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

Bureau Qualifications et Agréments

Paris, le 20 DEC. 2019
N° 4825 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU RENFORCE

***CHIPDOC P60 ON JCOP 3 SECID P60 (OSB) SSCD CHARGE SUR COMPOSANT P6022J VB* en version V7b4_2**

NXP SEMICONDUCTORS FRANCE

Route de l'orme des merisiers, parc des algorithmes
91190 Gif-sur-Yvette
France

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 3 : Base documentaire de la qualification.

Le Premier ministre,

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

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 la décision du 22 octobre 2014 portant délégation de signature (secrétariat général de la défense et de la sécurité nationale) ;

Vu le processus de qualification d'un produit, référence QUAL-PROD-PROCESS, version en vigueur ;

Vu le dossier de demande de qualification d'un produit fourni par la société *NXP* le 29 mars 2019,

Décide :

Art. 1er – Le produit fourni par la société *NXP* portant le nom *CHIPDOC P60 ON JCOP 3 SECID P60 (OSB) SSCD CHARGE SUR COMPOSANT P6022J VB* en version V7b4_2 respecte les règles fixées par le décret n° 2010-112 du 2 février 2010 et est qualifié au niveau renforcé sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

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

Art. 3 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

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

Fiche 1

Description du produit

Désignation et versions

Le produit qualifié est la solution « *ChipDoc P60 on JCOP 3 Secid P60 (OSB) SSCD* » en version V7b4_2 développée par l'entreprise *NXP Semiconductors* sur le composant *NXP P6022J VB*.

Présentation générale

La solution « *ChipDoc P60 on JCOP 3 Secid P60 (OSB) SSCD* » en version V7b4_2 sur le composant *NXP P6022J VB* propose la configuration suivante :

- dispositif avec génération de clé et importation de clé, avec une stricte conformité aux profils de protection :
  - BSI-CC-PP-0059-2009-MA-01 v2.0.1 ;
  - BSI-CC-PP-0075 v1.0.2.

Le produit est développé par *NXP Semiconductors*.

Les principaux services de sécurité fournis par le produit sont :

- la gestion du PIN afin d'authentifier le signataire ou l'administrateur ;
- l'importation et la génération des clés (SCD, SVD) ;
- l'ouverture d'un canal de confiance avec les entités externes (SCA, CGA) et la gestion du canal de confiance avec les entités externes (SCA, CGA) assurant l'intégrité et la confidentialité des échanges ;
- la fourniture d'une signature électronique conformément aux exigences des profils de protection BSI-CC-PP-0059-2009-MA-01, BSI-CC-PP-0075 ;
- l'export de la clé SVD pour la génération du certificat correspondant.

Fiche 2

Conditions et limites de la qualification

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 uniquement 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.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, version 1.0 du 06 janvier 2017. Disponible sur http://www.ssi.gouv.fr.
[RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Disponible sur http://www.legifrance.gouv.fr.

Documents rédigés par le centre d'évaluation : *THALES*

[CRYPTO_RE]	Analysis of Cryptographic Mechanisms : ChipDoc V2 Reevaluation, version 2.0, référence : ChipDoc_V2_RE_CRY, 13 novembre 2019, Thales.

Référentiels et standards

[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

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[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.

Guides d'utilisation et documentations techniques de l'industriel

[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*.