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 31 AOUT 2018
N° 16361 /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 ;

51, boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél +33.1.71.75.82.78 - Fax +33.1.84.82.40.60

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 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

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 énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

C1. la fonction de hachage SHA-1 n'est pas utilisée pour les mécanismes de signature ;

C2. la taille des modules et exposants privés RSA et des paramètres de la cryptographie à base de corps est suffisante (la taille du module et de l'exposant privé RSA est d'au moins 2048 bits) ;

C3. la taille des exposants privés RSA n'est pas inférieure à celle des modules ;

C4. un exposant public RSA trop petit n'est pas utilisé (l'exposant public doit être supérieur ou égal à $2^{16}+1$) ;

C5. l'authentification externe avec un chiffrement TDES n'est pas utilisée.