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 30 AOUT 2016
N° 3501 /ANSSI/SDE

QUALIFICATION AU NIVEAU RENFORCÉ

ID-One eIDAS v1.0 en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-5, SSCD-6 sur les composants P60x144PVA/PVE
OBERTHUR TECHNOLOGIES / NXP SEMICONDUCTORS

Annexe : Références de la qualification.

Le produit évalué est la carte à puce « ID-One eIDAS v1.0 en configuration SSCD-2, SSCD-3, SSCD-4, SSCD-5, SSCD-6, sur les composants P60x144PVA/PVE 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 [16] à [20], à la cotation cryptographique [15] 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 des rapports de certification [16] à [20] ;
- 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 [9] à [13] 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 (***).

En outre, la conformité du produit aux profils de protection [9] à [13] 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 : MINOS – ID-One eIDAS v1.0 in SSCD-2 configuration on NXP P60x144 PVA/PVE - Security Target, version 3, référence : 110 7844, 2 mars 2016, Oberthur Technologies.

[5]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-3 configuration on NXP P60x144 PVA/PVE Security Target, version 2, référence : 110 7845, 2 mars 2016, Oberthur Technologies.

[6]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-4 configuration on NXP P60x144 PVA/PVE - Security Target, version 2, référence : 110 7846, 2 mars 2016, Oberthur Technologies.

[7]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-5 configuration on NXP P60x144 PVA/PVE - Security Target, version 2, référence : 110 7847, 2 mars 2016, Oberthur Technologies.

[8]. Cible de sécurité de référence pour l'évaluation : MINOS – ID-One eIDAS v1.0 in SSCD-6 configuration on NXP P60x144 PVA/PVE - Security Target, version 2, référence : 110 7848, 2 mars 2016, Oberthur Technologies.

[9]. Protection profiles 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]. Protection profiles for secure signature creation device – Part 3: Device with key import, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.

[11]. Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012.

[12]. Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012.

[13]. Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, référence : prEN 14169-6:2013, version 1.0.4 datée du 3 avril 2013.

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

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

[16]. Rapport de certification ANSSI-CC-2016/26 du 03/06/2016

[17]. Rapport de certification ANSSI-CC-2016/27 du 03/06/2016

[18]. Rapport de certification ANSSI-CC-2016/28 du 03/06/2016

[19]. Rapport de certification ANSSI-CC-2016/29 du 03/06/2016

[20]. Rapport de certification ANSSI-CC-2016/30 du 03/06/2016