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 / Certification report EUCC-3090-2026-32

NPCT7xx TPM2.0 rev 1.59 (configuration version 1.1.5.5)

Paris, le 26/4/2026 | 19:06 CEST

Vincent Strubel

SÉCURITÉ CERTIFICATION

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

AVERTISSEMENT / *WARNING*

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.

This report is intended to provide individuals requesting evaluations with a document certifying the level of security provided by the product, under the usage or operating conditions defined in this report, for the version that was evaluated.

It is also intended to inform potential purchasers of the product about the conditions under which it can be used to ensure compliance with the requirements for which the product was evaluated and certified. For this reason, the certification report must be read in conjunction with the evaluated usage and administration guides, as well as the product's security target, which describes the assumed threats, environmental assumptions, and usage conditions. This allows users to determine whether the product meets their security objectives.

The certification does not in itself constitute a product endorsement by the Agence nationale de la sécurité des systèmes d'information (ANSSI), and does not guarantee that the certified product is entirely free from exploitable vulnerabilities.

Toute correspondance relative à ce rapport doit être adressée au :

All correspondence related to this report must be sent to:

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

PREFACE / *FOREWORD*

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 ;
- Les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits 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).

Certification of the security provided by information technology products and systems is governed by amended Decree 2002-535 of April 18th, 2002. This decree states that:

- *The Agence nationale de la sécurité des systèmes d'information drafts the certification reports. These reports specify the characteristics of the proposed security objectives. They may include any warnings authors deem necessary to mention for security reasons* ;
- *The certificates issued by the Director General of ANSSI certify that the specific product or system submitted for evaluation meets the defined security characteristics. They also confirm that the evaluations were carried out according to current rules and standards, with the required levels of competence and impartiality (Article 8).*

Ce rapport est conforme à [EUCC].
This report is in compliance with [EUCC].

Les procédures de certification sont disponibles sur le site Internet https://www.cyber.gouv.fr/.

The certification procedures are available on the website www.cyber.gouv.fr.

TABLE DES MATIERES / *TABLE OF CONTENT*

1 Résumé / *Summary*

Référence du rapport de certification / *Certification report reference* **EUCC-3090-2026-32**
Nom du produit / *Product name* **NPCT7xx TPM2.0 rev 1.59**
Référence/version du produit / *Product reference/version* **configuration version 1.1.5.5**
Type de produit / *Type of product* **Cartes à puce et dispositifs similaires** ***(Smart cards and similar devices)***
Conformité à un profil de protection / *Conformity with a protection profile* ***Protection Profile PC Client Specific TPM*** PP PCCS TPM F2.0 L0 r1.59 V1.3, certifié ANSSI-CC-PP-2021/02 le 30 novembre 2021
Critère d'évaluation et version / *Evaluation criteria and version* **ISO/IEC 15408-1:2009, 15408-2:2008, 15408-3:2008, 18045:2008** **Critères Communs version 3.1 rev. 5**
Niveau d'évaluation / *Evaluation level* **Elevé (*High*) / EAL4 augmenté (*augmented*)** ALC_FLR.1, ALC_DVS.2, AVA_VAN.4
Référence du rapport d'évaluation / *Evaluation report reference* *Evaluation Technical Report BARAK8 Project* Ref. BARAK8_ETR_v1.1 version 1.1 11/03/2026.
Fonctionnalité de sécurité du produit / *Product's security features* § 2.2.2Services de sécurité / *Security services*
Résumé des menaces / *Threat summary* *Compromise* *Bypass* *Export* *Hack_Crypto* *Hack_Physical* *Imperson* *Import* *Insecure_State* *Intercept* *Malfunction* *Modify* *Object_Attr_Change* *Replay* *Repudiate_Transact* *Residual_Info*

Leak
Unauthorized_Load
Bad_Activation
Toe_Identification

Exigences de configuration du produit / *Product configuration requirements*
§ 4.2 Restrictions d'usage / restrictions usage

Hypothèses liées à l'environnement d'exploitation / *Operating environment assumptions*
§ 4.2 Restrictions d'usage / restrictions usage

Développeur / *Developer*

NUVOTON TECHNOLOGY CORPORATION
No. 4, Creation Rd. III, Hsinchu Science Park
Taiwan, R.O.C

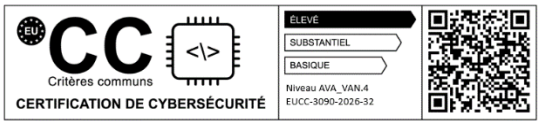
Commanditaire / *Sponsor*

NUVOTON TECHNOLOGY CORPORATION
No. 4, Creation Rd. III, Hsinchu Science Park
Taiwan, R.O.C

Centre d'évaluation (CESTI) / *Evaluation center (ITSEF)*

SERMA SAFETY & SECURITY
14 rue Galilée, CS 10071,
33608 Pessac Cedex, France

Marque EUCC / *EUCC Mark*



Accords de reconnaissance applicables / *Applicable recognition agreements*

CCRA

Ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.1.
This certificate is recognized at EAL2 level augmented with ALC_FLR.1.

2 Le produit / *Product*

2.1 Présentation du produit / *Product presentation*

Le produit évalué est « NPCT7xx TPM2.0 rev 1.59, configuration version 1.1.5.5 » développé par NUVOTON TECHNOLOGY CORPORATION.

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

The product evaluated is «NPCT7xx TPM2.0 rev 1.59, configuration version 1.1.5.5 » developed by NUVOTON TECHNOLOGY CORPORATION.

This product is a TPM (Trusted Platform Module). It is designed to guarantee the hardware and software integrity of trusted platforms (servers, computers, etc.) in accordance with TPM2.0 functional specifications.

2.2 Description du produit / *Product description*

2.2.1 *Introduction*

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

The security target [ST] defines the product that is evaluated, its security functionalities that are evaluated and its operating environment.

Cette cible de sécurité est conforme au profil de protection [PP-TPM].

This security target complies with the protection profile [PP-TPM].

2.2.2 *Services de sécurité / Security services*

Les services de sécurité évalués fournis par le produit sont présentés au chapitre 1.2 « *TOE Global Overview* » de la cible de sécurité [ST].

The main security services provided by the product are listed at chapter 1.2 "TOE Global Overview" of the security target [ST].

2.2.3 *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 2.2 « TOE Overview » de la cible de sécurité [ST]. La Figure 1 notamment présente l'architecture du produit.

The product consists of a hardware part and a software part, both of which are described in the security target [ST] in section 2.2 "TOE Overview". Figure 1 in particular shows the product architecture.

2.2.4 *Identification du produit / Product identification*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre 1.1 « *Security Target (ST) and Target of Evaluation (TOE) Identification* ».

The certified version of the product can be identified by the elements detailed in the security target [ST] in the « Security Target (ST) and Target of Evaluation (TOE) Identification » chapter 1.1.

La version 1.1.5.5 utilise la version 2.0.0.21 du BootLoader.

Version 1.1.5.5 uses BootLoader version 2.0.0.21.

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.

These elements can be verified by reading the registers located in a special area of memory specified in the [GUIDES], or by calling a function.

2.2.5 *Cycle de vie / Lifecycle*

Le cycle de vie du produit suit les phases décrites dans [PP-TPM] et les sites impliqués sont précisés dans la table 2-1 « *Sites of Development Environment, Manufacturing and Delivery* » de la cible de sécurité [ST].

The product lifecycle follows the phases described in [PP-TPM], and the sites involved are specified in the table 2-1 "Sites of Development Environment, Manufacturing, and Delivery" in the security target [ST].

2.2.6 *Configuration évaluée / Evaluated configuration*

Le certificat porte sur les configurations permises par la cible de sécurité [ST] pourvu que les [GUIDES] soient respectés.

The certificate covers the configurations permitted by the security target [ST], provided that the [GUIDES] are followed.

2.3 Contacts du produit / *Product contacts*

Les informations en matière de cybersécurité du produit sont disponibles ici :

The product's cybersecurity information is available here:

- https://www.nuvoton.com/products/cloud-computing/security/trusted-platform-module-tpm/

Le développeur peut être contacté via cette adresse :

The developer can be contacted at this address:

- security@nuvoton.com

La procédure complète de signalement d'une vulnérabilité est disponible sur le lien suivant :

The complete procedure for reporting a vulnerability is available at the following link:

- https://www.nuvoton.com/support/security/report-security-vulnerability/

Les informations sur l'Autorité nationale de certification de cybersécurité en France sont disponibles ici :

Information on France's National Cybersecurity Certification Authority is available here:

- https://cyber.gouv.fr/cybersecurity-act

3 L'évaluation / *Evaluation*

3.1 Référentiels d'évaluation / *Evaluation reference bases*

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

The evaluation was carried out in accordance with the Common Criteria [CC], and with the evaluation methodology defined in the manual [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.

For assurance components not covered by the [CEM] manual, methods specific to the evaluation center and validated by ANSSI have been used.

Pour répondre aux spécificités des cartes à puce et dispositifs similaires, les guides [SotA IC] et [SotA IC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [SotA IC 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).

To meet the specific requirements of smart cards and similar devices, the [SotA IC] and [SotA IC AP] guides were applied. Thus, the AVA_VAN level was determined using the rating scale from the [SotA IC AP] guide. As a reminder, this rating scale is more demanding than the default one defined in the standard [CC] methodology, which is used for other product categories (e.g., software products).

3.2 Travaux d'évaluation / *Evaluation tasks*

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** ».

*The Evaluation Technical Report [ETR], submitted to ANSSI on the day it is finalized by ITSEF, details the work carried out by the evaluation center and attests that all the evaluation tasks were rated as « **PASS** ».*

3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI / *Analysis of cryptographic mechanisms according to ANSSI technical standards*

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].

The cryptographic mechanisms implemented by the product's security functions (see [ST]) have been analyzed in accordance with procedure [CRY-P-01] and the results recorded in report [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel. 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 niveau d'attaquant visé.

This analysis identified non-conformities with respect to the standard [ANSSI Crypto]. They were taken into account in the independent vulnerability analysis carried out by the evaluator, which did not reveal any exploitable vulnerabilities at the targeted attacker level.

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.

The user must refer to the [GUIDES] to configure the product in accordance with the [ANSSI Crypto], for the cryptographic mechanisms that allow it.

4 La certification / *Certification*

4.1 Conclusion / *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 et à [EUCC].

The evaluation was carried out according to current rules and standards, with the levels of competence and impartiality required for an approved evaluation body. All of the evaluation work performed permits the delivery of a certificate in accordance with decree 2002-535 and to [EUCC].

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 (voir chapitre 1 Résumé / *Summary*).

This certificate confirms that the product under evaluation meets the security requirements specified in its security target [ST] for the intended evaluation level (see chapter 1 Résumé / Summary).

Le certificat associé à ce rapport, référencé EUCC-3090-2026-32 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

The certificate associated with this report, referenced EUCC-3090-2026-32 has an issue date identical to the signature date of this report and is valid for five years from that date.

Le certificat est délivré sous accréditation Cofrac Certification de produits et services, attestation n°5-0669, liste des sites et portée disponibles sous www.cofrac.fr.

The certificate is issued under accreditation of Cofrac Certifications, certificate n°. 5-0669, list of sites and scope availableat www.cofrac.fr.

4.2 Restrictions d'usage / *Use Restriction*

Ce certificat porte sur le produit spécifié au chapitre 2.2 du présent rapport de certification.

This certificate relates to the product specified in chapter 2.2 of this certification report.

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].

4.3 Reconnaissance du certificat / *Certificate recognition*

4.3.1 *Reconnaissance internationale critères communs (CCRA) / International Common Criteria Recognition*

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[1] , des certificats Critères Communs.

This certificate is issued under the conditions of the CCRA agreement [CCRA]. The "Common Criteria Recognition Arrangement" enables the recognition of Common Criteria certificates by the signatory countries.

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 :

Recognition applies up to the assurance components of CC EAL2 level as well as the ALC_FLR family. Certificates recognised under this agreement are issued with the following mark :

[1] 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 / *Documentary references for the product evaluated*

[ST]	Cible de sécurité de référence pour l'évaluation / *Security target for the evaluation:* - *NPCT7xx TPM2.0 rev 1.59 configuration ver 1.1.5.5 Security Target*, version 1.2, 05/03/2026. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation / *For publication purposes, the following security target has been provided and validated as part of this evaluation:* - *NPCT7xx TPM2.0 rev 1.59 configuration ver 1.1.5.5 Security Target Lite*, version 1.2, 05/03/2026.
[RTE]	Rapport technique d'évaluation / *Evaluation Technical Report :* - *Evaluation Technical Report BARAK8 Project*, ref. BARAK8_ETR_v1.1, version 1.1, 11/03/2026.
[GUIDES]	- *NPCT7xx TPM2.0 Programmer's Guide*, version 1.16, 18/11/2025. - *NPCT7xx Trusted Platform Module Family 2.0 (TPM2.0)*, version 1.35, 18/11/2025. - *NPCT7xx User Product Information*, version 2.20, 18/11/2025. - *NPCT7xx Guidance Document Common Criteria AGD Component*, version 2.5, 07/12/2025. - *Nuvoton TPM SPDM Guidance Document*, version 1.10, 17/08/2025.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation / *Document analysis and site audit reports for reuse:* - Site_NUVOTON_2024_ALC_GEN_v1.1 ; - Site_NUVOTON_2024-NTIL_STAR_v1.0 ; - Site_NUVOTON_2024_NTC_STAR_v1.1.
[PP-TPM]	*Protection Profile PC Client Specific TPM*, PP PCCS TPM F2.0 L0 r1.59 V1.3, certifié ANSSI-CC-PP-2021/02 le 30 novembre 2021.

ANNEXE B. Références liées à la certification / Certification references

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. *Amended decree No. 2002-535 of April 18th, 2002 relating to the evaluation and certification of the security provided by information technology products and systems.*	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4. *Certification procedure of the security provided by information technology products and systems, ref ANSSI-CC-CER-P-01.*
[EUCC]	Schéma européen de certification de cybersécurité fondé sur les critères communs (règlement d'exécution (UE) 2024/482) et ses amendements. *European cybersecurity certification scheme based on common criteria (implementing regulation (EU) 2024/482) and its amendments.*
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version en vigueur. *Methods for carrying out cryptographic analyses, reference ANSSI-CC-CRY-P01, current version.*
[CC]	*Information technology — Security techniques — Evaluation criteria for IT security* - *Part 1: Introduction and general model:* ISO/IEC 15408-1:2009 ; - *Part 2: Security functional components:* ISO/IEC 15408-2:2008 ; - *Part 3: Security Assurance components:* ISO/IEC 15408-3:2008 ; - et correctifs techniques associés / *and associated technical fixes*. Equivalent à la version CCRA */ equivalent to CCRA version :* - *Common Criteria for Information Technology Security Evaluation*, version 3.1, rev. *5, vol*. 1 -> 3, ref. CCMB-2017-04-001 -> CCMB-2017-04-003.
[CEM]	*Information technology — Security techniques — Methodology for IT security evaluation,* ISO/IEC 18045:2008, et correctifs techniques associés / *and associated technical fixes* Equivalent à la version CCRA */ equivalent to CCRA version :* - *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, version 3.1, rev. 5, ref. CCMB-2017-04-004.
[SotA IC]*	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT* Application *of CC to integrated circuits*, version 2, December 2024.

[SotA IC AP]*	*EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of attack potential to smartcards and similar devices*, version 2, February 2025.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2/07/2014.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques *Guide to cryptographic mechanisms: Rules and recommendations concerning the choice and sizing of cryptographic mechanisms* ANSSI-PG-083, version 2.04, 01/2020.

*Dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.

**Under the CCRA recognition agreement, the equivalent CCRA support document applies.*