

# Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

## **CERTIFICAT ANSSI-CC-2024/38**

Ce certificat est associé au rapport de certification ANSSI-CC-2024/38

### **STSAFE-V100-TPM & ST33KTPM2I**

#### **TPM FIRMWARE 10.512**

Développeur : STMICROELECTRONICS  
Commanditaire : STMICROELECTRONICS  
Centre d'évaluation : THALES - CNES

### **Critères Communs version 3.1, révision 5**

#### **EAL4 Augmenté**

**ALC\_DVS.2, ALC\_FLR.1, AVA\_VAN.5**

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

**Date de validité : date de signature + 5 ans.**

Paris, le 10 Janvier 2025

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

Vincent STRUBEL

[ORIGINAL SIGNE]



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 THALES – CNES sis en France en appliquant la *Common Methodology for Information Technology Security Evaluation*, version 3.1, révision 5, conforme aux Critères communs, version 3.1, révision 5.

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 SOG-IS, du CCRA et du schéma français. 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.