PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de maintenance
ANSSI-CC-2019/62-M01

P73N2M0B0.2C2/2C6

Certificat de référence : ANSSI-CC-2019/62

Paris le 10 Février 2023

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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.

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

1 Références

[CER]	Rapport de certification ANSSI-CC-2019/62, P73N2M0B0.2C2/2C6, 24 décembre 2019.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2019/62-S01, P73N2M0B0.2C2/2C6, 17 novembre 2020.
[R-S02]	Rapport de surveillance ANSSI-CC-2019/62-S02, P73N2M0B0.2C2/2C6, 14 janvier 2022.
[R-S03]	Rapport de surveillance ANSSI-CC-2019/62-S03, P73N2M0B0.2C2/2C6.
[IAR]	P73N2M0B0.2 Product Update F, Impact Analysis Report, Rev 1.1, 15 décembre 2022, NXP SEMICONDUCTORS.
[RM-Lab]	Surveillance Technical Report P732C6 project, P732C6_STR_v3.1, 12 janvier 2023, SERMA SAFETY & SECURITY.
[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 objet de la présente maintenance est « P73N2M0B0.2C2/2C6 » développé par la société NXP SEMICONDUCTORS.

Le produit a été initialement certifié sous la référence ANSSI-CC-2019/62 (référence [CER]).

3 Description des évolutions

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

- Clarifications relatives à SHA-1 et à la taille minimale de clefs RSA dans la cible de sécurité [ST] et dans les [GUIDES] ;
- Mise à jour du cycle de vie suivant les modifications de sites opérées.

Le CESTI en charge de l'évaluation initiale a émis un rapport (référence [RM-Lab]) pour réévaluer les composants d'assurance ALC impactés par l'évolution du cycle de vie du produit.

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-M01] référence la présente maintenance.

[ST]	*P73N2M0B0.2C2/2C6 (R2) Security Target, rev 3.6, 15 décmbre 2022, NXP ;* *P73N2M0B0.2C2/2C6 (R2) Security Target Lite, rev 3.6, 15 décmbre 2022, NXP.*	[R-M01]
[GUIDES]	*P73N2M0 High-performance secure controller, DocID 297432*, 5 juillet 2019, NXP.	[CER]
	P73N2M0B Wafer and delivery specification, DocID 328231, 27 avril 2018, NXP.	[CER]
	P73 family, SC300 User manual, DocID 341410, 12 août 2015, NXP.	[CER]
	ARMv-7-M Architecture Reference Manual, ARM DDI 0403E.b ID120114, 2 septembre 2015, ARM	[CER]
	P73 family, DMA Controller PL080 User manual, DocID 341510, 18 août 2015, NXP.	[CER]
	FLASH Service Architecture Overview NVM-resident Firmware Specification, Rev 1.0, 6 juin 2016, NXP.	[CER]
	P73N2M0B0.200 Information on Guidance and Operation, rev 1.01, 18 avril 2017, NXP.	[CER]
	P73 Services User Manual, API and Operational Guidance, Revision 2.0, 13 avril 2017, NXP	[CER]
	P73N2M0 Crypto Library : Information on Guidance and Operation, DocID 402813, NXP.	[R-M01]
	P73N2M0 Crypto Library : User Manual – RNG Library, DocID 401410, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – SHA Library, DocID 401710, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – Secure SHA Library, DocID 401810, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – SHA-3 Library, DocID 402010, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – Secure SHA-3 Library, DocID 402110, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – HASH Library, DocID 403810, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – HMAC Library, DocID 401310, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – Rsa Library (RSA), DocID 401510, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – RSA Key Generation Library (RsaKg), DocID 401610, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – ECC over GF(p) Library, DocID 401210, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – ECDAA, DocID 402410, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual –Utils Library, DocID 402210, NXP.	[CER]

	P73N2M0 Crypto Library : User Manual – Symmetric Cipher Library (SymCfg), DocID 401110, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – Korean SEED Library, DocID 402310, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – FELICA, Version 1.0, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – OSCCA-SM2 over GF(p) Library, DocID 402510, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – OSCCA-SM3 Library, DocID 402610, NXP.	[CER]
	P73N2M0 Crypto Library : User Manual – OSCCA-SM4 Library, DocID 402710, NXP.	[CER]

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 Reconnaissance du certificat

Reconnaissance européenne (SOG-IS)

Ce certificat est 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 puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. 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.eu.

Reconnaissance internationale critères communs (CCRA)

Ce certificat est 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 :

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