour s'identifier sans que cette personne n'enregistre la moindre donnée de cette photo signée.

Cette menace pour la vie privée n'est pas résolue par l'utilisation de deux certificats différents puisque tous deux transmettent des données signées. Bien que les signatures numériques authentifient en effet le signataire, elles révèlent, comme nous l'avons expliqué, des informations plus nombreuses à propos de la personne, avec un niveau de garantie plus élevé que nécessaire pour une action de simple authentification, ce qui est contraire au principe de divulgation minimale imposé par la législation européenne sur la protection des données (voir [23], article 7). Utiliser le mécanisme de signature numérique dans un protocole d'identification forte pour une authentification permet au prestataire de services de prouver l'authenticité de l'identification signée à un tiers [44] – ce qui constitue une atteinte plus importante à la vie privée du citoyen.

Tableau 5 – Comparaison Authentification/Signature numérique

Pays	Certificat d'authentification différent de la signature	Application de signature utilisée pour l'authentification?	Réf.
AT	**non (i)**	**oui**	**[1]**
BE	**oui**	**oui**	**[5]**
EE	**oui**	**oui**	**[6]**
FI	**oui**	**oui**	**[7]**
DE	**oui**	**non**	**[9][10]**
IT	**oui**	**oui**	**[11]**
PT	**oui**	**oui**	**[15]**
ES	**oui**	**oui**	**[16][53]**
SE	**oui**	**oui**	**[18]**
UK	**inconnu**	**inconnu**	
ECC	**facultatif**	**facultatif**	**[29][30]**

Commentaires:

i. Il existe une seconde paire de certificats/clés sur la carte pour les fonctionnalités supplémentaires, mais les applications de carte d'identité électronique et la signature électronique utilisent actuellement la même paire de clés.

ii. **Première colonne:** oui = utilisation de certificats et clés publiques et privées (et codes PIN définis) différents pour l'authentification et pour la signature numérique.
Deuxième colonne: oui = les *mécanismes* pour la signature électronique (signer le texte) et pour l'authentification (signer l'identification), y compris les longueurs des clés, etc., sont les mêmes.

4.3.3. Cartes d'identité électroniques sans contact

Deux pays de l'Union européenne délivrent actuellement des cartes d'identité pourvues d'une puce sans contact et d'une application OACI: les Pays-Bas et la Suède. Les deux pays ont adopté le BAC dans les caractéristiques de leurs cartes d'identité nationales où la zone de lecture optique (MRZ) est imprimée au dos de la carte.

Tableau 6 – Cartes d'identité électroniques sans contact

Pays	Application OACI	BAC	EAC	UID aléatoire	Réf.
DE	**oui (i)**	**non (i)**	**oui**	**oui**	**[9][10]**
NL	**oui**	**oui**	**non**	**oui**	**[37]**
SE	**oui**	**oui**	**non**	**inconnu**	**[37]**
ECC	**facultatif**	**facultatif**	**facultatif**	**facultatif**	**[29][30]**
OACI	**oui**	**facultatif**	**facultatif**	**facultatif**	**[37]**
OACI/UE	**oui**	**oui**	**oui**	**facultatif**	**[22][37]**

Commentaires:

i. Dans les caractéristiques de la carte d'identité électronique allemande, le BAC est remplacé par le PACE [9], et l'EAC s'applique à tous les groupes de données.

4.3.4. Informations personnelles et identifiants pouvant être liés

Les données à caractère personnel sur les cartes d'identité électroniques peuvent être stockées et transmises sous la forme de simples triplets pseudonyme-attribut-valeur (p. ex. Bob1 prénom «Bob») ou équivalents. De telles données *ne sont personnelles que si* le pseudonyme utilisé peut être relié à d'autres occurrences de ce pseudonyme qui sont d'une manière ou d'une autre associées de façon unique avec la personne physique. Par exemple, «coordonnées xyz: +51° 16' 26.76, +0° 21' 14.76» ne constitue pas des données à caractère personnel pour un prestataire de services sauf si ce prestataire de services connaît également la relation de ces données avec d'autres informations personnelles, p. ex. «numéro de sécurité sociale xyz: 1231412423412». Notez que les valeurs elles-mêmes peuvent également être des pseudonymes – p. ex. si la valeur est une chaîne de clé publique. Pour obtenir davantage d'informations sur ces possibilités de liaison, voir [45].

Bien entendu, le lien entre les identifiants est nécessaire dans toute application qui dépend d'une identité continue, mais dans de nombreux cas, une mauvaise gestion des pseudonymes divulgue davantage d'informations à davantage de parties que nécessaire pour l'exécution de l'application. Une mauvaise gestion des pseudonymes constitue dès lors une vulnérabilité en matière de vie privée puisqu'elle permet une divulgation inutile de données à caractère personnel par la mise en corrélation de différentes transactions.

Cette section décrit d'abord tous les champs de données disponibles sur la carte, et ensuite les mesures prises pour minimiser la possibilité de liaison entre les

pseudonymes utilisés dans différentes transactions. Notez que les technologies ICP à confidentialité améliorée (voir chapitre 3.3) pourraient permettre une gestion des pseudonymes plus sophistiquée que n'importe quel système de carte d'identité existant. Voici les possibilités offertes dans le cadre des fonctionnalités de carte d'identité existantes:

1. les UID spécifiques au citoyen: sont inféodés à chaque transaction et ne changent pas, même avec l'émission d'une nouvelle carte;
2. les UID spécifiques à la carte: changent lorsqu'une nouvelle carte est donnée au citoyen;
3. les identifiants spécifiques à un domaine. Des pseudonymes différents sont utilisés pour différents prestataires de services. Cette option peut être mise en œuvre avec divers degrés de granularité – c.-à-d. pas nécessairement un pseudonyme différent pour chaque fournisseur de services mais plutôt un ensemble limité de pseudonymes qui sont partagés par des groupes de fournisseurs.

Notons également que la gestion des UID ne figurant plus sur la carte a également des implications en matière de vie privée. Il existe dans certains cas des règlements et des politiques de sécurité qui empêchent l'utilisation des UID dans certains scénarios. Par exemple, l'utilisation d'un UID pourrait être limitée légalement à une utilisation uniquement par les pouvoirs publics et il pourrait être interdit aux fournisseurs d'applications de les stocker.

Les deux tableaux suivants montrent comment les pseudonymes sont gérés dans les systèmes actuels et quels champs de données sont disponibles. Les tableaux indiquent aussi les modalités d'accès à ces informations, ce critère étant important pour déterminer l'ampleur du risque que pose un système donné pour le respect de la vie privée. La question essentielle est de savoir combien d'efforts un attaquant doit fournir pour obtenir quelle quantité d'informations.

Nous distinguons les cas suivants:

NON UTILISÉ/STOCKÉ	Les informations ne sont pas stockées sur la carte ou n'existent pas.
SKIM	Tout le monde peut écrémer ces informations à une distance de quelques mètres. Un attaquant n'aurait qu'à se trouver à proximité de la carte pour pouvoir lire les informations. Notez que ce cas de figure ne s'applique à aucune des caractéristiques de carte examinées.
QUICONQUE	Quiconque est en possession de la carte peut accéder à ces informations, p. ex. si un attaquant trouve la carte en rue.
UTILISATEUR	L'utilisateur peut accéder à ces informations après avoir fourni des justificatifs d'identité (p. ex. un code PIN secret).
ÉTAT	L'État ou des entreprises privées agréées peuvent accéder à ces informations après avoir fourni des justificatifs d'identité (p. ex. une clé

secrète de l'État).

ÉTAT+UTILISATEUR	L'État ou des entreprises privées agréées peuvent accéder à ces informations après avoir prouvé la possession de justificatifs d'identité (p. ex. une clé secrète de l'État) *et* moyennant le consentement de l'utilisateur (p. ex. code PIN secret).
NON DÉFINI	Dépend de la mise en œuvre; dans certains cas, le cas le plus probable est indiqué entre accolades ({}).
INCONNU	Inconnu
GABARIT	Empreintes digitales: utilisation d'un gabarit; cette option peut être combinée à une des méthodes précédentes.

Tableau 7 – Informations personnelles I – identifiants uniques

Pays	UID carte (i)	UID citoyen (ii)	UID spécifique au domaine	Réf.
AT	NON DÉFINI {QUICONQUE}	NON DÉFINI {ÉTAT+UTILISATEUR}	QUICONQUE **(iv)**	**[1][4]**
BE	QUICONQUE	QUICONQUE	NON UTILISÉ	**[5]**
EE	QUICONQUE	QUICONQUE	NON UTILISÉ	**[6]**
FI	QUICONQUE	QUICONQUE	NON UTILISÉ	**[7]**
DE	ÉTAT **(iii)**	NON UTILISÉ	ÉTAT+UTILISATEUR	**[9][10]**
IT	QUICONQUE	UTILISATEUR	NON UTILISÉ	**[11][12]**
NL	QUICONQUE	QUICONQUE	NON UTILISÉ	**[13][37]**
PT	QUICONQUE	QUICONQUE	NON UTILISÉ	**[15][49]**
ES	QUICONQUE	ÉTAT+UTILISATEUR	NON UTILISÉ	**[16][53]**
SE ct (v)	QUICONQUE	QUICONQUE	NON UTILISÉ	**[38]**
SE cl	QUICONQUE	NON UTILISÉ	NON UTILISÉ	**[37]**
UK	INCONNU	INCONNU	INCONNU	
ECC	NON DÉFINI {QUICONQUE}	NON DÉFINI	NON DÉFINI	**[29][30]**
OACI	QUICONQUE	NON DÉFINI {NON UTILISÉ}	NON UTILISÉ	**[37]**
OACI/UE	QUICONQUE	NON DÉFINI {NON UTILISÉ}	NON UTILISÉ	**[22][37]**

Commentaires:

i. Un certificat, une clé publique ou un bloc de données chiffré unique peut également faire office, à toutes fins utiles, d'UID spécifique à la carte.
ii. Un sous-ensemble d'informations personnelles (p. ex. le nom et la date de naissance) n'est pas considéré comme un UID spécifique au citoyen dans ce contexte.
iii. Les clés publiques pour l'authentification de la puce ne seront *pas* uniques à chaque carte.
iv. Le calcul de l'identifiant spécifique au domaine (bPK) s'effectue dans un intergiciel spécial, hors de la carte. Les cartes sont déclinées sous de nombreuses formes variées (cartes de signature, cartes d'étudiant, etc.) et les mécanismes de contrôle d'accès peuvent varier. L'autorisation d'effectuer le hachage est conditionnée à la capacité à lire le code PIN source de la carte, ce qui dépend de nouveau de la version spécifique de cette carte. N.B.: la législation autrichienne sur l'administration électronique dispose que, pour les applications industrielles, ce calcul de hachage ne doit pas s'effectuer du côté serveur mais au niveau de l'intergiciel du citoyen.
v. Après personnalisation (les cartes d'identité électroniques suédoises sont fournies au citoyen sans personnalisation de la puce de contact).

Tableau 8 – Informations personnelles II

Pays	Informations personnelles (p. ex. le nom)	Image du visage	Informations sur les empreintes digitales	Réf.
AT	NON DÉFINI {QUICONQUE}	NON STOCKÉ	NON STOCKÉ	[1][2]
BE	QUICONQUE	QUICONQUE	NON STOCKÉ	[5]
EE	QUICONQUE	NON STOCKÉ	NON STOCKÉ	[6]
FI	QUICONQUE	NON STOCKÉ	NON STOCKÉ	[7]
DE	ÉTAT/ ÉTAT+UTILISATEUR (i)	ÉTAT	ÉTAT/NON STOCKÉ (i)	[9][10]
IT	UTILISATEUR	INCONNU (iii)	INCONNU (iii)	[11][12]
NL	QUICONQUE	QUICONQUE	NON STOCKÉ	[13][37]
PT	QUICONQUE	QUICONQUE	GABARIT	[15][49]
ES	ÉTAT+UTILISATEUR	ÉTAT+UTILISATEUR	NON STOCKÉ	[16][53]
SE ct (iii)	QUICONQUE	NON STOCKÉ	NON STOCKÉ	[18]
SE cl	QUICONQUE	QUICONQUE	NON STOCKÉ	[37]
UK	INCONNU	INCONNU	INCONNU	
ECC	NON DÉFINI	NON DÉFINI	NON DÉFINI	[29][30]
OACI	QUICONQUE	QUICONQUE	NON DÉFINI	[37]
OACI/UE	QUICONQUE	QUICONQUE	ÉTAT	[22][37]

Commentaires:

i. Selon [10], le citoyen peut décider si ses empreintes digitales seront stockées sur la carte.
ii. Les instances publiques (police, douanes) ont besoin de détenir la carte (pour un contrôle d'accès PACE utilisant le CAN (numéro d'accès à la carte) ou la zone de lecture optique, tous deux imprimés sur la carte) et doivent s'authentifier en utilisant une authentification basée sur une ICP. Les institutions d'affaires/d'administration en ligne ont besoin du consentement de l'utilisateur (PACE utilisant un code PIN) et doivent s'authentifier en utilisant une authentification basée sur une ICP.
iii. Déclaré comme «à définir» dans[12].
iv. Après personnalisation. Voir plus haut.

5. Conclusions

De nombreuses techniques très pratiques permettent de protéger la vie privée du citoyen et, à partir de l'enquête sur les techniques disponibles présentée dans ce document, il est possible d'identifier un ensemble de lignes directrices pour les meilleures pratiques en matière de protection des données à caractère personnel dans les systèmes nationaux de carte d'identité électronique. Les spécifications des cartes d'identité électroniques européennes sont très variées en ce qui concerne la mise en œuvre des fonctions de protection de la vie privée que nous avons identifiées: leur mise en œuvre n'est aucunement universelle et lorsqu'elles sont appliquées, leur interopérabilité technique n'est pas toujours garantie.

Un travail important est en cours en matière de planification des nouvelles spécifications des cartes d'identité électroniques, en vue de créer une interopérabilité transfrontalière entre les caractéristiques et de standardiser les caractéristiques des cartes d'identité électroniques. Il est important pour la création de ces spécifications et pour l'examen des aspects plus généraux de l'interopérabilité que les fonctions identifiées dans ce document soient bien prises en considération et intégrées «dès la conception».

6. Terminologie et abréviations

Abréviation	
EAC	*Extended Access Control* (Contrôle d'accès étendu)
ECC	Carte d'identité européenne (*European Citizen Card*)
EEE	Espace économique européen
eID	Identité électronique (*Electronic Identity*)
MRZ	Zone de lecture optique (*Machine Readable Zone*)
PACE	*Password Authentication Connection Establishment*
PET	Technologie de protection de la vie privée (*Privacy Enhancing Technology*)
UID	Identifiant unique (*Unique Identifier*)

7. Références et spécifications des cartes d'identité électroniques

Autriche

[1] *Autriche*, La carte d'identité électronique autrichienne «Bürgerkarte», http://www.buergerkarte.at/ (comprend les spécifications de la Bürgerkarte)
[2] *Autriche*, Which data is saved on the citizen card? (*Quelles données sont sauvegardées sur la carte du citoyen?*), http://www.buergerkarte.at/en/datenschutz-sicherheit/index.html
[3] *Autriche*, Bildung von Stammzahl und bereichsspezifischen Personenkennzeichen (bPK), Öffentlicher Entwurf vom 3.6.2004
[4] *Autriche*, Spezifikation MOA ID 2007-08-02

Belgique

[5] *Belgique*, La carte d'identité électronique belge, http://eid.belgium.be/ (comprend les spécifications de la carte d'identité électronique belge)

Estonie

[6] *Estonie*, EstEID, La carte d'identité électronique estonienne, http://www.id.ee/ (comprend les spécifications de l'EstEID)

Finlande

[7] *Finlande*, FINEID, La carte d'identité électronique finlandaise, http://www.fineid.fi/ (comprend les spécifications de la FINEID)

Allemagne

[8] *Allemagne*, Office fédéral pour la sécurité de l'information (BSI): Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11 (pour les passeports électroniques), http://www.bsi.bund.de/literat/tr/tr03110/TR-03110_v111.pdf
[9] *Allemagne*, Office fédéral pour la sécurité de l'information (BSI): Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC) and Password Authentication Connection Establishment (PACE), and Restricted Authentication, Version 2.0, (pour les cartes d'identité nationales), http://www.bsi.bund.de/english/publications/techguidelines/tr03110/TR-03110_v200.pdf
[10] *Allemagne*, ministère fédéral de l'intérieur (BMI): Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept, version 2.0, http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Themen/PaesseUndAusweise/Grobkonzept__Personalausweis,templateId=raw,property=publicationFile.pdf/Grobkonzept_Personalausweis.pdf

Italie

[11] *Italie*, Carta di Identità Elettronica (C.I.E), La carte d'identité électronique italienne, http://www.halnet.it/cie/ (comprend les spécifications de la C.I.E.)
[12] *Italie*, Carta di Identità Elettronica (C.I.E), système de fichiers, v.2.0.2

Pays-Bas

[13] *Pays-Bas,* Documents parlementaires, TK 2005-2006 25764 n° 30, http://www.overheid.nl/op/

Pologne

[14] *Pologne*, Powszechny Elektroniczny System Ewidencji Ludności, http://pesel2.mswia.gov.pl/

Portugal

[15] *Portugal*, La carte d'identité électronique portugaise, http://www.cartaodecidadao.pt/ (comprend les spécifications de la Cartão de Cidadão)

Espagne

[16] *Espagne*, La carte d'identité électronique espagnole, http://www.dnielectronico.es/

Suède

[17] *Suède*, Fakta om nationellt id-kort, http://www.polisen.se/inter/nodeid=33378&pageversion=1.jsp
[18] *Suède*, Cartes d'identification – carte d'identité électronique, profil suédois, Svensk Standard SS-61 43 32, Utgåva 3
[19] *Suède*, Cartes d'identification – certificat électronique d'identité, Svensk Standard SS-61 43 31, Utgåva 2

Royaume-Uni

[20] *Royaume-Uni,* Home Office, National Identity Scheme, Delivery Plan 2008
[21] *Royaume-Uni,* Home Office, ID Cards (*cartes d'identité*), http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/

Union européenne

[22] *Union européenne,* Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:FR:PDF
[23] *Union européenne*, Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML*
[24] *Union européenne,* Décision de la Commission C(2006)2909 du 28 juin 2006 établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_fr.pdf

[25] *Union européenne,* Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur, http://ec.europa.eu/internal_market/services/services-dir/proposal_fr.htm

Autres

[26] Groupe de travail «article 29» sur la protection des données: avis 4/2007 sur le concept de données à caractère personnel, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_fr.pdf
[27] BBC News, Foreign national ID card unveiled, 25 septembre 2008, http://news.bbc.co.uk/2/hi/uk_news/politics/7634111.stm
[28] Brands, Stefan; Demuynck, Liesje; de Decker, Bart: A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users, http://www.springerlink.com/content/e70m608878k11124/fulltext.pdf
[29] CEN: TC 224/WG 15 – European Citizen Card, Part 1-4, Technical Specification
[30] CEN: TC 224/WG 16 – Application Interface for Smart Cards Used as Secure Signature Creation Devices
[31] Credentica: U-Prove SDK, http://www.credentica.com/u-prove_sdk.html
[32] ENISA Position Paper: Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID), novembre 2008, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_mobile_eid.pdf
[33] epractice.eu: fiche factuelle sur l'administration en ligne – Slovénie – infrastructure nationale, http://www.epractice.eu/document/3476
[34] Eurosmart: RFID technology security concerns: Understanding Secure Contactless device versus RFID tag, octobre 2007
[35] Office fédéral allemand pour la sécurité de l'information (BSI): Messung der Abstrahleigenschaften von RFID-Systemen (MARS), Projektdokument 1: Teilbericht zu den Möglichkeiten des passiven Mitlesens einer RFID-Kommunikation, http://www.bsi.de/fachthem/rfid/Mars_Teilbericht_1Therorie.pdf
[36] IBM Zürich: Idemix – Pseudonymity for E-Transactions, http://www.zurich.ibm.com/security/idemix/
[37] OACI: Machine Readable Documents, Doc 9303 and Technial Reports, Machine Readable Travel Documents (*Documents lisibles par machine, doc 9303 et rapports techniques, documents de voyage lisibles par machine*), http://mrtd.icao.int/
[38] IDABC: eID Interoperability for PEGS, Country Profiles, http://ec.europa.eu/idabc/en/document/6484/5644
[39] Microsoft, Credentica, http://www.credentica.com/
[40] Modinis IDM, https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome
[41]J uels, Ari; Molnar, David; Wagner, David: Security and Privacy Issues in E-Passports
[42] Mayáš, Václav; Ríha, Zdenek, Švénda, Petr: Security of Electronic Passports, UPENET, UPGRADE European NETwork, Upgrade vol. VIII, n° 6, décembre 2007, http://www.upgrade-cepis.com/issues/2007/6/upg8-6Upenet.pdf
[43] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, ISBN: 0-8493-8523-7
[44] Naumann, Ingo; Hogben, Giles: Privacy Features of European eID Card Specifications, Elsevier Network Security Newsletter, août 2008, ISSN 1353-48-58, pp. 9-13, http://www.enisa.europa.eu/doc/pdf/publications/privacy_features_of_eid_cards.pdf
[45] Pfitzmann, Andreas; Hansen, Marit: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, version v0.31, 2008, http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[46] Rankl, Wolfgang; Effing, Wolfgang: Handbuch der Chipkarten, Carl Hanser Verlag, ISBN: 3-446-22036-4; traduction anglaise: Smard Card Handbook, John Wiley & Sons, ISBN: 0-470-85668-8
[47] Richter, Henning; Mostowski, Wojciech; Poll, Erik: Fingerprinting Passports, NLUUG 2008 Spring Conference on Security, pp. 21-30, 2008, http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf
[48] STORK: Secure Identity Across Borders Linked, http://www.eid-stork.eu/
[49] Vasconcelos, André: Cartão de Cidadão, Apresentação Técnica, présentation donnée lors de la conférence Agora 2006 du 25 octobre 2006
[50] Wikipedia, ID Card, http://en.wikipedia.org/wiki/Id_card, page consultée le 14 août 2008
[51] Wikipedia, List of Identity Card Policies by Country, http://en.wikipedia.org/wiki/List_of_identity_card_policies_by_country, page consultée le 18 août 2008
[52] Wikipedia, Van-Eck phreaking, http://en.wikipedia.org/wiki/Van_Eck_Phreaking, page consultée le 21 janvier 2009
[53] Communication par courrier électronique avec la police espagnole (Cuerpo Nacional de Policia), 15 avril 2008