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 certification ANSSI-CC-2021/49

NPCT7xx TPM2.0 rev 1.59 (configuration version 1.0.0.0)

Paris, le 22 octobre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

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

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

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

Référence du rapport de certification

ANSSI-CC-2021/49

Nom du produit

NPCT7xx TPM2.0 rev 1.59

Référence/version du produit

configuration version 1.0.0.0

Conformité à un profil de protection

Néant

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 4 augmenté

ALC_FLR.1, ALC_DVS.2, AVA_VAN.4,

Développeur

NUVOTON TECHNOLOGY CORPORATION

No4, Creation Rd. 3, Science-Based Industrial Park, Hsinchu, 300, Taiwan, R.O.C

Commanditaire

NUVOTON TECHNOLOGY CORPORATION

No4, Creation Rd. 3, Science-Based Industrial Park, Hsinchu, 300, Taiwan, R.O.C

Centre d'évaluation

SERMA SAFETY & SECURITY

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

Accords de reconnaissance applicables

CCRA

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

SOG-IS

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.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « NPCT7xx TPM2.0 rev 1.59, configuration version 1.0.0.0 » développé par NUVOTON TECHNOLOGY CORPORATION.

Ce produit est destiné à garantir l'intégrité matérielle et logicielle des plateformes de confiance (serveurs, ordinateurs, etc.) conformément aux spécifications fonctionnelles TPM2.0.

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.

La cible de sécurité s'inspire du profil de protection [PP-TPM-1.3] en cours d'élaboration.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :
- les algorithmes cryptographiques ECC, RSA, SHA-256, SHA-384, HMAC, AES ;
- la génération de nombres aléatoires ;
- la génération de clés ;
- l'auto-test ;
- la protection physique de la puce.

1.2.3 *Architecture*

La partie matérielle du produit est principalement constituée de :
- un processeur ;
- des accélérateurs pour les algorithmes cryptographiques ;
- un générateur physique d'aléa ;
- un module d'horloge ;
- des mémoires ROM, RAM et FLASH ;
- un module de communication, pour les interfaces SPI et I2C.

Le logiciel embarqué, *TPM Firmware*, est constitué de :
- un module *Booter* ;
- un module *Cryplib* ;
- un module *BootLoader* ;
- un module *Upgradable Software*.

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 dans la table 1.1 de la cible de sécurité [ST].

1.2.5 *Cycle de vie*

Le cycle de vie du produit suit les phases décrites dans [PP-TPM-1.3] et les sites impliqués sont précisés dans le tableau « *Sites of Development Environment, Manufacturing and Delivery* » de la cible de sécurité [ST].

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 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 « NPCT7xx TPM2.0 rev 1.38 (Hardware LAG019, Firmware 7.2.2.0) » certifié sous la référence [ANSSI-CC-2020/21].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 août 2021, 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 oeuvre 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 a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 potentiel d'attaque visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa du produit qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

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

Comme requis dans le référentiel [ANSSI Crypto], la sortie du générateur physique d'aléa subit un retraitement de nature cryptographique.

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

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 [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2] , des certificats Critères Communs.

[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.

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 :

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *NPCT7xx TPM2.0 rev 1.59 configuration version 1.0.0.0 Security Target, version 1.0, Confidential*, 15 juillet 2021, NUVOTON. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - *NPCT7xx TPM2.0 rev 1.59 configuration version 1.0.0.0 Security Target, version 1.0*, 15 juillet 2021, NUVOTON.
[RTE]	*Evaluation Technical Report, BARAK3 Project, BARAK3_ETR_v1.0*, 26 août 2021, SERMA SAFETY & SECURITY.
[CONF]	*CM scope, NPCT7xx_TPM2.0_rev1.59_IC_ALC_CMS.1.v1.0.0*, 12 juillet 2021, NUVOTON.
[GUIDES]	- *NPCT7xx Trusted Platform Module Family 2.0, revision 1.23*, juillet 2021, NUVOTON ; - *NPCT7xx TPM2.0 Programmer's Guide, revision 1.8*, juillet 2021, NUVOTON ; - *NPCT7xx User Product Information, revision 2.10*, Juillet 2021, NUVOTON ; - *NPCT75xxAB, NPCT75xxAD and NPCT76xxAA TPM2.0 Guidance Document, Common Criteria AGD Component, revision 1.6*, juin 2021, NUVOTON.
[PP-TPM-1.3]	*Protection Profile PC Client Specific TPM, TPM Library specification Family 2.0; level 0 Revision 1.59*, 22 mars 2021 version 1.3, TCG. Ce profil de protection n'est pas certifié.
[ANSSI-CC-2020/21]	Rapport de certification ANSSI-CC-2020/21, NPCT7xx TPM2.0 rev 1.38 (*Hardware* LAG019, *Firmware* 7.2.2.0), 10 juillet 2020.

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]	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.
[CRY-P-01]	Procédure ANSSI-CC-CRY-P01 Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, 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 and similar devices*, version 3.1, juin 2020.
[CCRA]	*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.
[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.

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