PREMIER MINISTRE

Liberté
Égalité
Fraternité

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

CERTIFICAT ANSSI-CC-2021/40

Ce certificat est associé au rapport de certification ANSSI-CC-2021/40

Trusted platform modules
ST33TPHF2X TPM Firmware 1.512 & 2.512
ST33GTPMA/I TPM Firmware 3.512 & 6.512

Développeur : STMICROELECTRONICS GRAND OUEST SAS
Commanditaire : STMICROELECTRONICS GRAND OUEST SAS
Centre d'évaluation : THALES / CNES

Critères Communs version 3.1, révision 5

EAL4 Augmenté

(ALC_FLR.1, AVA_VAN.5)

conforme au profil de protection : Protection profile PC Client Specific TPM
TPM Library specification Family 2.0, Level 0 Revision 1.38 version 1.2

Date de validité : date de signature + 5 ans.

Paris, le 23 septembre 2021

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

Guillaume POUPARD [ORIGINAL SIGNE]

Dans le cadre du CCRA, le produit est reconnu au niveau EAL2.

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.