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

Rapport de maintenance ANSSI-CC-2016/63-M02

NXP ASEPCOS-CNS v1.84 in SSCD Configuration on NXP P60D080PVG Dual Interface Microcontroller Patch PL07

Certificat de référence : ANSSI-CC-2016/63

Paris, le 5 octobre 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

1. Références

[CER]	Rapport de certification ANSSI-CC-2016/63, NXP ASEPCOS-CNS v1.84 in SSCD Configuration on NXP P60D080PVG Dual Interface Microcontroller, 2 novembre 2016, référence ANSSI-CC-2016/63.
[MAI]	Procédure ANSSI-CC-MAI-P-01 Continuité de l'assurance.
[R-M01]	Rapport de maintenance ANSSI-CC-2016/63-M02, NXP ASEPCOS-CNS v1.84 in SSCD Configuration on NXP P60D080PVG Dual Interface Microcontroller, Patch PL01, 15 juin 2017.
[IAR]	NXP Secure Smart Card ASEPCOS-CNS v1.84, Impact Analysis Report – Card Reset Sequence Change, revision 0.3, 15 mai 2018, *NXP SEMICONDUCTORS*.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[CCRA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, 2 juillet 2014.

2. Identification du produit maintenu

Le produit « NXP ASEPCOS-CNS v1.84 in SSCD Configuration on NXP P60D080PVG Dual Interface Microcontroller » a été initialement certifié sous la référence ANSSI-CC-2016/63 (référence [CER]).

Il a déjà fait l'objet d'une maintenance sous la référence ANSSI-CC-2016/63-M01 (référence [R-M01]).

Le produit objet de la présente maintenance est « NXP ASEPCOS-CNS v1.84 in SSCD Configuration on NXP P60D080PVG Dual Interface Microcontroller, patch PL07 » développé par la société *NXP SEMICONDUCTORS*.

Le patch est identifiable par l'utilisation de la commande GET DATA suivant la procédure d'application fournie par le développeur (référence [GUIDES]). La valeur de l'élément TAG_PDO_CODE_CRC32 (étiquette[1] « 0118 », sous-étiquette « 9D04 ») du produit maintenu est « 71 AC 9A 60». Les autres données d'identification restent inchangées par rapport au certificat initial (référence [CER]) et à la précédente maintenance (référence [R-M01].

[1] *Tag.*

3. Description des évolutions

Le rapport d'analyse d'impact de sécurité (référence [IAR]) mentionne que les modifications suivantes ont été opérées :

- désactivation du mécanisme de ticket pour le MOC (*Match-On-Card*) ;
- optimisation de la mémoire en déplaçant le mécanisme de protection en intégrité « *Recovery from interrupted 4BG transactions* » dans les couches basses du code et en désactivant le mécanisme *read-before-write*.

4. Fournitures applicables

Le tableau ci-dessous liste les fournitures, notamment les guides applicables au produit maintenu. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du document correspondant. En particulier, [R-M02] référence la présente maintenance.

[GUIDES]	NXP ASEPCOS-CNS v1.84 - Card Reference Manual Part 1 : Generic Guidance, version 1.2, 3 mai 2018, *NXP SEMICONDUCTORS.*	[R-M02]
	NXP ASEPCOS-CNS P60 - Card Reference Manual - Part 2 : Dedicated Guidance, version 1.1, 13 mai 2016, *NXP SEMICONDUCTORS.*	[CER]
	ASEPCOS-CNS P60 - Card Reference Manual - User manual, version 1.2, 5 mai 2018, *NXP SEMICONDUCTORS.*	[R-M02]
[ST]	Cible de sécurité de référence : - ASEPCOS-CNS v1.84 - NXP ASEPCOS-CNS v1.84 in SSCD Configuration – Security Target, version 1.2, 4 mai 2018 *NXP SEMICONDUCTORS* ; Version publique de la cible : - ASEPCOS-CNS v1.84 - NXP ASEPCOS-CNS v1.84 in SSCD Configuration – Security Target Lite, version 1.2, 4 mai 2018, *NXP SEMICONDUCTORS.*	[R-M02]
[CONF]	ASEPCOS-CNS v1.84 Configuration Lists, version 1.4, 16 mai 2018, *NXP SEMICONDUCTORS.*	[R-M02]

5. Conclusions

Les évolutions listées ci-dessus sont considérées comme ayant un impact mineur. Le niveau de confiance dans cette nouvelle version du produit est donc identique à celui de la version certifiée.

Les évolutions mineures du présent produit ne remettent pas en cause les évaluations menées en composition sur ce produit.

6. Avertissement

Le niveau de résistance d'un produit certifié se dégrade au cours du temps. L'analyse de vulnérabilité de cette version du produit au regard des nouvelles attaques apparues depuis l'émission du certificat n'a pas été conduite dans le cadre de cette maintenance. Seule une réévaluation ou une surveillance de cette nouvelle version du produit permettrait de maintenir le niveau de confiance dans le temps.

7. Reconnaissance du certificat

Ce rapport de maintenance est émis en accord avec le document : « Assurance Continuity : CCRA Requirements, version 2.1, June 2012 ».

Reconnaissance européenne (SOG-IS)

Le certificat initial a été émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Reconnaissance internationale critères communs (CCRA)

Le certificat initial a été émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.
[2] Les pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr