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 20 DEC. 2019
N°4828 /ANSSI/SDE/PSS/BQA

DECISION DE CERTIFICATION DE CONFORMITE D'UN DISPOSITIF DE CREATION DE SIGNATURE ELECTRONIQUE ET DE CACHET ELECTRONIQUE QUALIFIE

NXP SEMICONDUCTORS

Mikron-Weg 1
A-8101 Gratkorn
Austria

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information,

Vu le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 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, notamment l'alinéa 1 de son article 30 et l'alinéa 2 de son article 39 ;

Vu la décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'alinéa 3 de l'article 30, et à l'alinéa 2 de l'article 39, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », notamment son article 1er ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu le courrier du Secrétariat général des affaires européennes à Monsieur l'ambassadeur représentant permanent de la France auprès de l'Union européenne en date du 29 avril 2016, référence ITEC/2016/0529, informant qu'en application des articles 30 et 39 du règlement (UE) n° 910/2014 du 23 juillet 2014, l'Agence nationale de la sécurité des systèmes d'information est désignée comme organisme certificateur ;

Vu les exigences de l'ANSSI formulées dans le document « Dispositifs de création de signature / cachet électronique qualifiés – certification de la conformité au règlement *EIDAS* », version en vigueur ;

Vu le rapport de certification : ANSSI-CC-2017/64 du 20 novembre 2017,

Décide :

Art. 1er – Le produit *CHIPDOC P60 ON JCOP 3 SECID P60 (OSB) SSCD CHARGE SUR COMPOSANT P6022J VB* en version V7b4_2 développé par la société *NXP SEMICONDUCTORS* est certifié conforme aux exigences fixées par les articles 29 et 39 du règlement (UE) n° 910/2014 pour les dispositifs de création de signature et de cachet électronique qualifiés[1].

Art. 2 – Le produit doit être utilisé conformément aux conditions et restrictions d'utilisation définies dans le rapport de certification et à celles identifiées en annexe.

Art. 3 – La présente décision est valable dix ans à compter de la décision de certification du produit selon les Critères Communs, à savoir jusqu'au 20 novembre 2027.

Art. 4 – La présente décision est conditionnée au respect par la société *NXP SEMICONDUCTORS* :

- des engagements relatifs au suivi de sécurité du produit pris par la société au titre de sa demande de certification, conformément à l'annexe 2 du document « Dispositifs de création de signature / cachet électronique qualifiés – certification de la conformité au règlement *EIDAS* » ;
- à la fourniture à l'ANSSI du certificat de surveillance au plus tard cinq ans après la décision de certification du produit selon les Critères Communs, à savoir le 20 novembre 2022.

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

[1] Conformément au rapport de maintenance BSI-CC-PP-0059-2009-MA-02 et au rapport de certification BSI-CC-PP-0075-2012-MA-01, les profils de protection référencés dans le rapport de certification sont équivalents à ceux référencés dans la décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016.

Annexe 1

Conditions d'utilisation du dispositif de création de signature électronique et de cachet électronique

La décision de certification de conformité est valide sous réserve du respect des conditions et limites énoncées ci-après.

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

C1. Les restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [CERTIF] sont bien respectées, en particulier l'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans les cibles de sécurité [CDS].

C2. Les guides d'installation et d'utilisation [GUIDES] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie.

C3. La fonction de hachage SHA-256 peut être utilisée pour les mécanismes de signature.

C4. Le mécanisme d'intégrité du Secure Messaging basé sur le TDES peut être utilisé jusqu'en 2020 uniquement, et ce à condition que moins de 2^{27} calculs de MACs soient effectués par ce mécanisme pour une clé donnée.

C5. Le mécanisme de confidentialité du Secure Messaging basé sur le TDES peut être utilisé jusqu'en 2020 uniquement.

C6. Le mécanisme d'intégrité du Secure Messaging basé sur l'AES peut être utilisé à condition que moins de 2^{27} calculs de MACs soient effectués par ce mécanisme pour une clé donnée.

C7. Le mécanisme de confidentialité du Secure Messaging basé sur l'AES peut être utilisé.

C8. Le mécanisme de génération de nombres aléatoires basé sur le générateur matériel de nombres aléatoires et le post-traitement SP800-90A peut être utilisé.

C9. Les mécanismes d'initialisation et de gestion de PIN (*Reference Authentication Data*) peuvent être utilisés.

C10. Le mécanisme de génération de clés RSA peut être utilisé jusqu'en 2030 :

- si la taille minimale du module et de l'exposant privé RSA est d'au moins 2048 bits ;
- si l'exposant public est supérieur ou égal à $2^{16}+1$.

C11. Le mécanisme de calcul de signature RSA peut être utilisé jusqu'en 2030 :

- si la taille minimale du module et de l'exposant privé RSA est d'au moins 2048 bits ;
- si l'exposant public est supérieur ou égal à $2^{16}+1$;
- si le bi-clé utilisé est dédié à ce calcul de signature.

Limites

L1. Seules les fonctions décrites dans la fiche 1 sont couvertes par la présente décision de qualification.

L2. La fonction de hachage SHA-1 ne doit pas être utilisée pour les mécanismes de signature.

Annexe 2

Base documentaire

[CRYPTO_RE]	Analysis of Cryptographic Mechanisms : ChipDoc V2 Reevaluation, version 2.0, référence : ChipDoc_V2_RE_CRY, 13 novembre 2019, Thales.
[PP_IAS_ECC]	Profil de protection, *Protection profiles for secure signature creation device — Part 2: Device with key generation,* - version : 2.01 - certifié par le BSI - référence : BSI-CC-PP-0059- 2009-MA-01 - en date du : 23 janvier 2012 Profil de protection, *Protection profiles for secure signature creation device — Part 3: Device with key import,* - version : 1.0.2 - certifié par le BSI - référence : BSI-CC-PP-0075 - en date du : 24 juillet 2012
[CERTIF]	Rapport de certification : ChipDoc P60 on JCOP 3 SECID P60 (OSB) SSCD masqué sur composant P6022J VB (version v7b4), 20/11/2017, ANSSI-CC-2017/64.
[CDS]	Cible de sécurité de référence : ChipDoc V2 on JCOP 3 P60 in SSCD configuration, v1.2, 26/03/2019, *NXP*.
[GUIDES]	Guides du produit : - ChipDoc v7b4 applet in SSCD configuration – Preparation and Operation Manual, version 1.7, reference 414217, *NXP* ; - ChipDoc v7b4 applet SSCD – Personalization guide, version 1.4, reference 407014, *NXP*.