Vers une carte d'identité préservant la vie privée

Sébastien Gambs

sgambs@irisa.fr

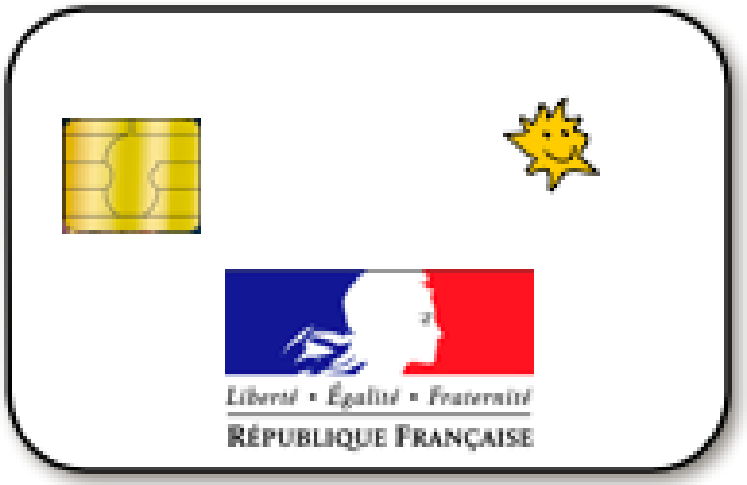
(travail conjoint avec Yves Deswarte, LAAS-CNRS)

6 février 2014

Introduction

Carte d'identité préservant la vie privée

Carte d'identité préservant la vie privée : dispositif personnel qui permet à son utilisateur de prouver des propriétés liées à son identité tout en minimisant la divulgation d'information personnelle.



Quelques utilisations usuelles d'une carte d'identité

- Prouver sa nationalité lorsqu'on passe la frontière.
  Exemple : lorsqu'on rentre en France (ou dans un pays de l'espace Schengen).
- Prouver qu'on se situe dans une certaine tranche d'âge.
  Exemple : Alice doit démontrer qu'elle a moins de 18 ans pour obtenir la réduction correspondante au cinéma.
- Prouver qu'on a le droit d'accéder à une certaine ressource.
  Exemple : je dois prouver que j'habite sur Rennes pour pouvoir emprunter un livre à la bibliothèque municipale.
- Vérifier une identité ou la non-présence sur une liste sensible.
  Exemple : lorsque je monte dans l'avion, on doit s'assurer que mon identité est bien celle de la personne marquée sur la carte d'embarquement et que je ne suis pas inscrit sur une liste de personnes recherchées.

Risques des cartes physiques actuelles

Sécurité insuffisante :

- Vol de carte ⇒ risque d'usurpation d'identité.
  - Facile à réaliser si la photo est plus ou moins ressemblante.
- Fabrication de faux (copie identique ou non).

Intrusion dans la vie privée :

- Toutes les informations sont lisibles,
- quelque soit l'utilisation qui est faite de la carte
- ou la personne qui consulte ces données.

Cartes d'identité électroniques

Meilleure sécurité (puce sécurisée) . . .

- Falsification plus difficile.
- Usurpation d'identité plus difficile si on utilise l'authentification biométrique.

mais toujours intrusive pour la vie privée :

- Les informations d'identité sont toujours lisibles et peuvent être facilement enregistrées.
- Risque d'abus ⇒ traçage généralisé, croisement d'information.
- Exemples : e-administration, e-commerce, . . .

Ce qui est arrivé au projet de carte d'identité au Royaume-Uni . . .

Home Office
Identity & Passport Service

Sitemap Accessibility SEARCH

REGISTRARS LOGIN

About us | Publications | Business Services | News | Careers | Contact us

Media

Announcements

Identity cards and National Identity Register to be scrapped

27 May 2010

The government plans for identity cards for British citizens to be scrapped within 100 days, it was announced today.

The National Identity Register, the database which contains the biographic and biometric fingerprint data of card holders, would also be destroyed by the first piece of legislation introduced to Parliament by the coalition government.

Home Secretary Theresa May said:

"This bill is a first step of many that this government is taking to reduce the control of the state over decent, law-abiding people and hand power back to them.

"With swift Parliamentary approval, we aim to consign identity cards and the intrusive ID card scheme to history within 100 days."

Deputy Prime Minister Nick Clegg said:

"The wasteful, bureaucratic and intrusive ID card scheme represents everything that has been wrong with government in recent years.

"By taking swift action to scrap it, we are making it clear that this government won't sacrifice people's liberty for the sake of Ministers' pet projects.

Le cas de la base de données des citoyens en Israël

Le fichier de la population israélienne, comprenant les données personnelles de plus de 9 millions d'Israéliens morts ou vivants, a été disponible sur le Net de 2009 à octobre 2011. Au menu : nom, prénoms, date et lieu de naissance (et, au besoin, de décès ou d'immigration en Israël), âge, sexe, adresse, n° de téléphone, statut marital, noms et prénoms des parents et enfants.

Un employé du ministère des affaires sociales l'avait copié sur son ordinateur personnel en 2006, puis confié à un ami, qui le vendit à un professionnel du commerce des fichiers clients, qui demanda à un informaticien d'en développer un logiciel. Ce dernier, Agron 2006, qui permettait de cartographier les liens familiaux des Israéliens, fut mis à la vente, par téléchargement, sur un site web par un autre informaticien, puis rendu disponible sur les réseaux P2P.

L'information a été révélée, la semaine dernière, par l'Israël Law, Information and Technology Authority (ILITA), l'autorité de protection des données personnelles israéliennes, dont l'enquête a conduit à l'arrestation de six suspects, dont le voleur présumé, Shalom Bilik, ainsi que Meir Leiver, le responsable du site qui expliquait comment se procurer la base de données, et utiliser le logiciel.

L'ILITA, qui a récupéré 6 terabytes (6 000 Gigabytes) de données, et qui a découvert à cette occasion que d'autres fichiers avaient eux aussi été volés, dont une base de données d'enfants adoptés, des données issus des fichiers électoraux, et des données relatives à la sécurité nationale a également mis en ligne deux étonnantes vidéos afin d'expliquer ce qui s'est passé :

Le ministre de la Justice s'est inquiété des risques de fraudes et d'usurpation d'identité qui pourraient en découler. Michael Eitan, ministre de l'amélioration des services publics, a quant à lui appelé dans la foulée le gouvernement à abandonner son projet de création d'une base de données biométriques des Israéliens :

Vers une carte d'identité électronique en France (été 2011)

. . .

La future carte d'identité, débattue au Parlement ce 6 7 juillet, reposera sur la création d'un "*fichier des gens honnêtes*" (sic) répertoriant les noms, prénoms, sexe, dates et lieux de naissance, adresses, tailles et couleurs des yeux, empreintes digitales et photographies de 45 millions de Français voire, à terme, de l'ensemble de la population.

L'expression "*fichier des gens honnêtes*" a été utilisée par François Pillet, sénateur (UMP) du Cher et rapporteur de la proposition de loi sur la protection de l'identité (voir le dossier), adoptée en première lecture au Sénat, et qui sera discutée à l'Assemblée le 6 juillet:

> Pour atteindre l'objectif du texte, il faut une base centralisant les données. Or cette base serait unique dans l'histoire de notre pays au regard de sa taille, puisqu'elle porterait sur 45 millions d'individus, si elle existait à l'heure actuelle. À terme, elle est susceptible de concerner 60 millions de Français. Ce sera de surcroît le premier « fichier des gens honnêtes ».
>
> Ce fichier n'a donc pas d'équivalent. Toutes les personnes auditionnées ont mis en garde, plus ou moins expressément, contre son usage à d'autres fins que la lutte contre l'usurpation d'identité, ce qui présenterait des risques pour les libertés publiques.

Le gouvernement cherche depuis 10 ans à moderniser la carte d'identité, afin d'y rajouter une "*puce électronique sécurisée*", et de centraliser dans une base de données les identifiants, notamment biométriques, des personnes fichées. Ce qui pose de nombreux problèmes techniques, juridiques et politiques. Au point, comme le reconnait François Pillet, qu'"*aucun des*

Vers une carte d'identité électronique en France (novembre 2012) . . .

SÉNAT

UN SITE AU SERVICE DES CITOYENS

Travaux parlementaires | Vos sénateurs | Europe & International | Territoires | Connaître le Sénat

21 novembre 2012 Accessibilité | Plan du site | Alertes Recherche OK

Base Questions > 2012

Carte nationale d'identité sécurisée

14 ème législature

Question écrite n° 01486 de M. Pierre Bernard-Reymond (Hautes-Alpes - NI)

publiée dans le JO Sénat du 09/08/2012 - page 1801

M. Pierre Bernard-Reymond demande à M. le ministre de l'intérieur de bien vouloir lui indiquer l'état d'avancement de la mise au point et de la mise en service de la carte nationale d'identité sécurisée.

Réponse du Ministère de l'intérieur

publiée dans le JO Sénat du 15/11/2012 - page 2608

La proposition de loi relative à la protection de l'identité, qui porte au plan juridique la carte nationale d'identité électronique (CNIe), a été adoptée en dernière lecture par l'Assemblée nationale le 6 mars 2012. La loi a été promulguée le 28 mars 2012. Le Conseil constitutionnel a censuré la création d'un traitement de données à caractère personnel (base centrale) et l'accès à cette base des agents de police et de gendarmerie. Il n'autorise pas non plus que la nouvelle carte contienne des données permettant de mettre en œuvre la signature électronique de son titulaire comme outil de transaction commerciale. Seule est autorisée une carte nationale d'identité électronique comportant un seul composant électronique sécurisé contenant l'état civil du titulaire avec la photographie et les empreintes digitales. Compte tenu des décisions prises par le Conseil constitutionnel, et conformément à la loi du 27 mars 2012 relative à la protection de l'identité, deux solutions sont envisageables pour la carte nationale d'identité : soit la production d'un document comportant une puce électronique (CNIe) avec les limites apportées par la loi à l'usage de cette puce. Le coût de ce projet est estimé en année pleine à 85 M€. Soit le dépôt d'un projet de loi sur une nouvelle base législative à reconstruire, permettant de relancer le projet de la CNIe. À ce stade, il apparait prématuré de décider du lancement de cette CNIe.

Vers une carte d'identité électronique en France (janvier 2013) . . .

Manuel Valls a-t-il enterré la carte d'identité électronique ?

Par Steven Belfils
Publié le 09/01/2013 à 06:45
1 réaction

A+ A-

L'avenir de la carte d'identité électronique est plus que jamais incertain. Dans une réponse adressée au député du Rhône Philippe Meunier, le ministère de l'Intérieur juge en effet que son lancement *"n'est pas souhaitable"*. En cause un coût de 85 millions d'euros par an *"trop élevé"* pour une carte d'identité privée de la plupart de ces dispositifs phares, censurés par le Conseil constitutionnel.

©Thomas Padilla

Manuel Valls va-t-il tuer la carte d'identité électronique dans l'oeuf ? Son lancement n'est en tout cas *"pas souhaitable"*, explique le ministère de l'Intérieur dans une réponse écrite faite à Philippe Meunier, député UMP du Rhône qui l'interrogeait sur le calendrier de

Desiderata pour une carte d'identité préservant la vie privée

Caractéristiques de la carte

- Émise par une autorité de certification (CA).
- Contient des informations personnelles d'état-civil, plus des preuves de droits et les références biométriques.
- Stocke ces données sur une puce supposée résistante aux attaques logicielles et matérielles.
- Carte à contact (consentement explicite du possesseur, pas de risque d'écumage RFID).
- Principes fondamentaux de la carte :
  - Les informations stockées ne quittent jamais la puce.
  - Une question est transmise à la carte (qui est fonction de l'habilitation du lecteur), la réponse est binaire (oui ou non).

Fonctionnement de la carte

Résumé du fonctionnement de la carte :

1. Authentification mutuelle entre la carte et le lecteur (certifié).
2. Vérification biométrique de l'utilisateur par un capteur situé sur la carte ou le lecteur.
   - Références biométriques maintenues dans la puce.
3. Protocole de type question-réponse.

Exemples de questions posées à la carte

- Preuve de nationalité :
  Réponse = OUI (dès la vérification biométrique)
- Vérification d'identité (ex. carte d'embarquement, chèque) :
  Question : Nom et prénom = Martin, Jacques ?
  Réponse : OUI ou NON
- Vérification de domicile : municipalité, région, état, ...
  (ex. accès à la bibliothèque ou la déchetterie)
  Question : Ville du domicile = Rennes ?
  Réponse : OUI ou NON
- Vérification de majorité, carte vermeil, ...
  Question : aujourd'hui = 6 février 2014 ; âge $\leq$ 18 ?
  Réponse : OUI ou NON

Remarque : une question plus complexe peut-être construite à partir d'une composition de ET, OU et NON sur les attributs.

Propriétés souhaitées

Divulgation d'information limitée :

- Minimisation de la quantité d'information personnelle révélée.
- Idéalement : seulement 1 bit d'information prouvant une propriété binaire liée au possesseur de la carte.

Non-chaînabilité :

- Impossibilité de relier les différentes actions réalisées par la même carte.
- Même si l'utilisateur prouve 2 fois la même propriété.

Exactitude :

- L'utilisateur ne devrait pas pouvoir prouver des propriétés invalides par rapport à son identité (*"soundness"*).
- Un vérificateur (lecteur) honnête devrait toujours accepter une propriété valide concernant l'utilisateur pourvu que celui-ci possède l'accréditation correspondante (*"completeness"*).

Propriétés souhaitées (suite)

Non-transférabilité :

- Seul l'utilisateur légitime de la carte doit pouvoir l'utiliser.
- Permet d'eviter le risque d'usurpation d'identité dans le cas de vol ou perte de la carte.

Authenticité et non-contrefaçon :

- Impossibilité de cloner une carte existante ou de fabriquer un fausse carte qui correspondrait à une identité choisie.
- Impossibilité d'usurper le rôle d'une carte valide ou d'un lecteur valide.

Propriétés additionnelles

Anonymat révocable :

- L'utilisateur de la carte est anonyme en tout temps sauf . . .
- dans des situations extrêmes où il devient nécessaire de lever son anonymat.
- Exemple : un meutre a été commis dans une pièce dont l'accès se fait en utilisant la carte d'identité.
- Collaboration explicite nécessaire entre l'autorité de certification et le vérificateur pour lever l'anonymat (par exemple suite à une demande d'un juge).

Transparence et consentement explicite :

- La carte surveille les questions qui lui sont posées et les affiche à l'utilisateur.
- Pour certaines questions vraiment critiques, une confirmation explicite de l'utilisateur pourrait être requise.

Implémentations proposées

La technologie existe déjà . . .

Initialisation de la carte

- L'utilisateur dépose une demande auprès de l'autorité de certification (CA) qui :
  1. vérifie ses informations personnelles,
  2. scanne son profil biométrique b et
  3. émet la carte d'identité correspondante.
- Contenu de la carte (sur une puce supposée "inviolable") :
  - Les k attributs personnels de l'utilisateur, $a_1, \ldots, a_k$,
  - la clé privée de signature de groupe SKG_U,
  - les informations biométriques nécessaires pour l'authentification, soit z $(= c \oplus b)$ et $h(c)$, pour c un mot de code choisi au hasard,
  - la clé publique de vérification de signature pour l'autorité de certification VK_{CA} (nécessaire pour que la carte puisse vérifier l'accréditation d'un lecteur).

Enregistrement d'un lecteur

À l'enregistrement :

- Le lecteur reçoit une accréditation cr de la forme : "*Ce lecteur est autorisé à poser la question f à une carte d'identité. La réponse à cette question doit être chiffré en utilisant la clé publique de chifferement* EK_R." ainsi que la signature du CA sur cette accréditation, $\sigma_{CA}(cr)$.
- La clé publique de chiffrement EK_R est supposée être spécifique au lecteur (peut-être vu comme son identifiant).
- Le lecteur garde secrète la clé de déchiffrement correspondante DK_R sur une puce considérée "inviolable".
- Il connaît aussi la clé publique de vérification du groupe VKG.

Authentification mutuelle (round 1)

Premier round (carte $\rightarrow$ lecteur) :

- La carte génère dynamiquement une paire de clés chiffrement/déchiffrement pour la session (EK_{temp}, DK_{temp}).
- La carte envoie la clé de chiffrement EK_{temp} ainsi qu'une signature de groupe sur cette clé $\sigma_{G,U}(EK_{temp})$.
- Le lecteur vérifie si cette signature est valide en utilisant la clé publique de vérification du groupe VKG.
- Si c'est le cas, le lecteur passe au deuxième round, sinon il avorte le protocole.

But principal du round : permettre au lecteur de s'assurer de l'authenticité de la carte sans que celle-ci divulgue explicitement son identité.

Authentification mutuelle (round 2)

Deuxième round (lecteur $\rightarrow$ carte):

- Le lecteur utilise la clé publique de la session EK_{temp} pour chiffrer son accréditation cr, la signature du CA sur cette accréditation $\sigma_{CA}(cr)$ ainsi qu'une chaîne aléatoire de bits r et envoie le message chiffré résultant à la carte.
- La carte déchiffre le message avec la clé secrète de session DK_{temp} et vérifie si l'accréditation et la signature de l'accréditation faite par le CA $\sigma_{CA}(cr)$ sont valides (en utilisant la clé publique de vérification VK_{CA}).
- Si c'est le cas, la carte passe au troisième round, sinon elle avorte le protocole.

Remarque : la carte devrait avoir un mécanisme pour limiter le nombre d'essais que peut faire le lecteur (par exemple 3 essais maximum par minute).

Authentification mutuelle (round 3)

Troisième round (carte $\rightarrow$ lecteur):

- La carte calcule une signature de groupe sur le challenge r envoyé par le lecteur, soit $\sigma_{G,U}(r)$.
- La carte chiffre cette signature en utilisant la clé publique du lecteur EK_R (qui était inscrite sur l'accréditation cr du lecteur) puis envoie le chiffré correspondant à la carte.
- Le lecteur déchiffre et vérifie la validité de la signature de groupe $\sigma_{G,U}(r)$ sur le challenge aléatoire.
- Si la signature est valide, le lecteur reconnaît la carte comme étant une carte véridique, sinon il avorte le protocole.

Anonymat révocable : le lecteur peut stocker toutes les paires $(r, \sigma_{G,U}(r))$ qu'il a vu avec les étiquettes temporelles correspondantes.

Vérification biométrique et protocole de question-réponse

Vérification biométrique :

- Fait "à la fuzzy commitment".

Protocole de question-réponse :

- Soit $f(a_i)$, la réponse à la question booléenne f portant sur l'attribut a_i (ou une combinaison d'attributs).
- La carte concatène $f(a_i)$ avec la chaîne aléatoire r obtenue durant l'authentification et signe le tout avec la clé privée du groupe pour obtenir $\sigma_{G,U}(f(a_i)||r)$
- La carte envoie le message $f(a_i)||r||\sigma_{G,U}(f(a_i)||r)$ au lecteur chiffré avec la clé EK_R qui vérifie la validité de la signature.
- Protège contre le rejeu et le détournement de session.
- Contrainte additionnelle : le cryptosystème utilisé doit être *sémantiquement sûr* et *non-malléable*.

Instanciation possible des primitives cryptographiques

Algorithme de chiffrement :

- Nécessite un cryptosystème sémantiquement sûr et non-malléable.
- Exemple de protocole : Cramer-Shoup 98.

Algorithme de signature de groupe (avec anonymat révocable) :

- Exemple de protocole : Camenisch et Lysyanskaya (2002).

Algorithme de signature "normal" :

- À priori n'importe quel algorithme de signature standard peut être utilisé (ex. DSA ou ECDSA).

Analyse de l'implémentation par rapport au desiderata

Divulgation d'information limitée :

- Les données personnelles sont stockées sur une puce sécurisée.
- La carte divulgue un seul bit d'information à chaque question qui lui est posée.

Non-chaînabilité :

- Assuré par l'utilisation d'une signature de groupe.
- Aucune utilisation de pseudonyme ou d'identifiant dans l'implémentation.

Exactitude :

- La puce étant considérée comme inviolable, elle est supposée répondre toujours honnêtement à une question posée.
- La non-mallabilité du cryptosystème interdit à un adversaire de flipper un bit de réponse.
- De plus, le bit de réponse est signé avec la clé de la carte.

Analyse de l’implémentation (suite)

Non-transférabilité :

- Vérification biométrique de l’utilisateur avant utilisation de la carte.

Authenticité et non-contrefaçon :

- Le lecteur doit prouvé son authenticité et son droit à poser une question en montrant une accréditation valide signé par le CA.
- La carte prouve qu’elle fait partie de l’ensemble des cartes valides en signant un challenge aléatoire de la part de ce groupe.
- La non-contrefaçon est assurée par l’aspect “inviolable” de la carte et du lecteur qui empêchent un attaquant d’apprendre les informations stockées dans la carte et le lecteur.

Implémentation avancée

Spécificités de la nouvelle implémentation

- Idée principale : lever l'hypothèse sur l'inviolabilité de la puce en utilisant un extracteur flou.
- La chaîne d'aide p nécessaire pour générer la chaîne aléatoire *rand* est stocké en clair dans la puce (ou même en dehors de celle-ci)
- Contenu de la carte (chiffré en utilisant une clé dérivée à partir de *rand*):
  - Les k attributs personnels de l'utilisateur, $a_1, \ldots, a_k$,
  - la signature du CA sur ces attributs $\sigma_{CA}(a_1), \ldots, \sigma_C A a_k$,
  - la clé privée de signature de groupe SKG_U,
  - la clé publique de vérification de signature pour l'autorité de certification VK_{CA} (nécessaire pour que la carte puisse vérifier l'accréditation d'un lecteur).
- L'authentification mutuelle se déroule de la même manière que dans l'implémentation "basique".

Protocole de mise en gage

- Phase de mise en gage : prend en entrée une valeur a ainsi que de l'information auxiliaire aux (généralement une chaîne aléatoire) et produit en sortie une mise en gage $comm(a)$ de cette valeur.
- Phase d'ouverture : prend en entrée une mise en gage $comm(a)$ et une information auxiliaire aux et révèle en sortie la valeur mise en gage a.

Propriétés attendues:

- Liant ("*binding*"): il existe une seule valeur possible a pour une mise en gage $comm(a)$ (l'adversaire ne peut pas ouvrir une mise en gage en choisissant parmi plusieurs valeurs).
- Camouflant : l'adversaire ne peut pas apprendre de l'information sur a à partir de sa mise en gage $comm(a)$.

Preuve d'identité relié à un attribut

- Soit a_i le ième attribut d'un utilisateur et $\sigma_{CA}(a_i)$ la signature de l'autorité de certification sur cet attribut.
- Pour prouver une propriété liée à cet attribut, l'utilisateur commence par se mettre en gage sur une valeur $comm(a_i) \leftarrow \text{Commit}(a_i, aux)$.
- L'utilisateur calcule ensuite $\pi \leftarrow \text{Prove}((a_i, \sigma_{CA}(a_i), aux) | \text{VerifySign}(a_i, \sigma_{CA}(a_i), VK_{CA}) = \text{accept} \wedge a_i = \text{Open}(comm(a_i), aux) \wedge f(a_i) = true)$, où VK_{CA} est la clé publique de vérification de l'autorité de certification qui peut être utilisée pour vérifier sa signature, $\sigma(a_i)$ la signature de l'autorité de certification sur cet attribut a_i et $f(a_i)$ une question booléenne en rapport avec a_i.

Preuve d'identité relié à un attribut (suite)

- π est une preuve non-interactive à divulgation nulle de l'énoncé suivant "L'utilisateur sait comment ouvrir la valeur commise *comm* à une certaine valeur a_i, et cette valeur a été signée par l'autorité de certification, et quand la fonction booléenne f est calculée sur a_i elle retourne vraie" ...
- qui peut être résumée par "L'autorité de certification atteste que l'utilisateur actuel satisfait la question booléenne f quand elle est appliqué sur son ième attribut i^{th}".

Algorithme de preuve à divulgation nulle non-interactive :

- Exemple de protocole : Belenkiy, Chase, Kohlweiss et Lysyanskaya (2008).

Algorithme de mise en gage :

- Exemple de protocole : Groth-Sahai (2008), possède des propriétés de *randomisation* et *f-extraction*.

Analyse de l'implémentation par rapport au desiderata

Divulgation d'information limitée :

- Les données personnelles sont stockées de manière chiffrée et ne peuvent être décryptés que par un utilisateur présentant le profil biométrique correspondant (dû aux extracteurs flous).
- Utilisation de preuve de connaissance à divulgation nulle.

Non-chaînabilité :

- Assuré par l'utilisation d'une signature de groupe et des preuves de connaissance à divulgation nulle *randomisables*.

Exactitude :

- Découle directement des propriétés de consistance et solidité des preuves à divulgation nulle.
- La non-mallabilité du cryptosystème interdit à un adversaire de flipper un bit de réponse.

Analyse de l’implémentation (suite)

Non-transférabilité :

- Vérification biométrique de l’utilisateur avant utilisation de la carte.

Authenticité et non-contrefaçon :

- Le lecteur doit prouvé son authenticité et son droit à poser une question en montrant une accréditation valide signé par le CA.
- La carte prouve qu’elle fait partie de l’ensemble des cartes valides en signant un challenge aléatoire de la part de ce groupe ainsi qu’en réussissant la preuve de connaissance à divulgation nulle.
- La non-contrefaçon est assurée par l’utilisation d’extracteurs flous.

Prototype expérimental (réalisé par Moussa Traoré)

Equipement utilisé :

- Lecteur d'empreintes : lecteur MORPHO MSO-350.
- Carte à puce :
  - Compatible ISO-7816.
  - Java Card Development Kit 2.1.
- JDK 1.6
- Netbeans 7.0

Prototype expérimental (suite)

- Signature de groupe utilisé :
  - Schéma proposé par Canard et Girault.
  - Particulièrement adapté pour les appareils avec ressources limitées (faible puissance de calcul, faible RAM, ...) tels que les cartes à puce.
- Authentification biométrique :
  - Se base sur les empreintes biométriques.
  - Algorithme fournit par MORPHO, se basant sur un algorithme initialement proposé par Batha *et al.*
  - Nécessite beaucoup de ressources lors de la phase d'assimilation $\Rightarrow$ plus d'un 1 Mo de mémoire EEPROM (trop pour notre carte à puce)
  - Version actuelle : matching réalisé par le terminal connecté au lecteur.

Prototype expérimental (résultats)

Points forts :

- Programme de petite taille.
- Temps d'exécution acceptable.
- Architecture simple d'utilisation et de déploiement.

Point faible :

- Authentification biométrique actuellement effectuée à l'extérieur de la carte.

Extensions possibles et conclusion

Extension 1

Extension : intégration du capteur biométrique et de l'écran (plus éventuellement un clavier) à la carte.

Avantages :

- Meilleure confiance dans la carte (pas besoin de supposer l'existence d'un capteur externe sécurisé).
- Peut afficher les questions posées à la carte et permettre le suivi de celle-ci et des usages de la carte.
- Interactivité possible avec l'utilisateur si l'interface le permet (par exemple pour lui demander son consentement).

Extension 2

Extension : preuve d'identité à distance.

Applications possibles :

- e-administration : déclaration de revenus, impression de document officiel, ...
- e-commerce,
- e-vote,
- ...

Potentiels risques de sécurité :

- Limite de la biométrie sans surveillance.
- Hameçonnage (*"phishing"*) avec un lecteur volé.

Extension 3

Extension : intégration de la carte d'identité dans un smartphone.

Avantages :

- Connexion sans fil (NFC, Bluetooth, WiFi, 3G).
- Biométrie : capteurs intégrés (voix, iris).
- Plus de possibilités du côté utilisateur (ex. écran, audit log).

Potentiels risques de sécurité :

- Confiance dans le smartphone (virus)?
- Plus de risque de traçage (IMEI, MAC@, . . .).
- Utilisation à l'insu du propriétaire par écumage (*"skimming"*).

Conclusion

- La carte d'identité préservant la vie privée est conçue pour divulguer le minimum d'information nécessaire concernant son propriétaire (soit 1 bit).
- Contrairement au carte actuelle, elle ne peut être utilisée que par son propriétaire :
  - peu de risque de vol.
  - pas de besoin de révocation en cas de perte.
  - sauvegarde/recréation facile.
- La technologie nécessaire existe aujourd'hui mais . . .
- reste à voir si les états ont (ou non) la volonté de l'adopter.

C'est la fin !

Merci pour votre attention.
Questions?