Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense nationale

*Direction centrale de la sécurité
des systèmes d'information*

Paris, le 24 octobre 2008

N° 2415/SGDN/DCSSI/SDR

Référence : NOTE/09.1

NOTE D'APPLICATION

E-PASSPORT : UTILISATION DU PROFIL DE PROTECTION EAC

Objet : E-passport : utilisation du profil de protection EAC

Application : Date de publication

Diffusion : Publique (www.ssi.gouv.fr)

Vérifié par	Validé par le sous-directeur de la régulation	Approuvé par le directeur central de la sécurité des systèmes d'information
Le responsable qualité [ORIGINAL SIGNE] *Le chef du centre de certification* [ORIGINAL SIGNE]	[ORIGINAL SIGNE]	[ORIGINAL SIGNE]

Suivi des modifications

Révision	Date	Modifications
1.0	24/10/2008	Création

TABLE DES MATIERES

1. Objet de la note

Les profils de protection [PP BAC] et [PP EAC] ont été rédigés pour spécifier l'évaluation du produit passeport électronique (Machine Readable Travel Document, noté MRTD en abrégé).

Cette note d'application a pour but d'apporter un éclairage sur certaines particularités de ces profils de protection, dans le but de faciliter la rédaction des cibles de sécurité, mais également de garantir une approche homogène dans les évaluations de passeports électroniques réalisées par les différents laboratoires.

1.1. Références

- [PP BAC] : Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Basic Access Control, référence : BSI-PP-0017, Version 1.0, 18 Août 2005, BSI. Publié sur le site Internet www.commoncriteriaportal.org[1].
- [PP EAC] : Common Criteria Protection Profile - Machine Readable Travel Document with „ICAO Application", Extended Access Control, référence : BSI-PP-0026, Version 1.2, 19 novembre 2007. Publié sur le site Internet www.commoncriteriaportal.org[2].
- [ICAO 9303 v1] : 9303 part 1 volume 1, Sixth edition, 2006, Passports with Machine Readable Data Stored in Optical Character Recognition Format. Accesible sur le site Internet www.icao.int[3]
- [ICAO 9303 v2] : 9303 part 1 volume 2, Sixth edition, 2006, Specifications for Electronically Enabled Passports with Biometric Identification Capability. Accesible sur le site Internet www.icao.int[4]
- [REF CRYPTO] : Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version 1.10, 14 septembre 2007, No. 1904/SGDN/DCSSI/SDS/LCR. Publié sur le site Internet www.ssi.gouv.fr[5]
- [PUBLI] : Security and Privacy Issues in E-passports, By Ari Juels, David Molnar, and David Wagner
- [PP9911] : Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999. Certifié par la DCSSI sous la référence PP/9911. Publié sur le site Internet www.ssi.gouv.fr[6].

1.2. Définition du cycle de vie

Le périmètre d'évaluation, défini dans les profils de protection [PP BAC] et [PP EAC] couvre une large partie du cycle de vie des produits, depuis la phase de développement des microcontrôleurs et des applications embarquées jusqu'à la phase de fabrication du livret du passeport. Ce périmètre couvre un large spectre d'acteurs et de métiers, allant de la microélectronique jusqu'à la fabrication du papier.

---

[1] http://www.commoncriteriaportal.org/files/ppfiles/PP0017b.pdf

[2] http://www.commoncriteriaportal.org/files/ppfiles/pp0026_ma1b.pdf

[3] http://www.icao.int/icao/en/sales/index.html

[4] http://www.icao.int/icao/en/sales/index.html

[5] http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/mecanismes_cryptographique_v1_10_standard_uk.pdf

[6] http://www.ssi.gouv.fr/site_documents/pp/pp9911.pdf

L'objectif du chapitre 2 est de guider la rédaction de cibles de sécurité pour réduire leur périmètre aux phases utiles du point de vue de la sécurité en permettant une approche réaliste de l'évaluation, tout en gardant la conformité au PP.

1.3. Résistance intrinsèque du mécanisme BAC – Entropie des données MRZ

Les spécifications de l'OACI (référence [ICAO 9303 v2] § III LDS (Logical Data Structure) et § IV PKI (Public Key Infrastructure)) relatives au produit passeport électronique (MRTD) décrivent le mécanisme de contrôle d'accès permettant de protéger les données stockées dans le MRTD, comprenant les données personnelles du porteur de passeport (données biographiques and photo numérique du visage). La fonction de contrôle d'accès protège le produit contre son activation à l'insu du porteur (skimming) ou l'interception des communications sans-contact (eavesdropping).

Le « Basic Access Control » (BAC) est un mécanisme d'authentification mutuelle entre le MRTD et le système d'inspection[7]. Il se déroule comme suit :

- le porteur présente son passeport sur le système d'inspection ;
- le système d'inspection effectue une lecture optique des données MRZ imprimées sur le livret du passeport ;
- le système d'inspection en déduit, par dérivation, la clé d'authentification du MRTD ;
- le système d'inspection s'authentifie auprès du MRTD (via l'interface « sans contact ») ;
- si l'authentification est réussie, le système d'inspection et le MRTD calculent une clé de session partagée pour chiffrer les futures communications (secure messaging) au cours desquelles transitent les données contenues dans le MRTD.

Une particularité du BAC est que la clé est statique et peut être dérivée des données MRZ imprimées sur le livret du passeport. Les profils de protection [PP BAC] et [PP EAC] incluent ce mécanisme dans leur périmètre. Le [PP BAC] vise un niveau de résistance AVA_VLA.2 (résistance à des attaquants disposant d'un potentiel d'attaque élémentaire) alors que le [PP EAC] vise un niveau AVA_VLA.4 (résistance à des attaquants disposant d'un potentiel d'attaque élevé). Or la résistance intrinsèque du mécanisme BAC, inclus dans les deux PP, est faible du fait de l'entropie de la clé BAC et ne peut atteindre le niveau de résistance requis par AVA_VLA.4.

Le chapitre 3 précise des éléments techniques relatifs à la résistance du mécanisme BAC et explique comment [PP EAC] traite ce problème.

[7] Système permettant de lire les passeports et d'identifier le porteur au contrôle frontalier.

2. Définition du cycle de vie

2.1. Comparaison entre les [PP BAC]/[PP EAC] et le [PP9911]

Le cycle de vie décrit dans [PP BAC] et [PP EAC] est clair et sans ambigüité. Il comporte quatre phases là où des profils de protection comme [PP9911] identifient un cycle de vie plus détaillé et correspondant aux différents métiers et acteurs impliqués dans le développement et la fabrication d'une carte à puce.

Le tableau ci-dessous résume les différences entre les [PP BAC]/[PP EAC] et [PP9911] :

<table>
<tr><th>[PP BAC] / [PP EAC]</th><th>[PP9911]</th></tr>
<tr><td rowspan="2">Phase 1:
- Développement du micro-circuit et du logiciel dédié, et des guides associés ;
- Développement de l'application et des guides associés.</td><td>Phase 1: Développement de l'application et des guides associés.</td></tr>
<tr><td>Phase 2: Développement du microcircuit et du logiciel dédié, et des guides associés. Fabrication du masque.</td></tr>
<tr><td rowspan="3">Phase 2:
- Production de la puce, données d'identification,
- Fabrication du MRTD, incluant :
▪ Pré-personnalisation: patch, activation de l'application, chargement des données d'authentification de l'agent de personnalisation,
▪ Fabrication de l'Inlay (antenne),
▪ Fabrication du livret.</td><td>Phase 3: Fabrication et pré-personnalisation du produit (clé de transport)</td></tr>
<tr><td>Phase 4: Mise en micro-module, tests.</td></tr>
<tr><td>Phase 5: Encartage, tests.</td></tr>
<tr><td>Phase 3: personnalisation du MRTD (enrôlement et chargement des données du porteur).</td><td>Phase 6: personnalisation, tests.</td></tr>
<tr><td>Phase 4: usage opérationnel.</td><td>Phase 7: utilisation, fin de vie.</td></tr>
</table>

En regard du cycle de vie du [PP9911], le produit évalué est celui qui sort de la phase de fabrication, tests et pré-personnalisation (phase 3). Les phases suivantes sont couvertes par les guides du produit et les tests (cf. [GUIDES]).

En regard du cycle de vie des [PP BAC]/[PP EAC], le produit évalué est par défaut le MRTD à la fin de la phase de fabrication (fin de phase 5 du cycle de vie du [PP9911]).

C'est un changement majeur comparé à ce qui était considéré dans les évaluations classiques de cartes à puce, et qui avait été construit de façon à être adapté à l'organisation des métiers de la carte à puce. Dans le cas des [PP BAC]/[PP EAC], il va s'agir d'analyser les procédures sécuritaires et de réaliser des audits de sites pour un grand nombre d'acteurs (dont le fournisseur d'antenne et le fabricant du livret) alors même que certains d'entre eux n'ont pas d'impact sur la sécurité du produit. Cependant, notons que, dans la mise à jour du [PP EAC] (version 1.2), l'éditeur a introduit plus de flexibilité sur un certain nombre de points décrits dans les paragraphes suivants, et qui peuvent être considérés comme applicables pour le [PP BAC] également.

2.2. Considérations sur l'application de passeport électronique et sa pré-personnalisation

La phase 2 du cycle de vie décrit dans [PP BAC]/[PP EAC] correspond :

- au chargement d'éventuels correctifs de l'application (patchs) en mémoire EEPROM ;
- à la « création de l'application MRTD », opération qui n'est pas vraiment définie dans les profils de protection ;
- à la pré-personnalisation des MRTD avec les données de pré-personnalisation (*i.e.* clé d'authentification de l'agent de personnalisation).

Tous les acteurs impliqués dans ces activités techniques doivent donc être couverts par l'évaluation (au titre des tâches ACM, ALC, ADO et AGD), bien que la note d'application n°5 en page 9 du [PP EAC] autorise certaines adaptations :

1. En fonction du processus de développement du passeport électronique, la « création de l'application MRTD » peut être couverte par les guides et analysée au travers des tâches ADO / AGD, tant que les procédures décrites dans les guides précisent comment configurer l'application, et que ce processus de configuration ne permet pas de baisser le niveau de sécurité du produit ;
2. Les acteurs responsables du chargement des correctifs du produit (patchs) doivent faire partie du périmètre de l'évaluation (pour les tâches relatives à l'environnement de développement). Si le chargement des correctifs est effectué par le fabricant du mirco-circuit, ce point peut être déjà couvert par l'évaluation du micro-circuit et n'a pas besoin d'être analysé à nouveau ;
3. L'acteur responsable du chargement de la clé, garantissant l'autoprotection du produit depuis sa livraison jusqu'à son utilisation par l'agent de personnalisation, doit être inclus dans le périmètre d'évaluation (pour les tâches relatives à l'environnement de développement).

2.3. Considérations sur le livret du passeport

La fabrication des livrets (incluant la mise de l'inlay dans la couverture du passeport) n'a a priori aucun impact sur la sécurité électronique du MRTD, tant que la puce électronique est auto protégée durant ces phases (par une clé d'authentification par exemple).

En suivant la note d'application n°5 en page 9 du [PP EAC], il n'est donc pas nécessaire d'inclure cette partie du cycle de vie dans le périmètre de l'évaluation (pour les tâches relatives à l'environnement de développement).

2.4. Considérations sur l'antenne

L'antenne du MRTD influe sur le champ électromagnétique utilisé pour alimenter la puce en énergie et pour établir le canal de communication entre la puce et le terminal. Cette interaction doit être prise en compte dans l'évaluation du canal en termes de « canaux auxiliaires ». Des analyses techniques montrent que l'antenne agit comme un filtre qui peut atténuer l'information recherchée dans le champ RF, voire masquer le champ dans le pire des cas. La sonde utilisée pour mesurer l'effet « canaux auxiliaires » a également un impact sur le champ RF.

Cependant, pour caractériser les canaux auxiliaires au travers de l'interface sans-contact, il est toujours possible de mesurer le signal directement sur les plots de connexion RF de la puce (à l'aide d'un banc de test approprié). L'antenne est alors « émulée » et l'éventuel effet « canaux auxiliaires » est mesuré à la source, sans modification du signal brute par une sonde ou l'antenne.

C’est donc la situation optimale pour effectuer cette caractérisation. Si le produit s’avère résistant dans cette configuration, il le sera *a fortiori* avec son antenne.

Au vu de cette analyse, et tant qu’elle n’est pas remise en cause par l’évolution de l’état de l’art, la note d’application n°2 en page 6 du [PP EAC] autorise à considérer le produit sans prendre en compte une antenne spécifique (y compris celle de la TOE). Il n’apparaît donc plus utile de vérifier la conformité du fournisseur d’antenne aux critères relatifs à l’environnement de développement (DVS, ACM…).

3. Résistance intrinsèque du mécanisme BAC – Entropie des données MRZ

3.1. Analyse de la résistance intrinsèque du mécanisme BAC

La clé BAC est dérivée des données MRZ imprimées sur le livret du passeport, selon le format suivant (exemple extrait de [ICAO 9303 V2], Appendix 7) :

```
                P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
                L898902C<3UTO6908061F9406236ZE184226B<<<<<14
Couleurs:       RRRRRRRRRBVVVRRRRRRBVRRRRRRBVVVVVVVVV
```

La clé BAC du MRTD est obtenue à partir des données en rouge[8] dans ce document (données personnalisées) et celles en bleu (« check digit », avec des valeurs fixes), et permet de calculer une clé de session commune partagée par le MRTD et le système d'inspection afin de chiffrer leur communication (« secure messaging »).

Le premier bloc de données personnalisées correspond au numéro de passeport. Le second est la date de naissance du porteur et le troisième donne la date d'expiration du passeport.

Les valeurs possibles de ces paramètres et l'entropie associée sont décrites pour chaque groupe :

- selon les spécifications ICAO (Cf. [ICAO 9303 V2]), le numéro de passeport est constitué de 9 symboles tirés des caractères alphanumérique [a-z, A-Z, 0-9] qui donnent lieu à une entropie de $9*\log_2(26 + 26 + 10)=53,5$ bits. Mais selon les spécifications[9] [ICAO 9303 V1], seuls les caractères majuscules doivent être utilisés. L'entropie est finalement de $9*\log_2(26 + 10)$ = **46,5 bits** ;
- la date de naissance d'une personne ayant au maximum 75 ans fournit une entropie de $\log_2(365*75)$=**14,7 bits**, mais la simple observation du porteur permet déjà de réduire cette valeur ;
- la date d'expiration d'un passeport est incluse dans une plage de 10 ans, ce qui donne une entropie de $\log_2(365*10)$=**11,8** bits.

Le total atteint un maximum de **73 bits**. Or les règles et spécifications cryptographiques de la DCSSI (Cf. [REF CRYPTO]) exigent un minimum de 80 bits jusqu'en 2010, 112 bits au-delà. Cette valeur **n'est donc pas** compatible avec le niveau **AVA_VLA.4**.

Des exemples d'entropie liés au format de numéro de passeport de certains pays sont donnés en Annexe A.

3.2. Conséquences et conclusion pour le [PP EAC]

D'un côté, le [PP EAC] vise un niveau AVA_VLA.4 et, de l'autre côté, il identifie les données logiques MRZ comme biens à protéger, mais ces biens sont seulement protégées par le mécanismes BAC.

Le profil de protection [PP EAC] comporte cependant une note d'application n°1 en page 6, afin de rendre réalisable l'évaluation d'un produit conforme à ce PP.

---

[8] Pour le lecteur ne disposant pas d'une impression du document en couleurs, la ligne « couleur » donne les couleurs de chaque caractère (R = rouge, B = bleu, V = vert).

[9] voir [ICAO 9303 V1], appendix 8, §9.4.1 page IV-14

Etant donné que les données MRZ sont imprimées sur le livret, pour des raisons d'interopérabilité, et étant donné sa relative faible entropie, elles ne peuvent être protégées au-delà du niveau AVA_VLA.2, même si le [PP EAC] vise un niveau AVA_VLA.4.

L'évaluation au niveau AVA_VLA.4 porte donc sur les données biométriques de référence et sur le mécanisme EAC (incluant le mécanisme « chip authentication »).

Annexe A Numéro de passeport dans différents pays

Selon l'étude citée en référence [PUBLI], l'entropie de la clé BAC pour les passeports émis par les Etats-Unis est proche de 52 bits : les passeports émis depuis 1981 portent un numéro constitué de 9 caractères, dont les deux premiers prennent pour valeur le code de l'un des 15 bureaux d'émission et les sept restants sont attribués de façon arbitraire. Cela donne un total maximum de $\log_2(15 * 10)+14+11 \sim 53$ bits.

Des pays de l'Union européenne, comme l'Espagne ou l'Italie, semblent utiliser une lettre majuscule puis 6 chiffres. En ce cas, l'entropie est de $\log_2(26 * 106)+14+11 \sim 51$ bits.

En France, les numéros de passeport sont actuellement constitués de :

- deux chiffres donnant l'année du lot, *i.e.* 10 possibilités ce qui donne $\log_2(10) = 3,3$ bits. Mais comme l'année de fabrication du passeport est vraisemblablement proche de la date d'émission, cela réduit le nombre de possibilité de l0 ans à environ 2 ans ;
- deux lettres majuscules pour le lot (excluant G, J, M, N, O, Q, S, U, W), *i.e.* 17 possibilités, donnant $2*\log_2(17) = 8,2$ bits ;
- cinq chiffres, donnant : $5*\log_2(10) = 16,6$ bits.

La date d'expiration devient alors : $\log_2(365*2) = 9,5$ bits.

Ainsi additionnée à l'entropie de la date de naissance, le total en France est de 52 bits.