Docusign Envelope ID: 34CACF07-B7F3-8A2C-83F2-5DADBA357DA1

PREMIER MINISTRE
Liberté
Égalité
Fraternité

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

CERTIFICAT EUCC-3090-2026-75

Ce certificat est associé au rapport de certification EUCC-3090-2026-75

ST33G1M2A1, including optional library NesLib & optional library SFM

(Type : Cartes à puce et dispositifs similaires)

C06

Développeur & Commanditaire : STMICROELECTRONICS, 190 avenue Celestin Coq, ZI de Rousset-Peynier, 13106 ROUSSET
Centre de certification : ANSSI
Centre d'évaluation : THALES / CNES

Critères Communs version 2022, révision 1

ISO/IEC 15408:2022 et ISO/IEC 18045:2022

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

Niveau d'assurance	Niveau d'évaluation
Elevé	**EAL5 Augmenté** (ALC_DVS.2, ALC_FLR.2, AVA_VAN.5)

conforme au profil de protection :

Security IC Platform Protection Profile with Augmentation Packages version 1.0, BSI-CC-PP-0084-2014

Date de validité : date de signature + 5 ans.

Paris, le 23/10/2026 | 10:06 CEST

Vincent Strubel

SÉCURITÉ CERTIFICATION

CC Critères communs CERTIFICATION DE CYBERSÉCURITÉ — ELEVÉ / SUBSTANTIEL / BASIQUE — Niveau AVA_VAN.5 EUCC-3090-2026-75

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.2.

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

Docusign Envelope ID: 34CACF07-B7F3-8A2C-83F2-5DADBA357DA1

Le produit, objet de cette certification, a été évalué par THALES / CNES (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 2022, révision 1, conforme aux Critères communs, Critères Communs version 2022, révision 1 ou ISO/IEC 15408:2022 et ISO/IEC 18045:2022*.

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 : ST33G1M2A | Product - STMicroelectronics.

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

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

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.