PREMIER MINISTRE
Liberté
Égalité
Fraternité

Schéma européen de certification de cybersécurité fondé sur les critères communs (EUCC)

CERTIFICAT EUCC-3090-2026-35

Ce certificat est associé au rapport de certification EUCC-3090-2026-35

NPCT7xx TPM2.0 rev 1.59

(Type : Cartes à puce et dispositifs similaires)

configuration version 1.5.5.5

Développeur et Commanditaire : NUVOTON TECHNOLOGY CORPORATION, No. 4, Creation Rd. III, Hsinchu Science Park, Taiwan, R.O.C
Centre de certification : ANSSI
Centre d'évaluation : SERMA SAFETY & SECURITY

Critères Communs version 3.1 révision 5

ISO/IEC 15408:2009 et ISO/IEC 18045:2008

Conformément au règlement d'exécution (UE) 2024/482

Niveau d'assurance	Niveau d'évaluation
Elevé	**EAL4 Augmenté** (ALC_FLR.1, ALC_DVS.2, AVA_VAN.4)

conforme au profil de protection :

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

Date de validité : date de signature + 5 ans.

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

Vincent Strubel

SÉCURITÉ CERTIFICATION

CC Critères communs
CERTIFICATION DE CYBERSÉCURITÉ
ÉLEVÉ
SUBSTANTIEL
BASIQUE
Niveau AVA_VAN.4
EUCC-3090-2026-35

cofrac
ACCREDITATION N°5-0669
Portée disponible sur www.cofrac.fr
CERTIFICATION DE PRODUITS ET SERVICES

Dans le cadre du CCRA, ce certificat est reconnu au niveau EAL2 augmenté de ALC_FLR.1.

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information.

Secrétariat général de la défense et de la sécurité nationale, Agence nationale de la sécurité des systèmes d'information
51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

Le produit, objet de cette certification, a été évalué par SERMA SAFETY & SECURITY (coordonnées disponibles sur le site https://cyber.gouv.fr) sis en France en appliquant la *Common Methodology for Information Technology Security Evaluation*, Critères Communs version 3.1 révision 5, conforme aux Critères communs, Critères Communs version 3.1 révision 5 ou ISO/IEC 15408:2009 et ISO/IEC 18045:2008.

Ce certificat s'applique uniquement à cette version spécifique de produit dans sa configuration évaluée. Il ne peut être dissocié de son rapport de certification complet. L'évaluation a été menée conformément aux dispositions du règlement d'exécution (UE) 2024/482 et du CCRA. Les conclusions du centre d'évaluation, formulées dans le rapport technique d'évaluation, sont cohérentes avec les preuves fournies.

Ce certificat ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Les informations en matière de cybersécurité du produit sont disponibles ici : https://www.nuvoton.com/products/cloud-computing/security/trusted-platform-module-tpm/

Le développeur (le cas échéant commanditaire si différent du développeur) peut être contacté via cette adresse : security@nuvoton.com

La procédure complète de signalement d'une vulnérabilité est disponible sur le lien suivant : https://www.nuvoton.com/support/security/report-security-vulnerability/

Le commanditaire s'engage à alerter systématiquement et sans délai le centre de certification de toute vulnérabilité en lui diffusant l'analyse d'impact associée conformément à la procédure ANSSI-CC-VUL-P-01, version en vigueur.

Les informations sur l'autorité nationale de certification de cybersécurité en France sont disponibles ici : https://cyber.gouv.fr/cybersecurity-act.

Le centre de certification peut être contacté via cette adresse : certification@ssi.gouv.fr.