



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de surveillance ANSSI-CC-2018/55-S03

P73N2M0B0.2C2

Certificat de référence : ANSSI-CC-2018/55

Paris, le 14 janvier 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]



AVERTISSEMENT

La surveillance du produit ne constitue pas en soi une recommandation d'utilisation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit soit totalement exempt de vulnérabilités exploitables.

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

La reproduction de ce document sans altération ni coupure est autorisée.

1 Références

[CER]	Rapport de certification ANSSI-CC-2018/55, P73N2M0B0.2C2, 14 décembre 2018.
[SUR]	Procédure : Surveillance des produits certifiés, référence ANSSI-CC-SUR-P-01.
[R-S01]	Rapport de surveillance ANSSI-CC-2018/55-S01, P73N2M0B0.2C2, 22 novembre 2019.
[R-S02]	Rapport de surveillance ANSSI-CC-2018/55-S02, P73N2M0B0.2C2, 17 novembre 2020.
[RS-Lab]	<i>Surveillance Technical Report, P73_P73CL_P73A_P73B_P732C6_STR_v2.0</i> , 7 décembre 2021, SERMA SAFETY & SECURITY.
[ETR_COMP]	Pour le besoin des évaluations ou surveillances en composition avec ce produit le rapport technique pour la composition a été mis à jour : <i>Surveillance Technical Report Lite for Composition, P73_P73CL_P73A_P73B_P732C6_STR_Lite_v2.0</i> , 7 décembre 2021, SERMA SAFETY & SECURITY.

2 Décision

Le rapport de surveillance [RS-Lab], transmis par le centre d'évaluation SERMA SAFETY & SECURITY, permet d'attester que le produit « P73N2M0B0.2C2 », initialement certifié sous la référence [CER], peut être considéré comme résistant à des attaques de niveau AVA_VAN.5 dans les mêmes conditions et restrictions d'usage que celles définies dans [CER], complétées par les recommandations sécuritaires additionnelles intégrées au fil des surveillances successives dans [GUIDES].

Le rapport d'évaluation pour composition [ETR_COMP] a été mis à jour pour refléter les résultats de cette dernière surveillance.

Le rapport de surveillance [RS-Lab] permet également d'attester que le cycle de vie du produit est conforme aux composants de la classe ALC définis dans [CER].

La périodicité de la surveillance de ce produit est de 1 an.

3 Guides applicables

Le tableau ci-dessous liste les guides applicables du produit évalué. La dernière colonne identifie l'origine de la prise en compte par l'ANSSI du guide correspondant.

Les guides ne contiennent pas de nouvelle recommandation sécuritaire par rapport à la précédente surveillance.

[GUIDES]	<i>P73N2M0 High-performance secure controller, DocID 297432, 5 juillet 2019, NXP.</i>	[R-S01]
	<i>P73N2M0B Wafer and delivery specification, DocID 328231, 27 avril 2018, NXP.</i>	[CER]
	<i>P73 family, SC300 User manual, DocID 341410, 12 août 2015, NXP.</i>	[CER]
	<i>ARMv-7-M Architecture Reference Manual, ARM DDI 0403E.b ID120114, 2 septembre 2015, ARM</i>	[CER]
	<i>P73 family, DMA Controller PL080 User manual, DocID 341510, 18 août 2015, NXP.</i>	[CER]
	<i>FLASH Service Architecture Overview NVM-resident Firmware Specification, Rev 1.0, 6 juin 2016, NXP.</i>	[CER]
	<i>P73N2M0B0.200 Information on Guidance and Operation, rev 1.01, 18 avril 2017, NXP.</i>	[CER]
	<i>P73 Services User Manual, API and Operational Guidance, Revision 2.0, 13 avril 2017, NXP</i>	[CER]
	<i>P73N2M0 Crypto Library : Information on Guidance and Operation, DocID 402811, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual – RNG Library, DocID 401410, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –SHA Library, DocID 401710, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –Secure SHA Library, DocID 401810, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –SHA-3 Library, DocID 402010, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –Secure SHA-3 Library, DocID 402110, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –HASH Library, DocID 403810, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –HMAC Library, DocID 401310, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –Rsa Library (RSA), DocID 401510, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –RSA Key Generation Library (RsaKg), DocID 401610 , NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –ECC over GF(p) Library, DocID 401210, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –ECDAA, DocID 402410, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –Utils Library, DocID 402210, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –Symmetric Cipher Library (SymCfg), DocID 401110, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –Korean SEED Library, DocID 402310, NXP.</i>	[CER]

	<i>P73N2M0 Crypto Library : User Manual –FELICA, Version 1.0, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –OSCCA-SM2 over GF(p) Library, DocID 402510, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –OSCCA-SM3 Library, DocID 402610, NXP.</i>	[CER]
	<i>P73N2M0 Crypto Library : User Manual –OSCCA-SM4 Library, DocID 402710, NXP.</i>	[CER]