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 MARS 2017
N° 1429 /ANSSI/SDE

QUALIFICATION AU NIVEAU RENFORCE

IDEAL PASS v2.0.1
EAC avec l'application PACE sur le composant M7892 B11

SAFRAN IDENTITY & SECURITY / INFINEON TECHNOLOGIES

Annexe : Références de la qualification (page 2).

La carte à puce IDEAL PASS v2.0.1 EAC avec l'application PACE sur le composant M7892 B11 pouvant être en mode contact ou sans contact, développée par *SAFRAN IDENTITY & SECURITY* sur un composant *INFINEON TECHNOLOGIES*, implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO) et européenne. Ce produit permet la vérification de l'authenticité du document de voyage et l'identification de son porteur lors du contrôle frontalier, à l'aide d'un système d'inspection.

Eu égard au rapport de certification [11] et à la cotation cryptographique [10], et conformément au processus de qualification [1], j'atteste que ce produit atteint le niveau de qualification renforcé dans le cadre du Référentiel général de sécurité [3], sous réserve :

- du respect des restrictions d'usage figurant aux chapitres 2.3 et 3.2 du rapport de certification [11] ;
- de l'activation du mécanisme « *Active Authentication* » permettant l'authentification du microcontrôleur ou du mécanisme « *Chip Authentication* » du protocole EAC ;
- du respect des condition suivantes concernant le choix et le dimensionnement des mécanismes cryptographiques :
  - l'algorithme TDES n'est pas recommandé pour un usage au-delà de 2020 ;
  - 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 ;
  - un exposant public strictement supérieur à 2^{16} doit être utilisé pour les clés RSA ;
  - pour les mécanismes de signature, les empreintes numériques doivent être d'au moins 224 bits jusqu'à 2020 et d'au moins 256 bits ensuite. À ce titre, la fonction de hachage SHA-l ne doit pas être utilisée, les fonctions SHA-224, SHA-256, SHA-384, SHA-512 sont à privilégier ;
  - une clé cryptographique chargée dans la carte à puce ne doit avoir qu'un seul type d'usage ;
  - pour les courbes elliptiques, l'ordre du groupe doit être un multiple d'un nombre premier d'au moins 200 bits jusqu'en 2020, et d'au moins 256 bits ensuite. La même exigence s'applique aux sous-groupes.

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

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

51, boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.85.80 - Télécopie 01.84.82.40.60

Annexe

Références de la qualification

[1]. Processus de qualification au niveau renforcé, version 2.0. 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 (RGS), version en vigueur. Disponible sur www.ssi.gouv.fr.

[4]. Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1). Disponible sur www.ssi.gouv.fr.

[5]. Cible de sécurité de référence pour l'évaluation : Security target for IDeal PASS V2.0.1 EAC with PACE application, version 6, référence 2016_2000018369, 29 novembre 2016, Morpho.

[6]. Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. Certifié par le BSI *(BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK)* sous la référence BSI-PP-0035-2007.

[7]. *Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE* (PACE PP), version 1.0, du 2 novembre 2011. Certifié par le BSI (*BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK*) sous la référence BSI-CC-PP-0068-V2-2011.

[8]. *Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE* (EAC PP), version 1.3.2, du 5 décembre 2012. Maintenu par le BSI (*BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK*) sous la référence BSI-CC-PP-0056-V2-2012-MA-02.

[9]. *Evaluation Technical Report* : ETR, référence LETI.CESTI.ARR.RTE.010 – v1.0, du 2 décembre 2016, CEA-LETI.

[10]. Cotation des mécanismes cryptographiques, LETI.CESTI.ARR.RT.012-v1.0, du 16 novembre 2016, CEA-LETI.

[11]. Rapport de certification ANSSI-CC-2017/06 du 16 février 2017.