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 27 NOV. 2015
N°4876/ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

Application IAS V4.2 sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D080PVC (version du patch 1.4)
Version de l'application IAS : 4.0.2.B
Version de l'application MOCA Server : 1.0
Version de la plateforme JavaCard MultiApp : 3.1
GEMALTO / NXP SEMICONDUCTORS

Annexe : Références de la qualification.

L'application IAS V4.2, dans sa version 4.0.2.B, sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D080 (patch v1.4), développée par *GEMALTO* et *NXP SEMICONDUCTORS*, permet la création et la vérification de signature électronique et offre des services de sécurité complémentaires, comme l'authentification du signataire par un code PIN ou par des données biométriques, ainsi que l'établissement de canal sécurisé entre la carte à puce et le lecteur de carte à puce.

Eu égard au rapport de certification [7] et à la cotation cryptographique [8], 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 du rapport de certification [7] ;
- du respect du guide [9] 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 jusqu'en 2030 et 3072 bits au-delà ;
  - la taille des courbes elliptiques ECDSA doit être d'au moins 200 bits pour une utilisation jusqu'en 2020 et 256 bits au-delà ;
  - l'usage d'un exposant public strictement supérieur à 2^{16} est recommandé ;
  - une même clé cryptographique chargée dans la carte à puce ne doit être affectée qu'à un seul usage (authentification ou signature par exemple);
  - la fonction de hachage SHA-1 ne doit pas être utilisée dans le cadre de la signature électronique, quel que soit le schéma de signature, RSA-PKCS#1 v1.5, RSASSA-PSS ou ECDSA ;
  - le schéma de signature ISO9796-2 [10] ne doit pas être utilisé ;

- le *Card Access Number* (CAN) doit être généré aléatoirement et être d'une longueur de 3 octets au moins ;

- 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*) :
  - 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 [11] ;
  - la vérification de chaque applet conformément aux guides [12] et [13] afin de s'assurer qu'elle respecte les contraintes et exigences relatives aux propriétés de cloisonnement d'applications ;
  - l'établissement, et la transmission au client le cas échéant, d'un rapport résultant de l'exécution de ces tâches de vérification.

En outre, la conformité du produit aux profils de protection [3] et [5], ainsi qu'aux spécifications IAS ECC [3], permet d'attester de l'aptitude du produit à satisfaire les exigences du niveau trois étoiles (***) des fonctions de sécurité « Signature » et « Authentification » du RGS [2], pour ce qui concerne respectivement le dispositif d'authentification et le dispositif sécurisé de création de signature, sous réserve que les clés d'authentification et de signature utilisées par l'application IAS ECC ne soient employées que dans des mécanismes respectivement d'authentification et de signature électronique.

Le produit est de plus déclaré apte à la protection de clés au niveau *Diffusion Restreinte*, ou classifiées au niveau *Diffusion Restreinte OTAN*, *Restreint UE/EU Restricted* ou *Diffusion Restreinte EUROCOR*.

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

[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.

Annexe

Références de la qualification

[1]. Processus de qualification au niveau renforcé, version 1.0 (disponible sur www.ssi.gouv.fr).

[2]. Référentiel Général de Sécurité version 2.0 et notamment ses annexes [RGS_A_2] (Politique de certification Type « Certificats électroniques de personne, version 3.0 du 27 février 2014) et [RGS_B_1] (Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques, version 2.03 du 21 février 2014).

[3]. Carte Européenne pour les Applications de Services Electroniques (e-Services) et d'Identité Electronique (e-ID) – IAS ECC – Spécifications techniques – Révision 1.0.1 – 21 mars 2008.

[4]. Profil de Protection « Protection Profile – Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001 ». Certifié par le BSI sous la référence BSI-PP-0005-2002.

[5]. Profil de protection « Protection Profile – Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001 ». Certifié par le BSI sous la référence BSIPP-0006-2002.

[6]. MultiApp V31 Delphes31 IAS CWA Security Target, Gemalto, reference ST_D1296546, version 1.0 du 18 octobre 2013.

[7]. Rapport de certification « Application IAS V4.2 sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D080PVC », ANSSI, ANSSI-CC-2015/08 du 10 mars 2015.

[8]. Cryptographic Mechanisms Evaluation Report – DELPHES31 – IAS Project, référence : DELPHES31_IAS_cryptography_v1.0/1.0, version 1.0 du 9/02/2014, SERMA Technologies.

[9]. Card Personalization Specification requirement for SSCD security evaluation - IAS Classic v4.0, référence IACv4_001_CPS_Req_For_CC_Evaluation, version 1.4 du 27 juin 2013, GEMALTO.

[10]. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2 : integer factorization based mechanisms – oct. 2002.

[11]. Rules for applications on Multiapp certified product, Référence : D1280572, version A00 de décembre 2012, GEMALTO.

[12]. Verification process of Third Party non sensitive applet loaded in pre-issuance, Référence : D1283120, version A00 de janvier 2012, GEMALTO.

[13]. Verification process of Gemalto non sensitive applet loaded in pre-issuance, Référence : D1283121, version A01 de juin 2013, GEMALTO.