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 10 JUIN 2016
N° 2309 /ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

ID-One eIDAS v1.0 en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-5, SSCD-6 sur les composants P60x080PVC/PVG
OBERTHUR TECHNOLOGIES / NXP SEMICONDUCTORS

Annexe : Références de la qualification.

La carte à puce ID-One eIDAS v1.0 en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-5, SSCD-6, sur les composants P60x080PVC/PVG, est un dispositif sécurisé de création de signature électronique pouvant être en mode contact ou sans contact. Le produit est développé par *OBERTHUR TECHONOLOGIES* sur un composant *NXP SEMICONDUCTORS*.

Eu égard aux rapports de certification [12] à [16], à la cotation cryptographique [11] et conformément au processus de qualification [1], j'atteste que ce produit, dans ses différentes configurations, atteint le niveau de qualification renforcé, sous réserve :

- du respect des restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [12] à [16] ;
- 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 ;
  - il est recommandé d'utiliser un exposant public RSA strictement supérieur à 2^{16} ;
  - 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 au profil de protection [9] permet d'attester de l'aptitude du produit à satisfaire les exigences relatives aux dispositifs de création de signature électronique et à créer des signatures qualifiées dans le cadre du référentiel général de sécurité [2] pour le niveau trois étoiles (***).

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

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Tél 01.71.75.82.25 – Télécopie 01.84.82.40.60

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 : MINOS – ID-One eIDAS v1.0 in SSCD-2 configuration Security Target, version 6, référence : 110 7676, 2 mars 2016, Oberthur Technologies.

[5]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-3 configuration Security Target, version 4, référence : 110 7732, 2 mars 2016, Oberthur Technologies.

[6]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-4 configuration Security Target, version 4, référence : 110 7733, 2 mars 2016, Oberthur Technologies.

[7]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-5 configuration Security Target, version 4, référence : 110 7734, 2 mars 2015, Oberthur Technologies.

[8]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-6 configuration Security Target, version 4, référence : 110 7735, 2 mars 2015, Oberthur Technologies.

[9]. Protection profile for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.

[10]. Evaluation Technical Report – MINOS-eSign, version : 2.2, référence : LETI.CESTI.MIN.RTE.002 v2.2, 14 avril 2016, LETI.

[11]. MINOS - Cotation des mécanismes cryptographiques, version : 2.0, référence : LETI.CESTI.MIN.RT.004, 1 avril 2016, LETI.

[12]. Rapport de certification ANSSI-CC-2016/17 du 12/05/2016.

[13]. Rapport de certification ANSSI-CC-2016/18 du 12/05/2016.

[14]. Rapport de certification ANSSI-CC-2016/19 du 12/05/2016.

[15]. Rapport de certification ANSSI-CC-2016/20 du 12/05/2016.

[16]. Rapport de certification ANSSI-CC-2016/21 du 12/05/2016.