

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CC-2019/62-R01

**P73N2M0B0.2C2/2C6
(B0.2C2 / B0.2C6)**

Paris, le 14 Juin 2024

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

Emmanuel NAEGELEN

[ORIGINAL SIGNE]



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 présumées 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

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

Référence du rapport de certification	ANSSI-CC-2019/62-R01
Nom du produit	P73N2M0B0.2C2/2C6
Référence/version du produit	B0.2C2 / B0.2C6
Conformité à un profil de protection	<i>Security IC Platform Protection Profile with Augmentation Packages, version 1.0</i> certifié BSI-CC-PP-0084-2014 le 19 février 2014 avec conformité aux packages : <i>"TDES", "AES"</i>
Critère d'évaluation et version	Critères Communs version 3.1 révision 5
Niveau d'évaluation	EAL5 augmenté ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ALC_FLR.1, ATE_COV.3, ATE_FUN.2, ASE_TSS.2, AVA_VAN.5
Développeur	NXP SEMICONDUCTORS Beiersdorfstr 12, 22529 Hamburg, Allemagne
Commanditaire	NXP SEMICONDUCTORS Beiersdorfstr 12, 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 ALC_FLR.1.

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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.cyber.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit.....	6
1.2.1	Introduction	6
1.2.2	Services de sécurité.....	6
1.2.3	Architecture	6
1.2.4	Identification du produit.....	7
1.2.5	Cycle de vie	7
1.2.6	Configuration évaluée	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation	8
2.2	Travaux d'évaluation	8
2.3	Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification	10
3.1	Conclusion.....	10
3.2	Restrictions d'usage	10
3.3	Reconnaissance du certificat.....	11
3.3.1	Reconnaissance européenne (SOG-IS).....	11
3.3.2	Reconnaissance internationale critères communs (CCRA)	11
ANNEXE A.	Références documentaires du produit évalué	12
ANNEXE B.	Références liées à la certification	14

1 Le produit

1.1 Présentation du produit

Le produit évalué est « P73N2M0B0.2C2/2C6, B0.2C2 / B0.2C6 » développé par NXP SEMICONDUCTORS.

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], avec :

- le package « *TDES* » ;
- le package « *AES* ».

1.2.2 Services de sécurité

Les principaux services de sécurité fournis par le produit sont présentés au chapitre 1.3 « *TOE Overview* » de la cible de sécurité [ST_IC].

1.2.3 Architecture

Ce produit peut être décomposé en deux parties distinctes : une partie logicielle et une partie matérielle.

Le produit est constitué des composants présentés au chapitre 1.4 « *TOE Description* » de la cible de sécurité [ST_IC].

1.2.4 Identification du produit

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

Le produit est identifiable par lecture de registres comme indiqué dans les [GUIDES]. La version certifiée correspond aux valeurs indiquées au chapitre 1.4.2 « *Evaluated Configurations* » de la cible de sécurité [ST_IC].

1.2.5 Cycle de vie

Le cycle de vie du produit est le cycle de vie décrit dans [PP0084]. Il est décrit au chapitre 1.4.4 « *Security During Development and Production* » de la cible de sécurité [ST_IC] et la liste des sites impliqués est présentée dans la table 7 « *Development and Manufacturing sites* ».

1.2.6 Configuration évaluée

Le certificat porte sur les configurations permises par la cible de sécurité [ST].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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

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

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

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

Cette analyse n'a pas permis de mettre en évidence de biais statistiques bloquants. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception. Comme énoncé dans le document [ANSSI Crypto], il est rappelé que, pour un usage cryptographique, la sortie d'un générateur matériel de nombres aléatoires doit impérativement subir un retraitement algorithmique de nature cryptographique, même si l'analyse du générateur physique d'aléa n'a pas révélé de faiblesse.

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

Ce générateur d'aléa a aussi été analysé conformément à la méthode d'évaluation [AIS20/31].

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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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 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'accord¹, 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 [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires², 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.eu.

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

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - <i>P73N2M0B0.2C2/2C6 (R2) Security Target</i>, version 3.7, 21 novembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - <i>P73N2M0B0.2C2/2C6 (R2) Security Target Lite</i>, version 3.7, 21 novembre 2023.
[ST_IC]	Cible de sécurité de référence pour l'évaluation : - <i>P73N2M0B0.202 Security Target</i>, version 2.5, 21 novembre 2023. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - <i>P73N2M0B0.202 Security Target Lite</i>, version 2.5, 21 novembre 2023.
[RTE]	Rapport technique d'évaluation : - <i>Evaluation Technical Report P73C Project</i>, référence P73C_ETR_v1.1, version 1.1, 27 mai 2024. Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé : - <i>Evaluation Technical Report Lite for Composition P73C Project</i>, référence P73C_ETR_Lite_v1.1, version 1.1, 27 mai 2024.
[CONF]	Liste de configuration du produit : - <i>P73 CONFIGURATION DOCUMENT P73N2M0B0.200/202/207/20C/2C0/2C2/2C6/2C8/2CB/2CC</i>, version 1.3, 3 février 2023. - <i>P73N2M0 B0.200/202/207/20C Bibliography Evaluation Evidences Overview</i>, version 1.14, 5 décembre 2023. - <i>P73N2M0 B0.2C0/2C2/2C6/2C8/2CB/2CC Bibliography Evaluation Evidences Overview</i>, version 1.25, 13 mars 2024.
[GUIDES]	- <i>P73N2M0 Crypto Library Information on Guidance and Operation</i>, référence 402814, version 1.4, 27 octobre 2023. - <i>P73N2M0B0.20n, Information on User Guidance and Operation, User Manual</i>, version 1.01, 18 avril 2017. - <i>P73N2M0 Crypto Library: User Manual – RNG Library</i>, référence 401410, révision 1.0, 12 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – SHA Library</i>, référence 401710, révision 1.0, 12 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – Secure SHA Library</i>, référence 401810, révision 1.0, 12 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – SHA-3 Library</i>, référence 402010, révision 1.0, 12 octobre 2016.

	- <i>P73N2M0 Crypto Library: User Manual – Secure SHA-3 Library</i>, référence 402110, révision 1.0, 12 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – HASH Library</i>, référence 403810, révision 1.0, 12 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – HMAC Library</i>, référence 401310, révision 1.0, 12 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – Rsa Library (Rsa)</i>, référence 401510, révision 1.0, 11 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – RSA Key Generation Library (RsaKg)</i>, référence 401610, revision 1.0, 11 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – ECC over GF(p) Library</i>, reference 401210, révision 1.0, 10 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – ECDAA</i>, reference 402410, revision 1.0, 10 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – Utils Library</i>, reference 402210, revision 1.0, 10 octobre 2016. - <i>P73N2M0 Crypto Library: User Manual – Symmetric Cipher Library (SymCfg)</i>, reference 401110, revision 1.0, 10 octobre 2016. - <i>P73 Services User Manual, API and Operational Guidance For P73N2M0B0.2C2 (Services 1.9.14)</i>, version 2.0, 13 avril 2017. - <i>P73 Services User Manual, API and Operational Guidance For P73N2M0B0.2C6 (Services 1.9.18)</i>, version 2.2, 19 janvier 2018. - <i>P73N2M0, High-performance secure controller, Product data sheet</i>, référence 297432, version 3.2, 5 juillet 2019. - <i>P73N2M0B Wafer and delivery specification</i>, référence 328231, version 3.1, 27 avril 2018. - <i>P73 family SC300 User manual</i>, référence 341410, version 1.0, 12 août 2015. - <i>P73 family DMA Controller PL080 User manual</i>, référence 341510, version 1.0, 18 août 2015.
[SITES]	La liste des sites est disponible dans la table 7 « <i>Development and Manufacturing sites</i> » de la cible de sécurité [ST_IC].
[PP0084]	<i>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages</i>, version 1.0, 13 janvier 2014. Certifié par le BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>) sous la référence BSI-PP-0084-2014.

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	<i>Common Criteria for Information Technology Security Evaluation:</i> - <i>Part 1: Introduction and general model</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - <i>Part 2: Security functional components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - <i>Part 3: Security assurance components</i>, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	<i>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology</i> , avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[IIWG IC] *	<i>Mandatory Technical Document – The Application of CC to Integrated Circuits</i> , version 3.0, février 2009.
[IIWG AP] *	<i>Mandatory Technical Document – Application of attack potential to smartcards and similar devices</i> , version 3.2, novembre 2022.
[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security</i> , 2 juillet 2014.
[SOG-IS]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates</i> , version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[AIS20/31]	<i>A proposal for: Functionality classes for random number generators, AIS20/AIS31</i> , version 2.0, 18 septembre 2011, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>).

[CC-NOTE-24]	Evaluation de générateurs d'aléa selon AIS20/31 dans le schéma français, ANSSI-CC-NOTE-24_1.0, version 1.0, 2 mars 2021.
--------------	--

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