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 certification ANSSI-CC-2019/62

P73N2M0B0.2C2/2C6
Version B0.2

Paris, le 24 décembre 2019

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié 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

Référence du rapport de certification

ANSSI-CC-2019/62

Nom du produit

P73N2M0B0.2C2/2C6

Référence/version du produit

B0.2

Conformité à un profil de protection

Security IC Platform Protection Profile with Augmentation Packages, version 1.0

certifié BSI-CC-PP-0084-2014 le 19 février 2014

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, ASE_TSS.2, AVA_VAN.5

Développeur

NXP Semiconductors

Troplowitzstrasse 20,
22529 Hamburg, Allemagne

Commanditaire

NXP Semiconductors

Troplowitzstrasse 20,
22529 Hamburg, Allemagne

Centre d'évaluation

Serma Safety & Security

14 rue Galilée, CS 10071, 33608 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Les produits évalués sont les microcontrôleurs « P73N2M0B0.2C2/2C6, version B0.2 » développés par *NXP SEMICONDUCTORS* avec des bibliothèques logicielles.
La différence entre le microcontrôleur « P73N2M0B0.2C2 » et le microcontrôleur « P73N2M0B0.2C6 » est la version de la bibliothèque logicielle embarquée.

Le microcontrôleur seul n'est pas un produit utilisable en tant que tel. Il est destiné à héberger une ou plusieurs applications. Il peut être inséré dans un support plastique pour constituer une carte à puce. Les usages possibles de cette carte sont multiples (documents d'identité sécurisés, applications bancaires, télévision à péage, transport, santé, etc.) en fonction des logiciels applicatifs qui seront embarqués. Ces logiciels ne font pas partie de la présente évaluation.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est strictement conforme au profil de protection [PP0084].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- la protection en intégrité et en confidentialité des données utilisateur et des logiciels embarqués exécutés ou stockés dans les différentes mémoires de la TOE ;
- la bonne exécution des services de sécurité fournis par la TOE aux logiciels embarqués ;
- le support au chiffrement cryptographique à clés symétriques ou asymétriques ;
- le support à la génération de nombres non prédictibles.

1.2.3. Architecture

Le produit est constitué :
- du produit P73N2M0B0.202 (i.e. des parties *Hadware* et *Firmware* évaluées via [ANSSI-CC-2018/52]) ;
- d'une bibliothèque logicielle : « *Services Software* » en version 1.9.14 pour la configuration 2C2 et en version 1.9.18 pour la configuration 2C6 ;
- d'une bibliothèque cryptographique logicielle : «*Crypto Library*» fournissant des algorithmes cryptographiques tels que AES, TDES, RSA, génération de clés RSA, ECDSA, ECDH, addition de points ECC, SHA, HMAC, fonctions de hachage, génération d'aléa avec retraitement cryptographique.

1.2.4. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée des microcontrôleurs est identifiable par les éléments donnés dans la table ci-après. Ces éléments peuvent être vérifiés par lecture des registres situés dans une zone spéciale de la mémoire spécifiée dans les [GUIDES], ou bien par appel à une fonction.

Eléments de configuration		Données d'identification lues
Identification du microcontrôleur	P73N2M0B0.2C2 : *version B0.2C2*	02 43 02
	P73N2M0B0.2C6 : *version B0.2C6*	02 43 06
Identification des logiciels embarqués	Bibliothèque logicielle pour P73N2M0B0.2C2 *: Service Software v1.9.14*	0x01090e00
	Bibliothèque logicielle pour P73N2M0B0.2C6 : *Service Software v1.9.18*	0x01091200
	Firmware version 1.5.4 Boot_OS v1.2.3 PL2 v8 Factory_OS v1.4.4 Services_flash v1.5.2	voir. [GUIDES_IC]
Identification de la bibliothèque cryptographique	*Crypto Library v1.0.8*	voir [GUIDES_CL] (Table 2 du guide « P73N2M0 Crypto Library - Information on Guidance and Operation, référence 402811 »)

Les procédures d'identification du microcontrôleur et de la bibliothèque logicielle sont décrites dans le guide « P73N2M0 – High-performance secure controller – Product data sheet » (voir [GUIDES_IC] et [GUIDES_SS]).

1.2.5. Cycle de vie

Le cycle de vie du produit est le cycle de vie décrit dans [PP0084] et la liste des sites impliqués est présentée dans la cible de sécurité [ST] au chapitre « *1.4.5 Life Cycle and Delivery of the TOE* » (voir [SITES] pour les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés).
Comme indiqué au paragraphe 1.3.2 de la cible de sécurité [ST], les bibliothèques logicielles sont fournies au développeur de logiciel embarqué pour permettre ses activités de Phase 1, et sont chargées en Flash sous le contrôle de *NXP SEMICONDUCTORS*.

1.2.6. Configuration évaluée

Le certificat porte sur les différentes variantes évaluées de P73N2M0B0.202 (voir configuration évaluée [ANSSI-CC-2018/52]), chargées avec les bibliothèques logicielles « *Services Software* » en version 1.9.14 (pour la configuration 2C2) ou 1.9.18 (pour la configuration 2C6) et « *Crypto Library* » en version 1.0.8.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].
Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation s'appuie sur les résultats d'évaluation des produits « P73N2M0B0.202 » certifié sous la référence [ANSSI-CC-2018/52] et « P73N2M0B0.2C2 » certifié sous la référence [ANSSI-CC-2018/55].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 10 décembre 2019 détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilité de conception et de construction pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [ANSSI-CC-2018/19]).
Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI [REF], la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « P73N2M0B0.2C2/2C6, version B0.2 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, ASE_TSS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Ce certificat donne une appréciation de la résistance du produit « P73N2M0B0.2C2/2C6, version B0.2 » à des attaques qui sont fortement génériques du fait de l'absence d'application spécifique embarquée. Par conséquent, la sécurité d'un produit complet construit sur le microcontrôleur ne pourra être appréciée que par une évaluation du produit complet, laquelle pourra être réalisée en se basant sur les résultats de l'évaluation citée au chapitre 2.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3. Reconnaissance du certificat

3.3.1. 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 :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

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

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	5	Complete semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	5	Advanced support
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR								1	Basic flaw remediation
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	3	Compliance with implementation standards - all parts
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	2	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		1	2	2	2	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	Ordered functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - P73N2M0B.2C2/2C6 Security Target, référence st_P73N2M0B0.2C2_2C6, version 3.3, 22/08/2019. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - P73N2M0B.2C2/2C6 Security Target, référence st_P73N2M0B0.2C2_2C6_Lite, version 3.3, 22/08/2019.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - P73 B0.2C6 project, référence P73B02C6_ETR_v1.1, version 1.1, 10/12/2019. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - Evaluation Technical Lite Report - P73 B0.2C6 project, référence P73B02C6_ETR-Lite_v1.1, version 1.10, 10/12/2019.
[CONF]	Liste de configuration du produit : - P73 Crypto Library - Life Cycle, référence Cl_ALC_p73n2m0, v1.0, 01/12/2016 ; - P73N2M0 B0.2C0/2C2/2C6 Bibliography evaluation evidences overview, référence P73N2M0B0.2C0_2C2_2C6 Bibliographyv1_18, v1.18, 20/11/2019 ; - P73 Crypto Library version 1.0.8, référence P73 CryptoLib v1.0.8 - cfgList.xls, version 16269, 13/12/2016 ; - Pour 2C2 (Services 1.9.14) : P73N2M0 High-performance secure controller- Firmware Configuration List – Services, référence alc_fw_p73, v0.8, 09/08/2017 ; - Pour 2C6 (Services 1.9.18) : P73N2M0 High-performance secure controller- Firmware Configuration List – Services, référence alc_fw_p73, v0.9, 19/01/2018.
[GUIDES]	Les guides du produit sont : – [GUIDES_IC] les guides de P73N2M0B0.202 (voir [ANSSI-CC-2018/52]) ; – [GUIDES_SS] les documents listés dans la Table 1 (ou Table 2) de la cible de sécurité [ST], pour l'usage de la bibliothèque *Services Software* ; – [GUIDES_CL] les documents listés dans la Table 3 de la cible de sécurité [ST], pour l'usage de la bibliothèque *Crypto Library*.
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

[ANSSI-CC-2018/52]	Rapport de certification ANSSI-CC-2018/52, P73N2M0B0.202. *Certifié par l'ANSSI le 16 novembre 2018.*
[ANSSI-CC-2018/55]	Rapport de certification ANSSI-CC-2018/55, P73N2M0B0.2C2. *Certifié par l'ANSSI le 14 décembre 2018.*
[ANSSI-CC-2018/19]	Rapport de certification ANSSI-CC-2018/19, P73N2M0B0.2C0/2P0. *Certifié par l'ANSSI le 13 avril 2018.*
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : – **NXP Semiconductors Caen** Site Techinal Audit Report NXP CAEN 2, référénce NXP_CAEN2_STAR_v1.0, version 1.0, 20 juillet 2018, *SERMA SAFETY AND SECURITY* ; – **NXP San Jose** Site Technical Audit Report NXP SAN JOSE 2, référence NXP SAN JOSE 2_STAR_v1.1, version : 1.1, 19 décembre 2018, *SERMA SAFETY AND SECURITY ;* – **Global Logic Wroclaw** Site Technical Audit Report REC WROCLAW 2, référence : REC WROCLAW 2_STAR_v1.0, version 1.0, 08 août 2018, *SERMA SAFETY AND SECURITY ;* – **SII Gdansk** Site Technical Audit Report NXP-GDANSK3, référence Site_NXP-GDANSK3_STAR_v1.0, version 1.0, 4 avril 2019, *SERMA SAFETY AND SECURITY ;* – **NXP Semiconductors Development Environment** NXP ALC_FLR Sites Visit Report, référence 17-0122_NXP_ALC-FLR_SVR_v1.0, version 1.0, 31 juillet 2017, *SERMA SAFETY AND SECURITY.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[AIS 31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.