PREMIER MINISTRE

Liberté
Égalité
Fraternité

Evaluation et certification de premier niveau de la sécurité des technologies de l'information

ANSSI-CSPN-2021-29

Ce certificat est associé au rapport de certification ANSSI-CSPN-2021-29

HP Sure Start Hardware Root of Trust

Version A0 (15.2.4) embarqué sur la puce NPCX998HA0BX

Catégorie de produit : Matériel et logiciel embarqué

Développeur : NUVOTON TECHNOLOGY ISRAEL LTD.
Commanditaire : HP INC.
Centre d'évaluation : CEA - LETI

Certification de sécurité de premier niveau
(Référentiel ANSSI)

Paris, le 10 décembre 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 CEA - LETI sis en France en appliquant la procédure ANSSI-CSPN-CER-P-01, version en vigueur.

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 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.