Déclaration de Budapest sur les Documents de Voyage à Lecture Automatique (MRTD - Machine Readable Travel Documents)

Résumé

En omettant de mettre en place un concept et un système de sécurité appropriés, les gouvernements européens obligent leurs citoyens à adopter des pièces d'identité – les nouveaux Documents de Voyage à Lecture Automatique (DVLA) – qui diminuent leur sécurité et la protection de leur sphère privée tout en accroissant les risques liés aux vols d'identité. En clair, la version actuelle du passeport européen utilise des technologies et des normes qui n'atteignent pas les objectifs visés. Dans cette déclaration, mise en forme lors d'une rencontre FIDIS à Budapest en septembre 2006, des chercheurs du Réseau d'Excellence [(1)] FIDIS – Futur de l'Identité dans la Société de l'Information – présentent les résultats de leur étude sur les DVLA. Ils font des recommandations aux responsables des gouvernements et de l'industrie au sujet des modifications à adopter.

Introduction

Outre les abus habituels des documents d'identité, les nouveaux Documents de Voyage à Lecture Automatique (DVLA) présentent de nombreuses menaces additionnelles. Nous voulons souligner le fait que :

- A la différence des documents d'identité habituels, les DVLA européens peuvent être lus et interceptés jusqu'à une distance de l0 mètres [(2)] du porteur, de façon transparente et sans contrôle interactif ; cette faiblesse est encore aggravée par un contrôle d'accès susceptible d'être contourné ou attaqué, de sorte qu'un tiers, autorisé ou non, peut y avoir accès pour identifier le porteur et le ficher afin de, par exemple, suivre à la trace les touristes dans un pays étranger.

- Les informations biométriques des documents d'identité peuvent être utilisées à d'autres fins par les secteurs public et privé en violation des

principes européens de respect de la sphère privée. De plus, les données biométriques elles-mêmes sont basées sur des probabilités : des erreurs d'authentification —positives et négatives—sont inévitables ; elles sont susceptibles d'affecter de nombreux citoyens européens chaque jour.

L'introduction du passeport européen DVLA (passeport électronique), en tant que document d'identification international, a débuté en 2005 ; ce passeport est basé sur les normes techniques internationales OACI [3] telles que définies dans le document 9303 [4] selon le règlement EC 2252/2004 [5]. Le présent communiqué est basé sur l'analyse des fondements légaux des DVLA et de la technologie qu'elle implique ainsi que de la mise en œuvre de la protection et de la sécurité des données ; cet objectif a été poursuivi par le Réseau d'Excellence FIDIS et exposé dans le rapport FIDIS D3.6 « Etude des documents d'identification » [6]. Les sources suivantes furent encore prises en considération pour la présente déclaration :

- Les profils de protection des mécanismes de vérification biométrique et des DVLA comprenant le Contrôle d'Accès de Base (BAC – Basic Access Control) [7] certifié par l'Office fédéral allemand pour la sécurité de l'information.
- La directive technique V1.0 concernant le Contrôle d'accès étendu (EAC – Extended Access Control) édicté par l'Office fédéral allemand pour la sécurité de l'information (BSI) en août 2006 [8].

Résumé des résultats obtenus

Aucun concept de sécurité, cohérent et intégré, concernant les DVLA a été présenté au public ou aux experts concernés. Les documents publiés tels que les Profils de protection ou les Directives techniques ne couvrent qu'une partie d'un tel concept de sécurité [(9)]. A l'origine, le BAC a été présenté comme une solution efficace au contrôle d'accès ; actuellement, l'EAC est présenté comme une solution améliorée. En fait, tous deux sont insuffisants dans de nombreuses situations comme contrôle d'accès pour l'utilisateur [(10)]. Un certain nombre de menaces théoriques démontrées scientifiquement et de faiblesses conceptuelles des DVLA ont déjà été publiées. Ces dernières ne sont pas couvertes par les Profils de protection, les directives techniques, les normes ou les réalisations actuelles. Citons entre autres, parmi les plus importantes :

- Etant donné que les données biométriques des DVLA ne peuvent pas être révoquées et que les caractéristiques biométriques de l'utilisateur tels qu'empreintes digitales et traits faciaux ne peuvent être modifiées, des données biométriques « volées » pourront être utilisées abusivement pendant longtemps.
- Gestion insuffisante de la clé d'accès avec le BAC : la clé pour accéder aux données du tag RFID est intégrée dans le passeport lui-même et peut être lue par des personnes et par des scanners. Cela signifie que quiconque ayant eu un accès physique au passeport et en ayant fait une copie optique par exemple, pourrait stocker l'information de la clé et l'utiliser pour avoir accès au tag RFID.
- Ecoute des communications entre le tag RFID et le lecteur, ainsi qu'attaque par force brute du BAC en utilisant des faiblesses cryptographiques reconnues pour extraire des données [(11)].
- Clonage des tags RFID dans les DVLA [(12)].
- Abus de lecture à distance des tags RFID des passeports pour faire éclater des bombes intelligentes, sensibles à l'identité de certaines personnes

La combinaison de ces menaces et de ces faiblesses met sérieusement en cause la sécurité et la sphère privée des citoyens européens ; ceci est tout particulièrement vrai si l'on considère le déploiement à grande échelle des DVLA actuels et leur longue durée de validité (jusqu'à 10 ans).

Recommandations aux responsables en Europe

Sur la base de nos recherches, nous avons élaboré un certain nombre de recommandations adressées aux responsables du domaine des DVLA en Europe (politiciens, industriels et chercheurs):

1. Etant donné que des DVLA comportant des faiblesses inhérentes ont déjà été introduits et seront inévitablement utilisés à l'avenir, nous recommandons les mesures suivantes pour diminuer les risques d'échec des mesures de sécurité et de vol d'identité, mesures à appliquer immédiatement et sans délai. Ces recommandations comportent des procédures et des technologies fondées sur des scénarios de secours et qui requièrent un développement et des accords au niveau international (p. ex. OACI).

a. Mise en place et contrôle de sa mise en oeuvre du principe de monovalence, spécialement pour les données biométriques des DVLA (le but spécifique poursuivi étant l'identification des voyageurs). L'utilisation des DVLA ne devrait pas être étendue pour l'authentification dans le secteur privé.
b. Les citoyens doivent être informés des risques inhérents à la possession des nouveaux DVLA et des mesures de sécurité qu'ils peuvent prendre, par exemple éviter de remettre les documents à des privés (des hôtels par exemple).
c. Des mesures de sécurité disponibles mais non utilisées aujourd'hui devraient être immédiatement intégrées dans les DVLA actuels par les Etats européens, par exemple les cages de Faraday.
d. Des procédures organisationnelles adéquates doivent être prévues en cas d'échec d'authentification biométrique dû à des problèmes non résolus tels que des rejets erronés ou des erreurs d'enregistrement, etc.
e. Des procédures adéquates sont requises –aussi bien organisationnelles que techniques– pour prévenir l'utilisation abusive des données personnelles contenues dans les DVLA.
f. Il faut établir des procédures techniques et administratives adéquates à appliquer en cas de vol d'identité impliquant les DVLA.

2. Dans le moyen terme (trois prochaines années), un nouveau concept de sécurité, intégré et convaincant, doit être élaboré pour les DVLA. Ce dernier devra tenir compte des aspects suivants :

a. Définition des niveaux requis de sécurité.
b. Protection des données personnelles des citoyens européens, y-compris les informations biométriques si elles sont encore utilisées.
c. Sécurité technique et organisationnelle dans l'utilisation des DVLA à l'échelle internationale, étant donné la multiplicité des opérateurs et des pays. Il faut en particulier répondre à la question de savoir comment éviter l'abus d'utilisation des données personnelles par des acteurs dans des Etats étrangers.
d. Risques et menaces provoqués par la combinaison de plusieurs technologies dans les DVLA telles que RFID, données biométriques, etc. et les caractéristiques des documents-papiers traditionnels en terme de sécurité.

e. Une ré-évaluation totale et une nouvelle conception des solutions choisies pour l'actuel DVLA doivent être mises en œuvre –basées sur les niveaux de sécurité définis et l'analyse des risques– tout spécialement concernant la technologie RFID et la biométrie. Ce projet examinera si les technologies actuellement en vigueur sont vraiment indispensables ou si d'autres, à la fois plus sûres et préservant la sphère privée, (par exemple des cartes à puce avec contact au lieu de mécanismes sans contact) sont suffisantes. Il faudra examiner la façon dont l'application des technologies peut être améliorée (par exemple pour la biométrie, senseurs et vérification sur la carte elle-même).
f. Le concept de sécurité entourant les DVLA devrait être débattu ouvertement à l'échelle européenne par les experts en sécurité et en protection de la sphère privée.

3. Les mesures techniques, administratives et organisationnelles élaborées dans ce concept doivent être standardisées (OACI), mises en œuvre dans la prochaine génération de DVLA et évaluées à l'échelle mondiale.

Notes

(1) FIDIS –Future of Identity in the Information Society (Futur de l'Identité dans la Société de l'Information). Voir www.fidis.net

(2) Les puces ISO 14443 du type utilisé dans les DVLA sont conçues de façon à pouvoir fonctionner avec un lecteur approprié dans un rayon de 10 à 15 cm. Cependant, l'interception et l'écoute des communications entre de tels passeports et les lecteurs est possible dans un rayon de 10 mètres (voir Finke, T., Kelter, H., Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems, Bonn 2004.

Télécharger : www.bsi.de/faachthem/rfid/Abh_RFID.pdf). Cette possibilité a été démontrée récemment par Robroch avec un passeport néerlandais (Référence : Robroch, H., ePassport Privacy Attack, 2006, www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf). L'auteur donne également les distances permettant de lire et d'intercepter les informations.

Quelques DVLA sont équipés de protections supplémentaires dans leur couverture ; par exemple, les passeports américains contiendront une toile de fibre métallique insérée dans la couverture. Mahaffey et Hering ont cependant démontré que si un passeport s'ouvre, ne serait-ce que d'un demi-pouce, comme cela peut se produire dans un sac à main ou dans un sac à dos, il peut révéler son contenu à un lecteur à une distance de deux pieds. (Voir www.flexilis.com/epassport.php).

(3) OACI = Organisation de l'Aviation Civile Internationale, http://www.icao.int/fr/index.html
(4) Information disponible via http://www.icao.int/MRTD/Home/Index.cfm
(5) Voir http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/1_385/l_38520041229en00010006.pdf
(6) Disponible sur :www.fidis.net/fidis-del/period-2-20052006/ c961
(7) Profil de protection BSI-PP-0016-2005 et BSI-PP-0017-2005, disponible sur http://www.bsi.de/zertifiz/zert/report.htm
(8) Annoncé sur : http://www.bsi.bund.de/fachthem/epass/eac.htm
(9) Par exemple, les profils de protection sont des directives concernant les mesures de sécurité s'appliquant uniquement à des produits définis dans le contexte des DVLA ; le degré et la qualité de leur mise en œuvre dans les DVLA actuels (genre passeport, p. ex.) ne sont pas explicités dans le texte. Actuellement, la documentation sur la mise en œuvre des profils de protection dans les passeports électroniques actuels n'est pas rendue publique. Les directives techniques actuelles, c'est-à-dire la directive « Extended Access Control » (EAC) –Contrôle d'accès étendu– ne couvre également qu'en partie la question de la sécurité technique.
(10) Le Contrôle d'accès étendu (EAC), par exemple, ne sera appliqué qu'à certaines parties des données personnelles contenues dans le passeport (tout spécialement les données considérées comme sensibles telles que les empreintes digitales) ; les données personnelles telles que la photo digitalisée du visage ou encore le nom ou la date de naissance, etc. ne sont pas couvertes. L'utilisation de l'EAC ne peut pas être introduite à l'échelle internationale, étant donné que l'EAC n'est pas une norme internationale acceptée par l'ICAO. Cela implique que, dans les pays non-européens, seul le contrôle d'accès de base (BAC) sera utilisé, avec un niveau de sécurité bien moindre.
(11) L'entropie de la clé peut baisser à 35, voire même 28 bits si, par exemple, les numéros des passeports dépendent des autres informations contenues dans les passeports (comme c'est le cas aux Pays-Bas et en Allemagne). [Référence: Beel, J., Gipp, B., ePass - der neue biometrische Reisepass, Shaker Verlag, Aachen 2005. Télécharger le chapitre 6 "Fazit": www.beel.org/epass/epass-kapitel6-fazit.pdf]
(12) Voir, par exemple, www.wired.com/news/technology/1,71521-0.html

Voir aussi :
http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_fr.pdf