



PREMIER MINISTRE

Secrétariat général  
de la défense  
et de la sécurité nationale  
*Agence nationale de la sécurité  
des systèmes d'information*

Paris, le 01 MARS 2016

N° 832/ANSSI/SDE/PSS/BQA

## QUALIFICATION AU NIVEAU RENFORCÉ

### **Application IAS V4.2.0.B sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144PVA (version du patch 1.3)**

Version de l'application IAS : 4.2.0.B

Version de l'application MOCA Server : 1.0

Version de la plateforme JavaCard MultiApp : 3.1

*GEMALTO / NXP SEMICONDUCTORS*

#### Annexe : Références

L'application IAS V4.2, dans sa version 4.2.0.B, sur la plateforme JavaCard ouverte MultiApp V3.1 masquée sur le composant P60D144 PVA (patch v1.3), 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 aux rapports de certification [13] et [14], à la cotation cryptographique [7] et conformément au processus de qualification [1], j'atteste que ce produit atteint le niveau de qualification renforcé, sous réserve :

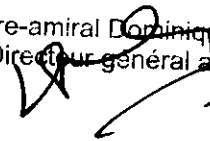
- du respect du guide [8] concernant le choix et le dimensionnement des mécanismes cryptographiques et notamment :
  - o la taille des modules RSA doit être d'au moins 2048 bits pour une utilisation jusqu'en 2030 et 3072 bits au-delà ;
  - o la taille des courbes elliptiques ECDSA doit être d'au moins 200 bits pour une utilisation jusqu'en 2020 et 256 bits au-delà ;
  - o la taille recommandée de l'exposant public est strictement supérieure à  $2^{16}$  ;
  - o une même clé cryptographique chargée dans la carte à puce ne doit être affectée qu'à un seul usage (chiffrement ou signature par exemple) ;
  - o 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 ;
  - o le schéma de signature ISO9796-2 [10] ne doit pas être utilisé ;
  - o 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<sup>1</sup> sur la carte à puce, que l'installation soit réalisée par *GEMALTO* (installation *pre-issuance*) ou par le client (installation *post-issuance*) :
  - o l'ensemble des contraintes et des exigences relatives aux propriétés de cloisonnement d'applications, imposées par la plateforme, avant leur installation effective [10] doit être satisfait ;
  - o chaque applet doit être vérifiée 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 un rapport résultant de l'exécution de ces tâches de vérification doit être établi et transmis au client le cas échéant.

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].

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

Contre-amiral Dominique RIBAN  
Directeur général adjoint



---

<sup>1</sup> 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**

- [1]. Processus de qualification au niveau renforcé, version 1.0 (disponible sur [www.ssi.gouv.fr](http://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\_D1371562, version 1.0 de Juillet 2015.
- [7]. Cryptographic Mechanisms Evaluation Report – DELPHES31 – IAS Project, référence : DELPHES31\_IAS\_cryptography\_v1.0/1.0, version 1.0 du 19/02/2014, *SERMA TECHNOLOGIES*.
- [8]. 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*.
- [9]. Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2 : integer factorization based mechanisms – oct. 2002.
- [10]. Rules for applications on Multiapp certified product, Référence : D1280572, version A00 de décembre 2012, *GEMALTO*.
- [11]. Verification process of Third Party non sensitive applet loaded in pre-issuance, Référence : D1283120, version A00 de janvier 2012, *GEMALTO*.
- [12]. Verification process of Gemalto non sensitive applet loaded in pre-issuance, Référence : D1283121, version A01 de juin 2013, *GEMALTO*.
- [13]. Rapport de certification ANSSI-CC-2016/03 du 09/02/2016.
- [14]. Rapport de certification ANSSI-CC-2016/04 du 09/02/2016.