ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

Rabat, le 18 MARS 2026

CERTIFICAT DE CONFORMITE N°: CC-1/2026

*D*élivré par **L'autorité nationale des services de confiance pour les transactions électroniques (Direction Générale de la Sécurité des Systèmes d'Information/Administration de la Défense Nationale)**

— En application des dispositions des articles 8 et 17 de la loi n°43-20 relative aux services de confiance pour les transactions électroniques promulguée par le dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020).

Pour le :

DISPOSITIF QUALIFIE DE CREATION DE SIGNATURE ET DE CACHET ELECTRONIQUE (QSigCD/QsealCD)

Désignation du produit	Carte PCIe nShield Solo XC embarquée dans l'Appliance nShield Connect XC (Hardware Security Module)
Version du produit	- Numéro de modèle de la carte PCIe : NC4335N-000 rev 06 - Numéro de modèle de l'Appliance : NH2089 - Version de Solo XC firmware image: 12.60.15
Développeurs	ENTRUST
Fonctions	Génération et protection des données de création et de vérification de signature électronique, création et vérification de signature électronique

REFERENCES D'EVALUATION

Références normatives	Critères Communs version 3.1 révision 5 (ISO/IEC 18045) Référence du rapport de certification : CSA_CC_21008		
Niveau	EAL4+	**Augmentations :**	AVA_VAN.5 et ALC_FLR.2
Conformité à un profil de protection	EN 419221-5 Protection profiles for TSP Cryptographic modules -Part 5, version 1.0, enregistré sous la référence ANSSI-CC-PP-2016/05-M01		

NOTES :

- *Ce certificat de conformité est valide tant que les références d'évaluation ayant permis de le délivrer n'ont pas subi de modification. Tout changement doit être signalé immédiatement à la Direction Générale de la Sécurité des Systèmes d'Information(DGSSI) ;*
- *Le produit doit être utilisé conformément aux conditions et restrictions d'utilisation définies dans le rapport de certification selon la norme « Critères Communs » ;*
- *Le produit objet du présent certificat ne peut être considéré comme dispositif qualifié de création de signature et de cachet électronique au sens de la loi n°43-20 que si les données de création de signature/cachet électronique de l'utilisateur y sont conservées dans un environnement de gestion entièrement sous le contrôle de celui-ci ;*
- *Le produit objet du présent certificat ne peut pas être considéré comme dispositif qualifié de création de signature et de cachet électronique au sens de la loi n°43-20 lorsque le prestataire de services de confiance agréé l'utilise pour assurer la gestion des données de création de signature/cacher électronique pour le compte du signataire/créateur du cachet, mais il peut être utilisé comme composant d'un dispositif qualifié de création de signature/cachet électronique lequel doit être attesté par un certificat de conformité délivré par la DGSSI conformément à la réglementation en vigueur ;*
- *Lorsque les conditions selon lesquelles ce certificat de conformité a été délivré ne sont plus réunies ou qu'elles ont subi des modifications ultérieures, ou par tout autre fait porté à la connaissance de la DGSSI et remettant en cause la conformité du dispositif y associé aux exigences de la loi n° 43-20, celle-ci procède au retrait de ce certificat ;*
- *La délivrance de ce certificat ne constitue pas en soi une recommandation d'utilisation du produit en question par la DGSSI, et ne garantit pas qu'il soit totalement exempt de vulnérabilités exploitables ;*
- *Le présent certificat est valable **5 ans** à compter de la décision de certification du produit y associé selon la norme « Critères Communs », à savoir jusqu'au **27 juin 2027**.*

Le Directeur Général de la Sécurité des Systèmes d'Information

Signé: Le Général de Brigade A. BOUTRIG

ROYAUME DU MAROC * ADMINISTRATION DE LA DEFENSE NATIONALE * Direction Générale de la Sécurité des Systèmes d'Information