Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale
*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 03 JUIN 2015
N° 1256/ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

Application eTravel EAC v2.1, en configuration SAC, sur la carte à puce fermée MultiApp V3.1 masquée sur le composant P60D080PVC (Version du patch : 1.4)

GEMALTO / NXP SEMICONDUCTORS

Annexe : Documents de référence de la qualification.

L'application eTravel EAC v2.1, en configuration SAC, sur la carte à puce MultiApp V3.1 masquée sur le composant P60D080PVC (version du patch : 1.4) en configuration fermée[1], implémente les fonctionnalités de document de voyage électronique de type passeport [2] conformément au profil de protection [5].

Eu égard au rapport de certification [6], à la cotation cryptographique [7] et conformément au processus de qualification [1], j'atteste que ce produit atteint le niveau de qualification renforcé, sous réserve :

- des restrictions d'usage figurant aux chapitres 2.3 et 3.2 du rapport de certification [6] ;
- de l'activation du mécanisme optionnel « *Active Authentication* » permettant l'authentification du microcontrôleur **ou** du mécanisme EAC « *Chip Authentication* »;
- de l'activation de l'authentification forte entre le document de voyage électronique et le système d'inspection par le mécanisme SAC (*Supplemental Access Control*) ;
- du respect de l'application du guide [8] concernant le choix et le dimensionnement des mécanismes cryptographiques et notamment :
  - la taille des modules RSA doit être d'au moins 2048 bits pour une utilisation ne dépassant pas 2030 et d'au moins 3072 bits au-delà de 2030 ;
  - il est recommandé d'utiliser un exposant public RSA strictement supérieur à 2^{16} ;
  - la fonction de hachage SHA-1 ne doit pas être employée, les fonctions SHA-224, SHA-256, SHA-384, SHA-512 sont à privilégier ;
  - une même clé cryptographique chargée dans la carte à puce ne doit avoir qu'un seul usage ;
  - le *Card Access Number* doit être généré aléatoirement et d'une longueur de 3 octets au moins.

[1] La plateforme Java Card MultiApp V3.1 sur laquelle est installée le produit est en configuration fermée ce qui ne permet plus de charger d'autres applets durant la phase opérationnelle.

- la taille des clés pour les mécanismes reposant sur des *courbes elliptiques* doit être d'au moins de 224 bits pour une utilisation jusqu'en 2020 et 256 bits au-delà de 2020;

Les autres applications embarquées dans le produit, notamment l'applet IAS Classic destinée à réaliser des opérations de signature électronique et l'application « MOCA Server » destinée à réaliser des opérations de *Match On Card*, ne font pas partie du périmètre de la qualification[2].

Cette qualification est valable pour une durée de 1 an. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

Contre-amiral Dominique RIBAN
Directeur général adjoint

[2] Elles sont inactivées dans la configuration évaluée du produit qualifié.

Annexe

Documents de référence de la qualification

[1]. Processus de qualification au niveau renforcé, version 1.0 (disponible sur www.ssi.gouv.fr).

[2]. 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.

[3]. Référentiel Général de Sécurité et notamment ses annexes [RGS_A_2] (fonction de sécurité « Authentification », version 2.3 du 11 février 2010), [RGS_A_3] (fonction de sécurité « Signature », version 2.3 du 11 février 2010) et [RGS_B_1] (règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques).

[4]. MultiApp v3.1 : eTravel 2.1 EAC Security Target, Gemalto, référence : D1296549, version1.0 de Novembre 2014.

[5]. Profil de protection « Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.0, 2 novembre 2011. Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 10 novembre 2011 sous la référence BSI-CC-PP-0068-V2-2011.

[6]. Rapport de certification ANSSI-CC-2015/03, Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme fermée MultiApp V3.1 masquée sur le composant P60D080PVC (Version du patch : 1.4) du 12 février 2015.

[7]. Cryptographic Mechanisms Evaluation Report - DELPHES 31 - MRTD Project, Reference : DELPHES31_MRTD_cryptography_v1.0/1.0 du 14/01/2014, Serma Technologies

[8]. eTravel v2.x EAC – CC Certified – Reference Manual, Référence : D1280261A, version du 9 Janvier 2015, Gemalto.