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 03 JAN. 2017
N° 14 /ANSSI/SDE

QUALIFICATION AU NIVEAU RENFORCÉ

Applet ID.me 1.28 on IdealCitiz MOSID v2.1.1
sur composant Infineon M7892/93 B11
SAFRAN IDENTITY & SECURITY / INFINEON TECHNOLOGIES AG

Annexe : Références de la qualification.

Le produit « Applet ID.me 1.28 (SSCD) en composition sur plate-forme Java ouverte IDeal Citiz MOSID V2.1.1 » en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-5, SSCD-6, sur les composants M7892/93 B11, est un dispositif sécurisé de création de signature électronique pouvant être en mode contact ou sans contact. Le produit est développé par *SAFRAN IDENTITY & SECURITY* sur un composant *INFINEON TECHNOLOGIES AG*.

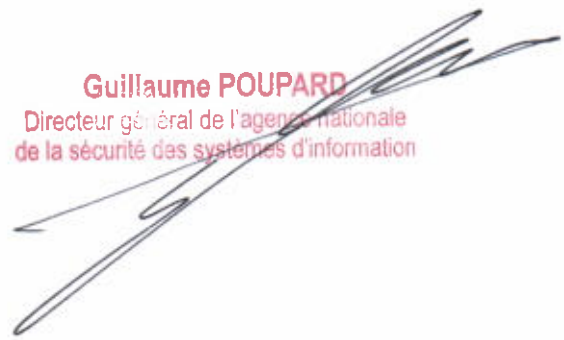
Eu égard au rapport de certification [10], à la cotation cryptographique [11] et conformément au processus de qualification [1], j'atteste que ce produit atteint le niveau de **qualification renforcé**, sous réserve :

- du respect des restrictions d'usage figurant aux chapitres 2.3 et 3.2 du rapport de certification [12] ;
- 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.

En outre, la conformité du produit aux profils de protection [5] à [8] permet d'attester de l'aptitude du produit à satisfaire les exigences relatives aux dispositifs de création de signature électronique qualifiés :

- du référentiel général de sécurité [2] pour le niveau trois étoiles (***) ;
- du règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement eIDAS [3].

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]. Référentiel Général de Sécurité, versions 1.0 et 2.0.

[3]. Règlement européen n'910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE

[4]. Cible de sécurité de référence pour l'évaluation : Security target ID.me 1.28 on IdealCitiz MOSID v2.1.1- Security Target, version 6, référence : 2016_2000016084, 16 octobre 2016, Morpho.

[5]. Protection profiles for secure signature creation device — Part 2: Device with key Generation - BSI-CC-PP-0059-2009-MA-01, Version 2.0.1, February 2012.

[6]. Protection profiles for secure signature creation device – Part3: Device with key import BSI-CC-PP-0075-2012, Version 1.0.2, September 2012

[7]. Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application BSI-CC-PP-0071-2012, Version 1.0.1, December 2012.

[8]. Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application BSI-CC-PP-0072-2012, Version 1.0.1, December 2012.

[9]. Protection profiles for secure signature creation device – Part6: Extension for device with key import and trusted communication with signature-creation application BSI-CC-PP-0076-2013, Version 1.0.4, April 2013.

[10]. Evaluation Technical Report – LETI.CESTI.CDR.RTE.1, version 1.2, 3 novembre 2016, Leti.

[11]. Application ID.me, LETI.CESTI.CDR.RT.004, v1.0, 30 juin 2016, Leti.

[12]. Rapport de certification ANSSI-CC-2016/70 du 15/11/2016.