Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification
ANSSI-CSPN-2026/14

ULS4 et SEAL System

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

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

Vincent Strubel

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

Référence du rapport de certification

ANSSI-CSPN-2026/14

Nom du produit

ULS4 et SEAL System

Référence/version du produit

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

Catégorie de produit

Identification, authentification et contrôle d'accès

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

OMNITECH Security
18 avenue Cassiopée
33160 Saint-Médard-en-Jalles, France

Développeur

OMNITECH Security
18 avenue Cassiopée
33160 Saint-Médard-en-Jalles, France

Centre d'évaluation

OPPIDA
6 - 8 rue Firmin Gillot
75015 - Paris, France

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Authentification des badges
Lecture transparente entre le badge et la carte SAM
Dispositif anti-relais
Protection de l'utilisation d'un SAM
Dispositif anti-arrachement de la tête de lecture
Communications sécurisées entre l'ULS et la tête de lecture
Communications sécurisées entre l'ULS et le MCS
Communications sécurisées entre l'ULS et SEAL
Dispositif anti-effraction du coffret sécurisé
Protection de la configuration
Protection des journaux locaux

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

Signature du micrologiciel *(firmware)* Protection des journaux centralisés Communications sécurisées entre SEAL et la station SEAL Exploitation Politique de droits Stockage sécurisé des secrets dans l'ULS et le MCS
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Non

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet cyber.gouv.fr.

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

TABLE DES MATIERES

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

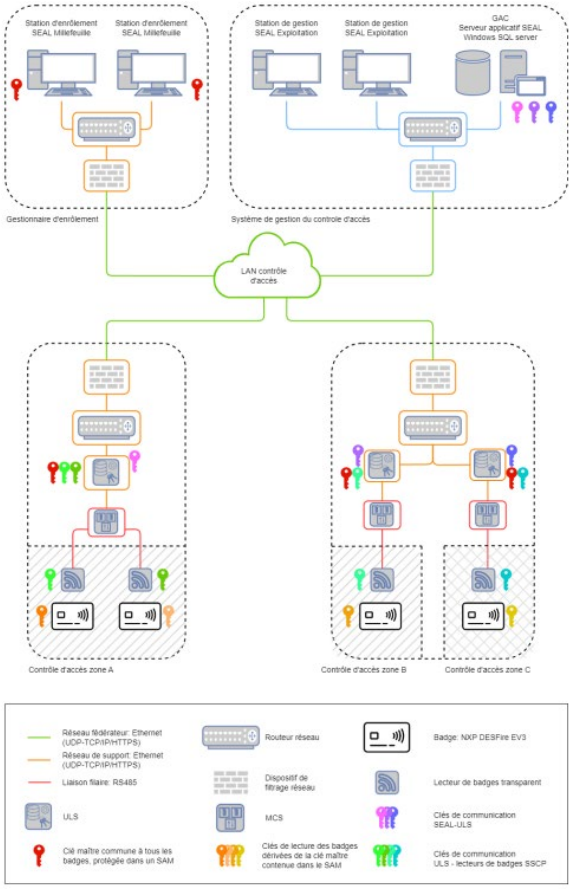
1 Le produit

1.1 Présentation du produit

Le produit évalué est « ULS4 et SEAL System, SEAL Exploitation 2025.2 (40), ULS4 – Firmware 2.38, MCS4 – Firmware 2.11 » développé par OMNITECH Security.

Ce produit est un système de contrôle d'accès physique (avec badges et têtes de lecture). Sont compris dans l'évaluation du produit le serveur GAC, L'UTL et le MCS.

La figure ci-dessous explicite l'architecture du produit :



Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☒	**6**	**identification, authentification et contrôle d'accès**
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	**ULS4 et SEAL System**
Numéro de la version évaluée	**SEAL Exploitation 2025.2 (40), ULS4 – Firmware 2.38, MCS4 – Firmware 2.11**

La version certifiée du produit peut être identifiée de la manière suivante :

- La version de SEAL peut être retrouvée depuis l'interface Web, dans le menu appelé « à propos », en haut à droite de la fenêtre :

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

- La version des MCS peut être retrouvée étant connecté sur le port série de l'ULS associé :

```
ULS4:~$ cat /tmp/firmware-spe.ver
MCS-b0475e500927=2.11.151 3.3.49
```

- La version de l'ULS peut être retrouvée en étant connecté sur son port série :

```
ULS4:~$ cat /tmp/firmware.ver
mlins_route.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_evt.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_tor.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_acs.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_dmn4.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_rtl.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_adv.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_gw_sam.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_mcs_update.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_mca4.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_sscpv2.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
mlins_uls_update.d=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
evtsend=MLINS ULS4 v2.38.194 250911/Omnitech rev:d691ca7
```

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- authentification des badges ;
- lecture transparente entre le badge et la carte SAM ;
- dispositif anti-relais ;
- protection de l'utilisation d'un SAM ;
- dispositif anti-arrachement de la tête de lecture ;
- communications sécurisées entre l'ULS et la tête de lecture ;
- communications sécurisées entre l'ULS et le MCS ;
- communications sécurisées entre l'ULS et SEAL ;
- dispositif anti-effraction du coffret sécurisé ;
- protection de la configuration ;
- protection des journaux locaux ;
- signature du micrologiciel (*firmware*) ;
- protection des journaux centralisés ;
- communications sécurisées entre SEAL et la station SEAL Exploitation ;
- politique de droits ;
- stockage sécurisé des secrets dans l'ULS et le MCS ;

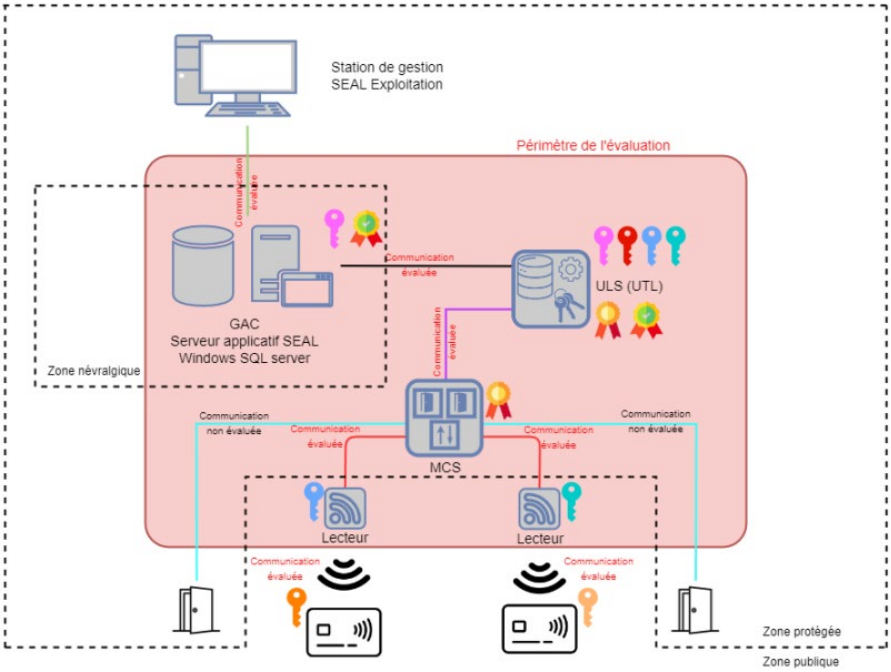
Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

1.2.4 *Configuration évaluée*

La configuration évaluée correspond à

- une station de gestion Windows 10 responsable du logiciel SEAL Exploitation ;
- un serveur (GAC) Windows 10 responsable de la base de données MSSQL et du serveur applicatif SEAL ;
- *firewall*/Routeur Fortinet responsable des sous-réseaux ;
- un boitier ULS4 ;
- un boitier MCS4 ;
- deux portes complètes avec chacune un lecteur transparent de badges, une ventouse de fermeture, un bouton d'ouverture à l'intérieur et un bouton d'ouverture d'urgence intérieur.

La plateforme de test est constituée des éléments suivants :



Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-07].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

La TOE a été livrée déjà configurée par le client.

2.2.1.3 Notes et remarques diverses

Sans objet

2.2.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

Le code source n'a pas fait l'objet d'une revue dans le cadre de cette l'évaluation.

L'évaluateur a revu le code source de l'intégralité du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies.

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « ULS4 et SEAL System, SEAL Exploitation 2025.2 (40), ULS4 – Firmware 2.38, MCS4 – Firmware 2.11 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (*Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Environnement de contrôle d'accès SEAL System avec ULS4 Cible de sécurité – CSPN, version 1.4, 14 octobre 2025 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Environnement de contrôle d'accès SEAL System avec ULS4 Cible de sécurité – CSPN, version 1.5-pub, 30 avril 2026
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN ULS4 et SEAL System – NAVY2, OPPIDA/CESTI/2026/NAVY2/RTE, version 1.1, 16 avril 2026
[GUIDES]	Guide d'utilisation du produit : - Support Formation - SEAL System ACS - Exploitation - SEAL Exploit - AD.pdf, version AD - Support Formation - SEAL System ACS - Gestion des droits d'accès.pdf, version EA - Support Formation - SEAL System ACS - Présentation Gamme - FF.pdf, version FF - Support Formation - SEAL System ACS - Procédures Maintenance - SEAL Exploit - ULS-4 - AB.pdf, version AB Guide d'installation du produit : - Procédures de maintenance et d'exploitation d'une installation CSPN : Guide de maintien en conditions de sécurité, version 40.0-b5bd61b50aec - Guide de l'exploitant de SEAL 2025.1 Service du Développement Logiciel, Omnitech Security, version 40.0.20387.1124 - ULS4 secured - mise en service.html version 1.2.186 - ULS4 secured - preparation atelier.html version 1.2.186

Docusign Envelope ID: 0F5CFD9D-DEDD-8260-82C5-2C2A1F611C97

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 12 juillet 2025. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0,6 mars 2024.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-07]	Note d'application - Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, référence ANSSI-CSPN-NOTE-07, version 2.1, 13 février 2025.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement*,version 2.0, mai 2024.