



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-2018/52**

### **P73N2M0B0.202**

*Paris, le 16 novembre 2018*

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

Guillaume POUPARD  
[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](mailto:certification@ssi.gouv.fr)

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

Référence du rapport de certification	<b>ANSSI-CC-2018/52</b>
Nom du produit	<b>P73N2M0B0.202</b>
Référence/version du produit	<b>B0.202</b>
Conformité à un profil de protection	<b>Security IC Platform Protection Profile with Augmentation Packages, version 1.0, certifié BSI-CC-PP-0084-2014 le 19 février 2014</b>
Critères d'évaluation et version	<b>Critères Communs version 3.1 révision 4</b>
Niveau d'évaluation	<b>EAL 5 augmenté</b> <b>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, AVA_VAN.5, ASE_TSS.2</b>
Développeur	<b>NXP Semiconductors</b> Troplowitzstrasse 20, 22529 Hamburg, Allemagne
Commanditaire	<b>NXP Semiconductors</b> Troplowitzstrasse 20, 22529 Hamburg, Allemagne
Centre d'évaluation	<b>Serma Safety &amp; Security</b> 14 rue Galilée, CS 10055, 33615 Pessac Cedex, France
Accords de reconnaissance applicables	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p><b>CCRA</b></p>  </div> <div style="text-align: center;"> <p><b>SOG-IS</b></p>  </div> </div> <p><b>Ce certificat est reconnu au niveau EAL2 augmenté de FLR.1.</b></p>

# 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](http://www.ssi.gouv.fr).

# Table des matières

<b>1. LE PRODUIT .....</b>	<b>6</b>
1.1. PRESENTATION DU PRODUIT .....	6
1.2. DESCRIPTION DU PRODUIT .....	6
1.2.1. <i>Introduction</i> .....	6
1.2.2. <i>Services de sécurité</i> .....	6
1.2.3. <i>Architecture</i> .....	6
1.2.4. <i>Identification du produit</i> .....	7
1.2.5. <i>Cycle de vie</i> .....	7
1.2.6. <i>Configuration évaluée</i> .....	7
<b>2. L’EVALUATION .....</b>	<b>8</b>
2.1. REFERENTIELS D’EVALUATION .....	8
2.2. TRAVAUX D’EVALUATION .....	8
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI .....	8
2.4. ANALYSE DU GENERATEUR D’ALEAS .....	8
<b>3. LA CERTIFICATION .....</b>	<b>9</b>
3.1. CONCLUSION .....	9
3.2. RESTRICTIONS D’USAGE .....	9
3.3. RECONNAISSANCE DU CERTIFICAT .....	10
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> .....	10
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> .....	10
<b>ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT .....</b>	<b>11</b>
<b>ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE .....</b>	<b>12</b>
<b>ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION .....</b>	<b>13</b>

# 1. Le produit

## 1.1. Présentation du produit

Le produit évalué est le microcontrôleur « P73N2M0B0.202 » 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].

### 1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection physique ;
- le support matériel au chiffrement cryptographique à clés asymétriques ;
- le support matériel au chiffrement cryptographique à clés symétriques ;
- le support matériel à la génération de nombres non prédictibles ;
- les contrôles d'accès aux mémoires.

### 1.2.3. Architecture

Le produit est constitué d'une partie matérielle et d'une partie logicielle, toutes deux décrites dans la cible de sécurité [ST] au paragraphe *TOE Description*.

La partie matérielle comporte principalement :

- un processeur ARM SC300 ;
- des coprocesseurs cryptographiques pour accélérer les calculs cryptographiques à clés symétriques ou asymétriques ;
- un générateur physique d'aléa ;
- des mémoires (RAM, Flash, ROM) ;
- des modules de sécurité : unité de gestion et protection des mémoires (MMU), horloges, contrôle d'intégrité ;
- des modules fonctionnels de gestion des entrées/sorties.

La partie logicielle est composée :

- d'un logiciel d'auto-test (*Factory OS*) ;
- d'un logiciel de démarrage du composant (*Boot OS*) ;

- d'un pilote d'accès à la mémoire Flash (*Flash Driver Software*).

#### **1.2.4. Identification du produit**

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

La version certifiée du produit est identifiable par la donnée *Type ID* décrite dans le guide *data sheet* au paragraphe 16.2. Les valeurs attendues de ses composantes sont :

- `nxp_hw_ident_code` : 0x02 ;
- `nxp_sw_ident_code` : 0x30 ;
- `nxp_sw_ident_version` : 0x02.

#### **1.2.5. Cycle de vie**

Le produit est développé sur les sites présentés en Table « *Development and Manufacturing sites* » de la cible de sécurité. Le cycle de vie s'inscrit dans le cycle de vie standard décrit dans [PP0084].

#### **1.2.6. Configuration évaluée**

Comme décrit dans la cible de sécurité [ST] au paragraphe *Evaluated Configurations*, le produit se décline en différentes configurations logiques, par le choix d'options. Le certificat porte sur toutes les configurations obtenues pourvu que chaque option ait l'une des valeurs évaluées indiquées dans [ST].

## 2. L'évaluation

### 2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 du produit P73N2M0B0.200 certifié sous la référence [ANSSI-CC-2018/08].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 9 novembre 2018, 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 a fait l'objet d'une évaluation selon la méthodologie [AIS31] et il répond aux exigences de la classe PTG.2.

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 [REF] 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'aléas n'a pas révélé de faiblesse.



## 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 « P73N2M0B0.202 » 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, ACL\_DVS.2, ALC\_FLR.1, ALC\_TAT.3, ATE\_COV.3, ATE\_FUN.2, AVA\_VAN.5, ASE\_TSS.2.

### 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 « P73N2M0B0.202 » 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 micro-circuit 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<sup>1</sup>, 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<sup>2</sup>, 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 :



---

<sup>1</sup> La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : [www.sogis.org](http://www.sogis.org).

<sup>2</sup> La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : [www.commoncriteriaportal.org](http://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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	3	Minimally complex internals
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	5	5	Complete semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	5	Advanced support
	ALC_CMS	1	2	3	4	5	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR									1	Basic flaw remediation
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	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	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	2	2	TOE summary specification with architectural design summary
ATE Tests	ATE_COV		1	2	2	2	3	3	3	3	Rigorous analysis of coverage
	ATE_DPT			1	1	3	3	4	3	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	2	2	Ordered functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

## Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> <li>- P73N2M0B0.202 Security Target, rev. 2.4, 2 novembre 2018, <i>NXP</i>.</li> </ul> <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> <li>- P73N2M0B0.200 Security Target Lite, rev. 2.4, 2 novembre 2018, <i>NXP</i>.</li> </ul>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report - P73A Project, P73A_ETR_v1.1, 9 novembre 2018, <i>SERMA</i>.</li> </ul> <p>Pour le besoin des évaluations en composition avec ce microcontrôleur un rapport technique pour la composition a été validé :</p> <ul style="list-style-type: none"> <li>- Evaluation Technical Report Lite - P73A Project, P73A_ETR-Lite_v1.1, 9 novembre 2018, <i>SERMA</i>.</li> </ul>
[CONF]	<p>Liste de configuration du produit :</p> <ul style="list-style-type: none"> <li>- P73_Configuration_List, 28 février 2017, <i>NXP</i>,</li> <li>- P73N2M0 Bibliography, v1.9, 5 novembre 2018, <i>NXP</i>.</li> </ul>
[GUIDES]	<p>Les guides du produit sont les documents mentionnés en Table 1 de la cible de sécurité [ST], à savoir :</p> <ul style="list-style-type: none"> <li>- P73N2M0 High-performance secure controller, ref 297431 rev. 3.1, 8 juin 2017, <i>NXP</i> ;</li> <li>- P73N2M0B Wafer and delivery specification, ref 328231 rev 3.1, 27 avril 2018, <i>NXP</i> ;</li> <li>- P73 family, SC300 User manual, ref 341410 rev.1.0, 12 août 2015, <i>NXP</i> ;</li> <li>- ARMv-7-M Architecture Reference Manual, ARM DDI 0403E.b ID120114, 2 septembre 2015, ARM ;</li> <li>- P73 family, DMA Controller PL080 User manual, ref 341510 rev. 1.0, 18 août 2015, <i>NXP</i> ;</li> <li>- P73N2M0B0.20n Information on Guidance and Operation, rev 1.01, 18 avril 2017, <i>NXP</i> ;</li> <li>- Electronic Order Entry Form, online document, <i>NXP</i>.</li> </ul>
[PP0084]	<p>Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.</i></p>
[ANSSI-CC-2018/08]	<p>Rapport de certification ANSSI-CC-2018/08, P73N2M0B0.200, 16 février 2018.</p>

### 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 : <ul style="list-style-type: none"> <li>- Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001;</li> <li>- Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002;</li> <li>- Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.</li> </ul>
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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 <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a> .
[AIS31]	A proposal for: Functionality classes for random number generators, AIS20/AIS31, version 2.0, 18 Septembre 2011, BSI ( <i>Bundesamt für Sicherheit in der Informationstechnik</i> ).

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