



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CSPN-2021/06

UTL ULS PoE Secured

Version 1.70.59

Paris, le 16 mars 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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 présumées 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.

Référence du rapport de certification	ANSSI-CSPN-2021/06
Nom du produit	UTL ULS PoE Secured
Référence/version du produit	Version 1.70.59
Catégorie de produit	Identification, authentification et contrôle d'accès
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	OMNITECH SECURITY Bâtiment Omega, 18 rue Cassiopée, CS 10152 33160 Saint-Médard-en-Jalles, France
Développeur	OMNITECH SECURITY Bâtiment Omega, 18 rue Cassiopée, CS 10152 33160 Saint-Médard-en-Jalles, France
Centre d'évaluation	OPPIDA 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées	Authentification des utilisateurs et badges Chiffrement des échanges entre le badge et la centrale Communications d'administration sécurisées Protection de la configuration Protection des logs Anti-arrachement des lecteurs de badges Anti-effraction du coffret de l'ULS-POE secured
Fonctions de sécurité non évaluées	Néant
Restriction(s) d'usage	Non

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 www.ssi.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	7
1.2.1	Catégorie du produit	7
1.2.2	Identification du produit	7
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée	7
2	L'évaluation.....	9
2.1	Référentiels d'évaluation.....	9
2.2	Charge de travail prévue et durée de l'évaluation.....	9
2.3	Travaux d'évaluation	9
2.3.1	Installation du produit.....	9
2.3.2	Analyse de la documentation.....	9
2.3.3	Revue du code source (facultative).....	9
2.3.4	Analyse de la conformité des fonctions de sécurité	10
2.3.5	Analyse de la résistance des mécanismes des fonctions de sécurité	10
2.3.6	Analyse des vulnérabilités (conception, construction, etc.)	10
2.3.7	Analyse de la facilité d'emploi	10
2.4	Analyse de la résistance des mécanismes cryptographiques	10
2.5	Analyse du générateur d'aléas.....	10
3	La certification	11
3.1	Conclusion.....	11
3.2	Recommandations et restrictions d'usage.....	11
ANNEXE A.	Références documentaires du produit évalué	12
ANNEXE B.	Références à la certification.....	13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « UTL ULS PoE Secured, Version 1.70.59 » développé par OMNITECH SECURITY.

La solution ULS PoE Secured est un système de contrôle d'accès par badge qui utilise un lecteur totalement transparent. Le lecteur n'embarque aucune logique applicative et n'agit que comme un dispositif de lecture et de transport d'information (le lecteur ne fait que transmettre les informations, aucune opération cryptographique n'est effectuée par ce dernier).

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

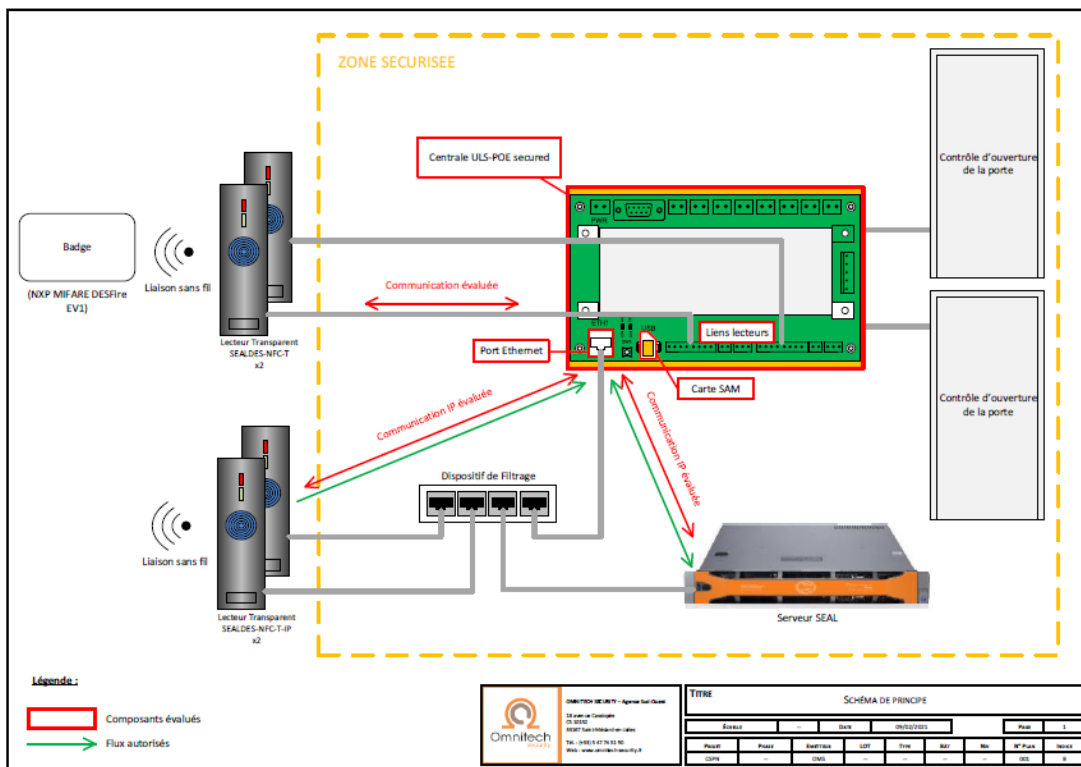


Figure 1 - Architecture Produit.

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

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

1.2.2 Identification du produit

Produit	
Nom du produit	UTL ULS PoE Secured
Numéro de la version évaluée du produit	Version 1.70.59
Référence du produit	ULS2P-IP-POE

La version certifiée du produit peut être vérifiée :

- dans le fichier /tmp/firmware.ver disponible sur la centrale ULS PoE secured ;
- sur l'étiquette collée sur le PCB qui mentionne également le numéro de version.

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- authentification des utilisateurs et badges ;
- chiffrement des échanges entre le badge et la centrale ;
- communications d'administration sécurisées ;
- protection de la configuration ;
- protection des *logs* ;
- anti-arrachement des lecteurs de badges ;
- anti-effraction du coffret de l'ULS-POE secured.

1.2.4 Configuration évaluée

La configuration évaluée correspond à la version détaillée à la section 1.2.2

La plateforme de test est constituée des éléments suivants :

- 1 unité de traitement logique ULS2P-IP-POE avec carte SAM (référence NXP MIFARE SAM AV2) ;
- 1 lecteur de badge Ethernet (référence SEALDES-NFC-T-IP E663 2.37.1) ;
- 1 lecteur de badge RS485 (référence SEALDES-NFC-T-IP S663 2.37.1) ;
- 1 poste d'administration hébergeant le logiciel de gestion SEAL ;
- 1 switch Dlink ;
- des badges MIFARE Desfire EV1.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en ANNEXE B.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 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].

2.3.1 Installation du produit

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

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

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

L'évaluateur n'a procédé à aucune installation du produit. Le commanditaire a fourni une maquette préinstallée et prête à l'emploi, et a procédé à la mise en route du produit au côté de l'évaluateur.

2.3.1.3 Durée de l'installation

Sans objet.

2.3.1.4 Notes et remarques diverses

Néant.

2.3.2 Analyse de la documentation

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

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

2.3.3 Revue du code source (facultative)

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit. L'analyse a été effectuée manuellement.

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

2.3.4 Analyse de la conformité des fonctions de sécurité

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

2.3.5 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.

2.3.6 Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur les briques logicielles tierces, mais se sont révélées inexploitable pour le niveau d'attaquant considéré.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitable pour le niveau d'attaquant considéré dans le contexte défini par la cible de sécurité [CDS].

2.3.7 Analyse de la facilité d'emploi

2.3.7.1 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.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le produit est facile à utiliser et ne nécessite pas de formation particulière pour son utilisation.

2.3.7.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Des non-conformités au RGS (voir [RGS]) ont été identifiées, mais celles-ci n'engendrent pas de vulnérabilités exploitables pour le niveau d'attaquant visé.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé, il en ressort que le produit utilise soit un composant externe, qui n'a pas fait l'objet d'une analyse au titre de cette évaluation, soit le générateur d'aléa du système d'exploitation de Windows qui n'introduit pas de vulnérabilités.

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 « UTL ULS PoE Secured, version Version 1.70.59 » 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].

Aucune recommandation particulière n'est formulée par l'évaluateur.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	ULS-POE secured avec lecteur transparent Version : BC ; Date : 9 février 2021.
[RTE]	Rapport Technique d'Réévaluation CSPN ULS-POE secured Référence : OPPIDA/CESTI/POE2/RTE/1.2 ; Version : 1.2 ; Date : 10 février 2021.
[GUIDES]	Omnitech Security Capture des échanges entre le badge et l'ULSPOE secured Référence : eaosca3 ; Version : AA.

ANNEXE B. Références 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]	<p>Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020.</p> <p>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019.</p> <p>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018.</p> <p>Documents disponibles sur www.ssi.gouv.fr.</p>
[RGS]	<p>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.</p>