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 03 DEC 2018
N°17868 /ANSSI/SDE/PSS/BQA

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

NXP SEMICONDUCTORS GERMANY GMBH
HRB 84 865

Troplowitzstr 20
22529 Hamburg
Germany

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-2016/63 du 2 novembre 2016 ;

Vu la décision de certification de conformité n° 10248/ANSSI du 19 janvier 2018 ;

Vu le rapport de maintenance ANSSI-CC-2016/63-M02 du 5 octobre 2018,

Décide :

Art. 1er – Le produit *NXP ASEPCOS-CNS v1.84 in SSCD configuration with patch PL07 on NXP P60D080PVG dual interface microcontroller* développé par la société *NXP Semiconductors Germany GmbH* 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] sous réserve du respect des conditions d'utilisation énoncées en annexe.

Art. 2 – La présente décision est valable jusqu'au 31 décembre 2020.

Art. 3 – La présente décision est conditionnée au respect par la société *NXP Semiconductors Germany GmbH* 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* ».

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

[1] Conformément aux rapports de maintenance BSI-CC-PP-0059-2009-MA-02 et 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) n° 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. Les restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification 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 ;

C2. Les guides d'installation et d'utilisation 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. Les fonctions de hachage SHA-1 et RIPEMD-160 ne sont pas utilisées pour les mécanismes de signature ;

C4. Le mécanisme d'*EXTENDED SECURE MESSAGING* utilisant le TDES est utilisable jusqu'en 2020 uniquement ;

C5. Le mécanisme de génération de nombres aléatoires mis en œuvre est basé sur le générateur matériel de nombres aléatoires et le post-traitement utilisant le SHA-256 ;

C6. Les mécanismes d'initialisation et de gestion de PIN (*Reference Authentication Data*) sont utilisables ;

C7. Le mécanisme de génération de clés RSA est utilisable jusqu'en 2030 si :

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

C8. Le mécanisme de calcul de signature RSA est utilisable jusqu'en 2030 si :

- la taille minimale du module et de l'exposant privé RSA est d'au moins 2048 bits ;
- l'exposant public est supérieur ou égal à $2^{16}+1$;
- la fonction de hachage SHA-256 est utilisée ;

C9. Le mécanisme de *STANDARD SECURE MESSAGING* n'est pas utilisé ;

C10. Le mécanisme d'*EXTENDED SECURE MESSAGING* utilisant l'AES n'est pas utilisé car il ne fait pas partie du périmètre d'évaluation du produit.