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 29 AOUT 2016
N° 3471/ANSSI/SDE

QUALIFICATION AU NIVEAU RENFORCÉ

ID-One ePass Full EAC v2 MRTD sur les composants P60x144PVA/PVE en configuration :
1) PACE avec AA, CA et PACE CAM
2) EAC et PACE avec AA
3) EAC avec AA
OBERTHUR TECHNOLOGIES / NXP SEMICONDUCTORS

Annexe : Références de la qualification.

Le produit évalué est la carte à puce « *ID-One ePass Full EAC v2 MRTD sur les composants P60x144PVA/PVE en configuration :*

1. *PACE avec AA, CA et PACE CAM*
2. *EAC et PACE avec AA*
3. *EAC avec AA* »

pouvant être en mode contact ou sans contact. Le produit est développé par *OBERTHUR TECHONOLOGIES* sur un composant *NXP SEMICONDUCTORS*.

Ce produit 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 aux rapports de certification [14] à [16] à la cotation cryptographique [13] et conformément au processus de qualification [1], j'atteste que ce produit atteint le niveau de qualification renforcé, sous réserve :

- du respect des restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [14] à [16] ;
- de l'activation du mécanisme « *Active Authentication* » permettant l'authentification du microcontrôleur ;
- du respect des conditions suivantes 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 ;
  - un exposant public RSA strictement supérieur à 2^{16} doit être utilisé ;

- 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 type d'usage ;
- 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.

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

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 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]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One ePass Full EAC v2 MRTD in PACE configuration with AA, CA and PACE CAM on NXP P60x144 PVA/PVE – Security Target, version 2, référence : 110 7888, 2 mars 2016, Oberthur Technologies.

[5]. MINOS – ID-One ePass Full EAC v2 MRTD in EAC with PACE configuration with AA on NXP P60x144 PVA/PVE –Security Target, version 2, référence : 110 7887, 2 mars 2016, Oberthur Technologies.

[6]. MINOS – ID-One ePass Full EAC v2 MRTD in EAC configuration with AA on P60x144 PVA/PVE – Security Target, version 2, référence : 110 7886, 2 mars 2016, OberthurTechnologies.

[7]. Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0, 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 1.3.1, 22 mars 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 26 mars 2012 sous la référence BSI-CC-PP-0056-V2-2012-MA-0*

[9]. Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0, 2 novembre 2011. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011*

[10]. Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control, version 1.10, 25 mars 2009. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056-2009.*

[11]. Security IC Platform Protection Profile, version 1.0, août 2007.Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007

[12]. Evaluation Technical Report – MINOS MRTD, version 2.0, référence : LETI.CESTI.MIN.RTE.001, 18 mars 2016, LETI.

[13]. MINOS - Cotation des mécanismes cryptographiques, version : 2.0, référence : LETI.CESTI.MIN.RT.033, 18 mars 2016, LETI.

[14]. Rapport de certification ANSSI-CC-2016/38 du 23/06/2016

[15]. Rapport de certification ANSSI-CC-2016/39 du 23/06/2016

[16]. Rapport de certification ANSSI-CC-2016/40 du 23/06/2016