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*

Bureau Qualification et Agrément

Paris, le 10 MAI 2017
N° 2259 /ANSSI/SDE

QUALIFICATION AU NIVEAU RENFORCE

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

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit (page 2).

Fiche 2 : Conditions et limites de la qualification (page 3).

Fiche 3 : Base documentaire de la qualification (page 4).

Eu égard aux rapports de certification [4] [5] [6], à la cotation cryptographique [16] et conformément au processus de qualification [1], l'Agence nationale de la sécurité des systèmes d'information atteste que la solution « ID-ONE EPASS FULL EAC v2 MRTD » développée par *OBERTHUR TECHNOLOGIES* sur les composants P60x144PVA/PVE de *NXP SEMICONDUCTORS* atteint le niveau de qualification renforcé dans le cadre du Décret n°2010-112 du 2 février 2010 [2], sous réserve du respect des conditions d'utilisations et limites présentées en fiche 2.

Cette qualification est valable jusqu'au 29 août 2019. 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

Fiche 1

Description du produit.

Désignation et versions

Le produit qualifié est la solution « ID-ONE EPASS FULL EAC V2 MRTD » développée par *OBERTHUR TECHNOLOGIES* sur les composants P60x144PVA/PVE de *NXP SEMICONDUCTORS.*

Présentation générale

La solution « ID-ONE EPASS FULL EAC V2 MRTD » sur les composants P60x144PVA/PVE est une carte à puce en configuration :

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

Elle peut être en mode contact ou sans contact et 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.

Fiche 2

Conditions et limites de la qualification.

Conditions

C1. les restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [4] à [6] doivent être respectées ;

C2. l'activation du mécanisme « *Active Authentication* » permettant l'authentification du microcontrôleur ou du mécanisme CA *«Chip Authentication »* du protocole EAC doit être respectée ;

C3. le choix et le dimensionnement des mécanismes cryptographiques doivent respecter les conditions suivantes :

- 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.

Fiche 3

Base documentaire de la qualification

[1]. Processus de qualification d'un produit, version en vigueur.

[2]. Décret n°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

[3]. 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.

[4]. Rapport de certification ANSSI-CC-2016/38 du 23 juin 2016.

[5]. Rapport de certification ANSSI-CC-2016/39 du 23 juin 2016.

[6]. Rapport de certification ANSSI-CC-2016/40 du 23 juin 2016.

[7]. 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, du 2 mars 2016, *OBERTHUR TECHNOLOGIES.*

[8]. 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, du 2 mars 2016, *OBERTHUR TECHNOLOGIES.*

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

[10]. *Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE,* 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

[11]. *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 le 26 mars 2012 sous la référence BSI-CC-PP-0056-V2-2012-MA-0.

[12]. *Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE*, version 1.0, du 2 novembre 2011. Certifié par le BSI sous la *référence BSI-CC-PP-0068-V2-2011.*

[13]. *Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control*, version 1.10, du 25 mars 2009. Certifié par le BSI sous la référence BSI-PP-0056-2009.

[14]. *Security IC Platform Protection Profile*, version 1.0, d'août 2007.Certifié par le BSI sous la référence BSI-PP-0035-2007.

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

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