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 NOV. 2015
N° 4517 /ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

Application eTravel EAC v2.1, en configuration *EAC on SAC*, sur la carte à puce ouverte MultiApp V3.1 masquée sur le composant P60D144PVA (Version du patch : 1.3)

GEMALTO / NXP SEMICONDUCTORS

Annexe : Documents de référence de la qualification.

L'application eTravel EAC v2.1, en configuration *EAC on SAC*, sur la carte à puce MultiApp V3.1 masquée sur le composant P60D144PVA (version du patch : 1.3), en configuration ouverte, 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 [4] 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 ;
  - l'usage d'un exposant public RSA strictement supérieur à 2^{16}est recommandé ;
  - 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 être 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 reposant sur des courbes elliptiques doit être d'au moins 224 bits pour une utilisation jusqu'en 2020, et d'au moins 256 bits pour une utilisation au-delà de 2020 ;

- du respect des conditions suivantes pour l'intégration d'applets supplémentaires[1] sur la carte à puce, que l'installation soit réalisée par *GEMALTO* (installation pre-issuance) ou par le client (installation post-issuance) :
    - o la satisfaction de l'ensemble des contraintes et des exigences relatives aux propriétés de cloisonnement d'applications, imposées par la plateforme, avant leur installation effective : guides [9] et [10] ;
    - o la vérification de chaque applet conformément aux guides [11] et [12] afin de s'assurer qu'elle respecte les contraintes et exigences relatives aux propriétés de cloisonnement d'applications ;
    - o l'établissement, et la transmission au client le cas échéant, d'un rapport résultant de l'exécution de ces tâches de vérification.

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 3 ans. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

Contre-amiral [illegible]
Directeur général adjoint

[1] Une applet supplémentaire installée sur la carte à puce, même si elle respecte les contraintes et les exigences mentionnées dans cette décision, est hors du périmètre de cette qualification.
[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 V31 Delphes31 eTravel EAC Security Target, Gemalto, reference ST_D1361392, version 1.0 du 23 Avril 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-2015/39, Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme ouverte ou fermée MultiApp V3.1 masquée sur le composant P60D144PVA, (Version du patch : 1.3) du 28 Septembre 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.

[9]. Guide de développement d'applications : Rules for applications on Multiapp certified product, reference D1280572, version A00 de décembre 2012, GEMALTO.

[10]. Guide de développement d'applications sécurisées : Guidance for secure application development on Multiapp platforms, référence : D1280580, version A00 de décembre 2012, GEMALTO.

[11]. Guide pour l'autorité de vérification : Verification process of Third Party non sensitive applet loaded in POST-issuance, référence D1322491, version A00 de février 2014, GEMALTO.

[12]. Guide pour l'autorité de vérification : Verification process of GEMALTO non sensitive applet loaded in pre-issuance, Référence : D1283121, version A01 de juin 2013, GEMALTO.