PREMIER MINISTRE

Liberté
Égalité
Fraternité

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

CERTIFICAT ANSSI-CSPN-2026/14

Ce certificat est associé au rapport de certification ANSSI-CSPN-2026/14

ULS4 et SEAL System

SEAL Exploitation 2025.2 (40), ULS4 – Firmware 2.38, MCS4 – Firmware 2.11

Catégorie de produit : **Identification, authentification et contrôle d'accès**

Développeur : OMNITECH Security
Commanditaire : OMNITECH Security
Centre d'évaluation : OPPIDA

Certification de sécurité de premier niveau

(Référentiel ANSSI)

Date de validité : date de signature + 3 ans.

Paris, le 27/5/2026 | 18:55 CEST

Vincent Strubel

SÉCURITÉ TI CERTIFICATION

fixed time certification

Dans le cadre de l'accord de reconnaissance mutuelle BSZ_CSPN, ce certificat est reconnu par le BSI (Bundesamt für Sicherheit in der Informationstechnik).
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 OPPIDA 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 et de l'accord de reconnaissance mutuelle *Mutual recognition agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI*. 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.

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.