Sécurité du passeport électronique : 10 ans après son lancement, quelles lecons en tirer ?

Patrick Lacharme

Sécurité du passeport électronique : 10 ans après son lancement, quelles lecons en tirer ?

P. Lacharme

Résumé

Les passeports électroniques proposés par l'ICAO en 2004 sont désormais utilisés dans le monde entier. Ce type de document possède une puce sans contact contenant des données personnelles très sensibles incluant des données biométriques. Une série de protocoles cryptographiques a été spécifié pour assurer la sécurité des données stockées et transmises aux lecteurs. La sécurité des premiers protocoles a été fortement critiquée et des protocoles plus solides ont ensuite été proposés. Cet article décrit l'historique de la sécurité du passeport électronique et explique pourquoi la sécurité du passeport est toujours un problème.

Mots clés : Passeports électroniques

1 Introduction

Les premiers passeports électroniques ont été proposés par la Malaisie en 1998 [Ism07], mais il faudra attendre le début des années 2000 pour que ceux-ci commencent à se généraliser aux autres pays. En octobre 2004, l'organisation internationale d'aviation civile (ICAO) publie un ensemble de spécifications sur les passeports électroniques [(IC04], incluant l'intégration d'une puce sans contact contenant des informations biométriques sur le titulaire. L'intégration des empreintes digitales dans le passeport a transformé son nom en passeport biométrique. Des protocoles cryptographiques sont proposés pour assurer la sécurité des données du passeport. Les passeports électroniques sont désormais diffusés dans beaucoup de pays et la tendance actuelle est de généraliser ce format à d'autres documents comme les visas, les cartes d'identités ou même le permis de conduire biométrique.

Plusieurs vulnérabilités ont tout de suite été identifiées dans les protocoles cryptographiques implémentés sur les passeports électroniques de différents pays (par exemple [JMW05, KK05, Sch06, AKQ08]), pouvant être exploitée grâce à l'utilisation d'une technologie sans contact. L'Union Européenne a donc proposé rapidement un nouvel ensemble de protocoles en 2006 appelé EAC v.1 (*Extended Access Control*) [JA06, KÖ5] dont l'objectif était de corriger certaines imperfections. Une nouvelle série de protocoles est introduite par le BSI en 2008 appelée EAC v.2, amenée à remplacer la première série de spécification qui était loin de tout corriger [fSidIB10, Nit09, CV09]. Son utilisation est désormais obligatoire pour les documents de l'Union Européenne depuis juin 2009, notamment à cause de l'introduction des empreintes digitales dans le passeport qui réclame un protocole d'accès aux données plus solide.

L'utilisation de ces nouveaux protocoles cryptographiques *à l'état de l'art* laissait penser que la sécurité des passeports électroniques était enfin assurée. Malheureusement, les passeports électroniques contiennent toujours des problèmes de sécurité, notamment à travers la gestion des clés utilisées pour l'accès aux données, indépendamment des protocoles cryptographiques utilisés.

2 Description d'un passeport électronique

Les standards de l'ICAO spécifient que le passeport électronique doit contenir un circuit intégré utilisant une technologie sans contact contenant des informations biométriques identifiant le possesseur du passeport (Doc 9303). Cette puce contient aussi d'autres données reliées au porteur du passeport, comme celles écrites en clair à l'intérieur du document dans la zone lisible du passeport (MRZ, *Machine Readable Zone*).

2.1 Zone lisible du passeport

La zone lisible du passeport correspond aux deux lignes de texte en bas du passeport. Les informations contenues dans ces deux lignes sont : le nom et prénom du porteur, 3 lettres correspondant au code du pays, le numéro du passeport, la date de naissance du porteur, la date d'expiration du passeport et 3 digits de contrôle. Cette zone est lue par un scanner optique (OCR) lors du contrôle du document. Pour calculer les digits de contrôle, on réalise la procédure suivante où les lettres sont codées de 10 à 35 : la suite des symboles est considérée par triplets $x_1x_2x_3$, et on calcule la somme $7 * x_1 + 3 * x_2 + x_3$. Le digit de contrôle est alors le résutat modulo 10. Cette technique de calcul est aussi appliquée aux cartes d'identité ou aux permis de séjour.

2.2 Technologie sans contact

D'après les spécifications de l'ICAO, la puce embarquée dans le passeport doit être conforme à la norme standard ISO 14443 sur la technologie sans contact de proximité [(IS00]. Contrairement à beaucoup de puces RFID, celles qui sont utilisées dans les passeports électroniques, sont capable d'effectuer des calculs cryptographiques importants, permettant par exemple de s'authentifier à l'aide d'un protocole d'authentification challenge/réponse et d'utiliser des algorithmes de cryptographie asymétrique. Toutes les données contenues dans la mémoire de la puce du passeport sont néanmoins vulnérables aux problèmes de sécurité engendrés par la technologie sans contact, incluant récupération malveillante des données en mémoire, l'écoute illegale, l'usurpation d'identité, les attaques par relais, le deni de service ou encore des problèmes de protection de la vie privée comme la traçabilité malveillante ([Avo05, Avo06, BGM08, Jue06]). Un des enjeux de sécurité important de la technologie RFID est de ne pas pouvoir activer la carte sans contact à l'insu du porteur du tag [1]

1. *Afin de réduire de façon significative le risque de fraude et de falsification, les pays de l'Union européenne ont décidé d'introduire un nouveau type de passeports équipés d'une puce à radiofréquence ("chip RFID") qui remplace le passeport "classique"*(Commission Nationale pour la protection des données, Luxembourg).

2.3 Données biométriques

La première spécification sur les passeports électroniques publiée par l'ICAO en 2004 propose l'encodage des caractéristiques biométriques dans la mémoire de la puce. Les données biométriques sont encodées selon le format CBEFF (*Common Biometric File Format*), décrit dans la norme ISO 19785 et concernent les données suivantes :

1. Des données biométriques considérées comme *non sensibles* : la photographie faciale numérisée en format jpeg du possesseur du document, prise sous certaines conditions (obligatoire).
2. Un emplacement pour des données biométriques considérées comme *sensibles* : les empreintes digitales et l'iris.

L'Union Européenne a proposé de rendre obligatoire à partir de 2009 la présence de d'empreintes digitales dans la mémoire du passeport. Ainsi, deux empreintes digitales sont désormais stockées dans le passeport, tandis que huit empreintes sont par ailleurs stockées dans un fichier centralisé.

2.4 Données intégrées en mémoire

La mémoire de la puce du passeport électronique doit être au moins 32 kB, afin de stocker les données de la zone MRZ et surtout la photographie du visage. Cette mémoire est structurée en 16 groupes de données (appelée structure logique de données ou LDS, *Logical Data Structures*), conforme à la norme ISO 7816 pour assurer l'interopérabilité des passeports. Ces 16 groupes de données sont protégés en écriture et sont organisés de la manière suivante, où seuls les deux premiers groupes étaient obligatoires dans la première spécification de l'ICAO :

1. DG1 contient les deux lignes de la zone MRZ.
2. DG2 contient le fichier jpeg de la photo.
3. DG3 contient les empreintes digitales et DG4 l'iris.
4. DG14 et DG15 contiennent des clés publiques.

Ces données sont hachées, puis signées par le pays d'origine du passeport. Le résultat est stocké dans le fichier SOD (*Document Security Object*), avec la clé publique de la signature. Il existe une section sécurisée utilisée pour stocker des clés privées, qui ne peut être lue ou copiée de l'extérieur (si le passeport utilise de tels protocoles comme les protocoles d'authentification active ou de les protocoles de contrôle d'accès).

3 Protocoles cryptographiques

La première spécification de l'ICAO contenait un ensemble de trois protocoles cryptographiques : L'authentification passsive (AP, *Passive Authentication*), l'authentification active (AA, *Active Authentication*) et un protocole de contrôle d'accès (BAC, *Basic Acces Control*). Le protocole d'authentification passive était à l'origine le seul protocole obligatoire.

3.1 Protocole d'authentification passive

Le protocole d'authentification passsive permet au lecteur de vérifier que le contenu de la mémoire du passeport n'a pas été modifié. Il permet au lecteur de contrôler l'authenticité des 16 groupes de données contenus dans la mémoire du passeport électronique, en vérifiant que la signature (générée par l'émetteur du passeport durant la phase de personalisation) de ces données est correcte. Le lecteur vérifie la signature utilisée pour signer les données contenues dans la zone SOD, calcule ensuite le haché de chaque données dans la zone LDS et les compare avec les valeurs stockées dans la zone mémoire SOD pour en vérifier l'authenticité.

3.2 Protocole d'authentification active

L'authentification active est un protocole d'authentification challenge/réponse dont l'objectif est de permettre au lecteur de contrôler que le passeport n'a pas été copié ni fabriqué. La puce signe un challenge aléatoire de 64 bits envoyé par le lecteur, et prouve au lecteur qu'elle possède bien la clé secrète de signature stockée dans la section sécurisée de sa mémoire (qui ne peut pas être lue de manière externe à la puce). La clé publique correspondante se trouve dans la zone DG15 (dont l'authenticité est vérifiée à l'aide du protocole d'authentification passive).

3.3 Protocole d'accès aux données (BAC)

Le protocole de contrôle d'accès BAC est utilisé avant d'accéder aux données stockées dans le passeport et de réaliser les protocoles d'authentification active et passive. Le protocole BAC vérifie que le lecteur n'accède pas aux données à l'insu du porteur du document. Il établit aussi une clé de session destinée à chiffrer les communications futures entre le lecteur et la puce (une nouvelle clé de session est établie à chaque contrôle).

Pour cela le lecteur doit montrer qu'il a connaissance des données de la zone MRZ (le numéro du passeport, la date de naissance, la date d'expiration du passeport et 3 digits de contrôle), justifiant ainsi l'accord du porteur pour l'accès aux données. Le lecteur utilise ces données pour en tirer une clé secrète K de 128 bits, appelée clé d'accès $K = 128msb(SHA1(MRZ))$. Deux clés de 128 bits chacunes, K_{enc} et K_{mac}, sont ensuite dérivées de la clé d'accès K :

$$K_{enc} = 128msb(SHA1(K||1)), \quad K_{mac} = 128msb(SHA1(K||2)).$$

Ces deux clés sont utilisées par un algorithme de chiffrement 3-DES et un MAC dans un mécanisme de challenge/réponse dans la suite du protocole :

1. La puce génère et envoit un challenge C_p de 64 bits.
2. Le lecteur génère deux mots K_l et C_l de 64 bits et chiffre $C_l||C_p||K_l$ avec un triple DES et la clé K_{enc}, puis calcule le MAC du chiffré avec la clé K_{mac} et envoie le chiffré concaténé avec le MAC du chiffré à la puce :

$$MAC(ENC(C_l||C_p||K_l))||ENC(C_l||C_p||K_l).$$

3. La puce contrôle le message MAC avec la clé K_{mac}, déchiffre le chiffré avec K_{enc}, vérifie qu'il retrouve son challenge C_p et extrait la clé K_l.

4. La puce génère une clé K_p de 64 bits et chiffre $C_p||C_l||K_p$ avec un triple DES et K_{enc}, puis calcule le MAC du chiffré avec la clé K_{mac} et envoie au lecteur :
$$MAC(ENC(C_p||C_l||K_p))||ENC(C_p||C_l||K_p).$$
5. Le lecteur contrôle le message MAC avec la clé K_{mac}, déchiffre le chiffré avec K_{enc}, vérifie qu'il retrouve son challenge C_l et extrait la clé K_p.
6. Le lecteur et la puce ont désormais une clé de session commune $K = K_l \oplus K_p$ et génèrent une nouvelle clé de session de chiffrement K_{enc} et une nouvelle clé de session MAC K_{mac} en calculant respectivement $K_{enc} = 128msb(\text{SHA-1}(K||1))$, et $K_{mac} = 128msb(\text{SHA-1}(K||2))$.

3.4 Sécurité pour l'accès aux données

Le premier problème de sécurité concernant l'accès aux données vient du fait que l'authentification passive est le seul protocole obligatoire. Par ailleurs, les données décrites sur la zone MRZ servant à dériver la clé d'accès peuvent être lues directement sur le passeport (personnel d'un aéroport,..) ou connues, même partiellement (date de naissance).

Le protocole BAC utilise une clé dérivée de la zone MRZ qui possède peu d'entropie. Il est donc possible de faire une recherche exhaustive sur la clé d'accès, comme présenté sur différents passeports européens [CLRPS06, AKQ07, AKQ08]. Ces attaques utilisent le fait que l'entropie de la date de naisance du porteur est $\log(100 \times 365, 25) = 15, 16$. De plus dans certains pays, il y a une corrélation entre la date d'expiration et du numéro du passeport électronique. Il y a deux manières de monter une telle attaque : une attaque on-line et une attaque off-line. L'attaque on-line consiste à se munir d'un lecteur et d'envoyer suffisament de requêtes au passeport électronique pour déterminer la clé de session par force brute. Cette attaque est toutefois difficile à mener à cause du temps de réponse de la puce et du taux de communication (entre 106 kbits/s et 848 kbits/s selon la norme ISO 14443). L'attaque off-line est beaucoup plus efficace que l'attaque précédente et requière juste un texte chiffré pour être montée. Cela signifie que l'attaquant doit intercepter une communication entre un lecteur et un passeport électronique puis faire une attaque par force brute sur la clé.

D'autres vulnérabilités ont été relevées sur les passeports comme les problèmes de traçabilité, de challenge sémantiques, les attaques par relais ou simplement les attaques par canaux cachés ou le deni de service [fSidIB10, HR07, MVV07, Whi05, CS10, RMP08, PPW08, BGSV08a, BGSV08b].

4 Deuxième génération de protocoles (EAC)

Les protocoles cryptographiques spécifiés dans la seconde génération de passeports électroniques (2006) consistent en un ensemble de deux nouveaux protocoles appelé EAC, proposé par le BSI [fSidIB10] pour les passeports de l'Union Européenne :

1. L'authentification de la puce (CA, *Chip Authentication*)
2. L'authentification du lecteur (TA, *Terminal Authentication*).

Le porteur du passeport présente la zone MRZ au lecteur. Le lecteur et la puce établissent un canal de communication chiffré à l'aide d'une clé de session établie avec le protocole BAC. Les protocoles d'authentification de la puce et du terminal sont ensuite effectués (non décrits ici). Vers la fin 2008, le BSI présente une nouvel ensemble de spécifications [fSidIB10], pour remplacer celles de 2006. Cette suite comprend un nouveau mécanisme pour établir une connection entre le lecteur et la puce appelé PACE (*Password Authenticated Connection Establishment*), ayant pour but de remplacer le protocole BAC, ainsi qu'une nouvelle version pour l'authentification du terminal (TA v.2) et de la puce (CA v.2). Ces deux derniers protocoles forment l'ensemble EAC v.2 et sont réalisés de manière inversée par rapport à la v1. PACE est adopté par l'ICAO en 2010 [(IC10].

4.1 Authentification du terminal

Le lecteur doit désormais s'authentifier auprès du passeport avant celui ci, contrairement à la première version de l'EAC. Le but de ce protocole est de s'assurer que le lecteur est bien autorisé à accéder aux données du passeport. C'est un schéma challenge/réponse avec vérification d'une chaine de certificats.

1. Le lecteur envoie la chaine de certificats au passeport.
2. La puce vérifie l'authenticité de ces certificats et extrait la clé publique du lecteur PuK_l.
3. Le lecteur génère une paire de clé Diffie-Hellman $(PuK_{l,ta}, PrK_{l,ta})$ à l'aide du domaine D_p et envoie la clé publique compressée $H(PuK_{l,ta})$ à la puce. Il peut aussi envoyer une donnée auxilière A_l.
4. La puce envoie un challenge aléatoire R_p au lecteur.
5. Le lecteur signe la chaine $(ID_p||R_p||H(PuK_{l,ta})||A_l)$ à l'aide de sa clé secrète PrK_l et l'envoie à la puce.
6. La puce vérifie que la signature est correcte avec la clé publique du lecteur PuK_l, connaissant les autres paramètres.

ID_p est l'identifiant de la puce qui correspond à la MRZ si le protocole BAC est utilisé et à la clé publique compressée $H(PuK_p)$ si le protocole PACE est utilisé.

4.2 Authentification de la puce

Ce protocole utilise la paire de clé du lecteur $(PuK_{l,ta}, PrK_{l,ta})$, générée pendant l'authentification du terminal. Pour s'assurer de l'authenticité de la clé publique PuK_p de la puce, le lecteur doit utiliser auparavant le protocole d'authentification passive.

1. La puce envoie au lecteur sa clé publique PuK_p et les paramètres D_p.
2. Le lecteur envoie à la puce la clé publique provisoire $PuK_{l,ta}$ générée pendant le protocole d'authentification du terminal.
3. La puce calcule la compression de la clé publique provisoire$PuK_{l,ta}$ (et éventuellement des données auxilières A_l) et le compare avec le celui calculé lors du protocole d'authentification du terminal.
4. Les deux parties ont alors suffisament partagé d'informations pour dériver une clé de commune K en calculant respectivement

$$K = KA(PrK_p, PuK_{l,ta}, D_p) = KA(PrK_{l,ta}, PuK_p, D_p).$$

5. La puce génère ensuite aléatoirement une donnée R_p. Elle calcule les clés de sessions par $K_{enc} = \text{SHA-1}(K||R_p||1)$ et $K_{mac} = \text{SHA-1}(K||R_p||2)$. La puce calcule ensuite $T_p = MAC(K_{mac}, PuK_{l,ta}, D_p)$ et envoie la donnée R_p et T_p au lecteur.
6. Le lecteur utilise R_p pour calculer les clés de session K_{enc} et K_{mac} à partir de la clé commune K. Il vérifie ensuite que la valeur T_p est correcte.

La puce est authentifiée par une paire de clé statique (PrK_p, PuK_p), en remplacement du protocole d'authentification active. Ce protocole évite toutefois les problèmes de *challenges sémantiques* et génère aussi une clé de session.

4.3 Protocole d'accès PACE

Le protocole PACE permet à la puce de vérifier que le certificat du lecteur est valide et établit une clé de session. PACE utilise une clé π partagée par le lecteur et le passeport qui supporte de multiples types de clés, par exemple un court mot de passe écrit sur le passeport. Il n'y a aucune raisons que ce mot de passe ait un quelconque rapport avec les données personnelles inscrites sur la MRZ, évitant ainsi une surestimation de l'entropie. PACE réalise un échange de clé (Diffie Hellman traditionnel ou courbes elliptiques) pour établir une clé de session où toutes les clés utilisées sont provisoires (pas de clés statiques) :

1. La puce génère un challenge R_p, calcule $K_\pi = \text{SHA-1}(\pi||3)$, chiffre R_p avec la clé K_π et envoie le chiffré z au lecteur, et les paramètres D_p.
2. Le lecteur calcule $K_\pi = \text{SHA-1}(\pi||3)$, déchiffre z et R_p.
3. La puce et le lecteur calculent les nouveaux paramètres du domaine D' avec R_p et D_p.
4. La puce et le lecteur génèrent chacun un couple de clé provisoire, notés $(PuK_{p,pace}, PrK_{p,pace})$ et $(PuK_{l,pace}, PrK_{l,pace})$, et envoient à l'autre leur clé publique provisoire respective.
5. Les deux parties dérivent une clé K en calculant
$$K = KA(PrK_{p,pace}, PuK_{l,pace}, D') = KA(PrK_{l,pace}, PuK_{p,pace}, D').$$
6. La puce et le lecteur calculent les clés de session :
$K_{enc} = \text{SHA-1}(K||1)$ et $K_{mac} = \text{SHA-1}(K||2)$.
7. Authentification mutuelle entre la puce et le lecteur :
   (a) Le lecteur calcule et envoie $T_l = MAC(K_{mac}, PuK_{p,pace})$ à la puce qui le calcule de son coté et le vérifie.
   (b) La puce calcule et l'envoie $T_p = MAC(K_{mac}, PuK_{l,pace})$ au lecteur qui le calcule de son coté et le vérifie.

PACE est un protocole d'échange de clés authentifié par mots de passe (PAKE), dont la preuve de sécurité a été étudiée dans [BFK09, DF10], en relation avec ce type de protocoles [BPR00, AFP05]. Une variante du protocole PACE est le protocole SAC. La différence concerne le point 3 de l'algorithme précédent, où SAC utilise une technique différente pour calculer les paramètre du domaine [Ica09, BCI$^+$10, CIP12]. Le principe d'un protocole d'échange de clés authentifié par mot de passe est que le mot de passe contenant à priori une entropie réduite, la clé de session

obtenue ne doit pas dépendre directement de ce mot de passe afin d'empêcher les attaques off-line, ce qui est le cas dans le protocole PACE. Le mot de passe doit simplement ralantir suffisament le protocole pour empêcher les attaques on-line (en jouant sur les temps de réponse) Le protocole PACE évite ainsi les vulnérabilités de son prédécesseur.

5 Sécurité des données

La numérisation des documents d'identité s'est accompagné de nouvelles menaces de sécurité, en particulier avec l'introduction des données biométriques. Ces problèmes de sécurité sont accentués par l'utilisation d'une technologie sans contact. Les données du passeport pouvant être lues à l'insu de l'utilisateur sans protection adéquates, jusqu'à une distance de 10 mètres selon le réseau Européen FIDIS (Future of Identity in the Information Society) en 2006 [FID06]. Le G29 [2] souligne dans son avis du 30 septembre 2005 que l'introduction d'éléments biométriques numérisés dans les passeports aura de lourdes conséquences sur la vie privée pour les titulaires de ces documents, ce que confirme aussi la Commission Nationale Informatique et Liberté (CNIL) dans son rapport de juin 2008 [eLC08]. On peut se poser des questions sur la pertinence d'introduire de telles données dans le passeport. L'exemple de la carte d'identité française donne quelques réponses sur le sujet. Ainsi, dans le rapport du sénat sur la proposition de loi relative à la protection de l'identité de 2011, on peut y lire textuellement que *Le sujet engage aussi des enjeux économiques, industriels : la sécurisation des échanges électroniques est un marché ; les collectivités, les administrés paient le coût de ces titres biométriques. Les entreprises françaises, en pointe sur ce domaine, veulent investir le marché français.* La création de la plus grande base de données biométriques de France ne semble pas vraiment concerner tout le monde, puisqu'à peine 11 députés étaient présents à l'assemblée nationale pour voter la création de la carte d'identité biométrique le 7 juillet 2011.

Le cas du passeport biométrique n'est pas plus rassurant. Les protocoles cryptographiques assurant la sécurité des données des passeports de la dernière génération sont spécifiés pour être très solides. Mais les choses différent beaucoup dans la pratique. Par exemple, la procédure APIS (Advanced Passenger Information System) consiste à transmettre aux autorités d'immigration de certain pays avant le départ de l'avion différentes informations incluant toutes les données de la MRZ. Cette procédure s'applique à de plus en plus de pays incluant notament le Canada, les États unis, l'Inde, la Chine, le Japon, le Royaume-Uni, l'Espagne et l'Australie (la liste a tendance à augmenter). Dans la pratique, cela signifie que si vous passez par une agence de voyage pour acheter des billets d'avion, celle-ci vous demandera ces informations (éventuellement avec une copie de la première page du passeport). Les agences de voyage ignorent totalement la possibilité d'utiliser les données de la MRZ pour accéder aux données du passeport et stockeront sans doute ces informations en clair sur un support non sécurisé. Elles n'ont aucune recommendations de sur ce sujet. On peut aussi raisonablement imaginer que ces informations sont potentiellement accompagnées de votre addresse personnelle, afin de faciliter la vie de quelqu'un qui souhaiterait les utiliser en ayant plus qu'à s'approcher de votre résidence et vous intercepter discrètement avec votre passeport. En clair, le passage

2. Le groupe de travail Article 29 (l'ensemble des *cnil européennes*).

du protocole BAC au protocole PACE se fait avec des clés dont le stockage est potentiellement réalisé de manière non sécurisée.

La sécurité principale pour empécher un faux lecteur d'accéder aux données à l'insu du porteur du passeport semble donc être le certificat du lecteur, utilisé dans le protocole d'authentification du terminal. Adam Laurie et Jeroen Van Beek ont présenté une technique simple pour se passer de certificats dans le cadre du protocole d'authentification passive [CNN]. Ceux-ci ont même réussi à se faire passer pour Elvis Presley à l'aéroport d'Amsterdam en septembre 2008, avec une photo signée par un pays n'existant pas (authentification passive). En effet, en 2008, il n'existait pas de liste commune de tous les certificats de tous les pays et le certificat du pays imaginaire était considéré comme valide. Si cette liste s'est faite depuis, le fait que la puce ne possède pas d'horloge interne pour vérifier la validité des certificats du lecteur pose quand même un sérieux problème. C'est le lecteur qui donne au passeport le jour et l'heure au passeport, ce qui peut s'avérer très utile pour éviter une liste de révocation.

6 Conclusion

Dans ce papier, les deux premières générations de passeports électroniques sont présentées. La sécurité des protocoles a été analysée en prenant en compte la protection de la vie privée du possesseur du passeport qui est très importante au regard de la sensibilité des données contenues dans le document. Les protocoles de la dernière spécification ont corrigé de nombreux problèmes de sécurité contenus dans les premières générations de passeports électroniques, mais ne sont toutefois pas encore intégrés dans les passeports électroniques actuels.

De manière générale, l'utilisation d'une puce sans contact lors du contrôle du passeport a pour but de rendre plus rapide ce contrôle pour les usagers. Toutefois, la nécessité de lire la zone MRZ pour l'authentification du système d'inspection (que ce soit lors des protocoles BAC ou PACE) rend cette option beaucoup moins intéressante, tout en engendrant des vulnérabilités caractéristiques aux systèmes utilisant des puces sans contact de type RFID.

Références

[AFP05] M. Abdalla, P.A. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In *Public Key Cryptography (PKC'05)*, LNCS 3386, pages 65–84, 2005.

[AKQ07] G. Avoine, K. Kalach, and J.J. Quisquater. Belgian biometric passport does not get a pass.. Your pesonal data are in danger !, 2007.

[AKQ08] G. Avoine, K. Kalach, and J.J. Quisquater. epassport : Securing international contacts with contactless chips. In *Financial Cryptography and Data Security (FC'08)*, LNCS 5143, pages 141–155, 2008.

[Avo05] G. Avoine. Cryptography in radio frequency identification and fair exchange protocols. thèse de doctorat, 2005.

[Avo06] G. Avoine. RFID et sécurité font-ils bon ménage ? In *SSTIC*, 2006.

[BCI+10] E. Brier, J.S. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi. Efficient indiferentiable hashing into ordinary curves. In *CRYPTO'10*, LNCS 6223, pages 237–254, 2010.

[BFK09] J. Bender, M. Fischlin, and D. Kügler. Security analysis of the pace key-agreement protocol. In *Information Security and Conference (ISC'09)*, LNCS 5735, pages 33–48, 2009.

[BGM08] C. Boursier, P. Girard, and C. Mourtel. Activation des cartes à puce sans contact à l'insu du porteur. In *SSTIC*, 2008.

[BGSV08a] C. Blundo, G.Persiano, A. R. Sadeghi, and I. Visconti. Improved security notions and protocols for non-transferable identification. In *ESORICS'08*, LNCS 5283, pages 364–378, 2008.

[BGSV08b] C. Blundo, G.Persiano, A. R. Sadeghi, and I. Visconti. Resettable and non-transferable chip authentication for e-passports. In *RFIDSec'08*, 2008.

[BPR00] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Eurocrypt 2000*, LNCS vol 1807, pages 139–155, 2000.

[CIP12] J. S. Coron, A. Gouget T. Icart, and P. Pailler. Supplemental access control (pace v2) : Security analysis of pace integrated mapping. In *Cryptography and Security*, LNCS 6805, pages 207–232, 2012.

[CLRPS06] D. Carluccio, K. Lemke-Rust, C. Paar, and A.R. Sadeghi. The global traceability or how to feel like an ups package. In *WISA'06*, LNCS 4298, pages 391–404, 2006.

[CNN] CNN. Hackers expose security flaws with 'elvis presley' passport. `http://edition.cnn.com/2010/TECH/02/19/passport.security/`.

[CS10] T. Chotia and V. Smirnov. A traceability attack against e-passports. In *Financial Cryptography and Data security (FC'10)*, LNCS 6052, pages 20–34, 2010.

[CV09] R. Chaabouni and S. Vaudenay. The extended access control for machine readable travel machine, technical report, 2009.

[DF10] O. Dagdelen and M. Fischlin. Security analysis of the extended access control protocol for machine readable travel documents. In *Information Security Conference (ISC'10)*, LNCS 6531, pages 54–68, 2010.

[eLC08] Commission Nationale Informatique et Liberté (CNIL). Passeports biométriques : la CNIL réservée sur la création de la première base de données biométriques relatives aux citoyens français. rapport technique, 2008.

[FID06] FIDIS. Déclaration de budapest sur les documents de voyage à lecture automatique (MRTD - machine readable travel documents), 2006.

[fSidIB10] Bundesamt fur Sicherheit in der Informationstechnik (BSI). Advanced security mechanism for machine readable travel documents. Technical guideline TR-03110, version 2.05, 2010.

[HR07] M. Hlavác and T. Rosa. A note on the relay attacks on e-passport : the case of czech e-passports. technical report, eprint, 2007.

[(IC04] International Civil Aviation Organization (ICAO). Doc 9303 : Machine readable travel documents - part 1, volume 1, 2004.

[(IC10] International Civil Aviation Organization (ICAO). Supplemental access control for machine readable travel documents, 2010. `http://www.icao.int/Security/mrtd/Pages/default.aspx`.

[Ica09] T. Icart. How to hash into elliptic curves. In *CRYPTO'09*, LNCS 5677, pages 303–316, 2009.

[(IS00] International Standards Organization (ISO/IEC). ISO/IEC 14443 identification cards - contactless integrated circuit(s) card - proximity card, 2000.

[Ism07] N. Ismail. Rfid : Malaysia's privacy at the crossroads ? In *Cyber Privacy and Security*, pages 207–224, 2007.

[JA06] Justice and Home Affairs. Eu standard specifications for security features and biometrics in passports and travel documents. technical report, european union, 2006.

[JMW05] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In *IEEE SecureComm*, pages 74–88, 2005.

[Jue06] A. Juels. RFID security and privacy : a research survey. *IEEE Journal on Selected Areas in Communications*, 24(2) :381–394, 2006.

[KÖ5] D. Kügler. Advanced security mechanism for machine readable travel documents. technical report, version 0.90, bsi, 2005.

[KK05] G. Kc and P. Karger. Security and privacy issues in machine readable documents. technical reports, eprint, 2005.

[MVV07] J. Monnerat, S. Vaudenay, and M. Vuagnoux. About machine-readable travel documents - privacy enhancement using (weakly) non-transferable data authentication. In *RFIDSec'07*, 2007.

[Nit09] R. Nithyanand. A survey on the evolution of cryptographic protocols in epassports. technical report eprint, 2009.

[PPW08] V. Pasupathinathan, J. Pieprzyk, and H. Wang. An on-line secure e-passport protocol. In *ISPEC'08*, LNCS 4991, pages 14–28, 2008.

[RMP08] H. Richter, W. Mostowski, and E. Poll. Fingerprinting passports. In *NLUUG Spring Conference on Security*, 2008.

[Sch06] B. Schneier. The id chip you dont want in your passport. the washinton post, 2006.

[Whi05] M. Whitteman. Attacks on digital passports. in what the hack, liempde, netherlands, 2005.