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 23 OCT. 2015

N°411 /ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

Application eTravel Essential 1.0, avec SAC, AA et EAC activés, sur composant M7794 A12/G12 (version 1.0)

GEMALTO / INFINEON TECHNOLOGIES AG

Annexe : Références de la qualification.

L'application eTravel Essential 1.0, avec SAC (*Supplemental Access Control)*, AA (*Active Authentication*) et EAC (*Extended Access Control*) activés, sur composant M7794 A12/G12 (version 1.0), 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 ;
  - la fonction de hachage SHA-1 ne doit pas être employée, les fonctions SHA-224, SHA-256, SHA-384, SHA-512 sont à privilégier ;
  - il est recommandé d'utiliser un exposant public strictement supérieur à 2^{16} ;
  - une même clé cryptographique chargée dans la carte à puce ne doit affectée qu'à un seul usage (chiffrement, authentification, signature, etc.) ;
  - le *Card Access Number* doit être généré aléatoirement et d'une longueur de 3 octets au moins ;
  - la taille des clés pour les mécanismes de courbes elliptiques doit être au moins de 224 bits pour un usage jusqu'en 2020, et au moins de 256 bits pour un usage au-delà de 2020.

Cette qualification est valable pour une durée de 3 ans. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

Contre-amiral Dominique RIBAN
Directeur général adjoint

Annexe

Références 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 v2.0.

[4]. eTravel Essential 1.0 EAC on PACE Security Target, Gemalto, référence : D1315455, version1.3 du 26 février 2015.

[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-2015/32, Application eTravel Essential 1.0, avec SAC, AA et EAC activés, sur composant M7794 A12/G12 (Version : 1.0).

[7]. Cryptographic Mechanisms Evaluation Report: ERODIUM Project, ERODIUM_MRTD_cryptography_v1.0/1.0, 6 février 2015, Serma Technologies.

[8]. eTravel Essential 1.0 Reference Manual, reference D1325786, 25 février 2015, Gemalto.