« Ensemble, construisons l'@venir » ®

ULS-POE secured avec lecteur transparent

Cible de sécurité CSPN

Auteur	Modification	Version
PGE	01/08/2017	AA
PGE	11/04/2018 – mise à jour de la version du firmware.	AB
SDO	22/11/2018 – prise en compte des remarques issues des pré-tests CSPN. §3.2 : Mise à jour de la version du firmware. §3.2 : Précision sur la matrice de flux IP. §6.1 : authentification des badges, non du porteur. §6.1 et §6.2 : fonctions de sécurité 6 (anti-arrachement du lecteur) et 7 (anti-effraction du coffret de l'ULS-POE).	AC

OMNITECH SECURITY Tél : +33 547 745 190 http://www.omnitech-security.fr
25 rue Marcel Issartier Fax : +33 547 748 030
F-33700 MERIGNAC SAS au capital de 250 000 €
R.C.S. BORDEAUX 482 646 015 00040 APE 7112B

PGE	18/05/2020 – prise en compte des remarques et levée des vulnérabilités exposées dans le RTE v. 1.1. 22/06/2020 §1.2 Firmware 1.70.53 §2.1 Mise à jour des illustrations §2.2.4 Manquait "3", le nombre d'entrées RSA dans le SAM §3.1 Remise en forme de la figure du périmètre évalué §3.2 Le dispositif de filtrage présenté n'est pas un pare-feu, mais un switch paramétré avec un VLAN asymétrique. Dans le reste du document, utilisation homogène du terme "dispositif de filtrage IP" au lieu de pare-feu. §3.4 Ajout section "Agents menaçants". §3.5 Clarification des formulations des hypothèses 5 et 7. §4.2 on précise que les logs sont en zone sécurisée.	BA
PGE	§1.2 Firmware 1.70.59	BB
PGE	09/02/2021 – prise en compte du RTE OPPIDA/CESTI/POE2/RTE/1.1 §1.2 Coquille : firmware 1.70.59 §3.1 Schéma : l'évaluation porte aussi sur le lien IP vers le serveur. §3.2 La matrice de flux ne référence plus les ports. Pied de document : Mise à jour de l'adresse du siège de l'entreprise.	BC

TABLE

✦

Glossaire

Dans le document, le mot *utilisateur* renvoie au client du produit. Lorsque le contexte ne permet pas de le distinguer des usagers du système, c'est-à-dire les personnes possédant un badge et souhaitant utiliser le produit pour ouvrir une porte, on utilisera le terme *usager* ou *porteur de badge*.

1 Identification

1.1 Identification du document

Ce document décrit la cible de sécurité relative au contrôleur de porte ULS-POE secured de la solution Omnitech Security en vue de l'obtention d'une certification de sécurité de premier niveau des technologies de l'information (CSPN).

1.2 Identification du produit

Editeur	Omnitech Security
Site de l'éditeur	https://www.omnitech-security.fr/
Nom commercial du produit	ULS-POE secured
Identification technique du produit	ULS2P-IP-POE[1] Scellé « ULS-POE secured »[2]
Version évaluée	Firmware 1.70.59
Catégorie de produit	Identification, authentification et contrôle d'accès

2 Argumentaire du produit

2.1 Description générale du produit

Dans les systèmes de contrôle d'accès par badge traditionnels, le lecteur de badge possède une certaine intelligence, et suit le scénario suivant :

[1] ULS2P pour « ULS 2 portes », IP pour « sur réseau IP », POE pour « alimentée par POE ».
[2] Le scellé est une étiquette anti-fraude prouvant que l'ULS est rendue conforme à ce document.

1. Le lecteur s'authentifie auprès de la puce,
2. Le lecteur lit les données qui l'intéressent depuis la puce,
3. Le lecteur rentre en communication avec la centrale ULS-POE secured et lui transmet les données qu'il vient de lire depuis la puce.

Ce mode de fonctionnement comporte 2 failles majeures :

- Le lecteur, qui est à l'extérieur de la zone sécurisée (devant la porte…) contient la ou les clés permettant de s'authentifier auprès des puces. Si un lecteur volé en vient à être compromis, le système entier est compromis,
- La centrale ne connaît de la puce que ce que le lecteur veut bien lui en dire. Un lecteur corrompu, ou remplacé par un dispositif capable de se faire passer pour un lecteur, peut transmettre à la centrale des données arbitraires, ou rejouer des données passées.

La centrale ULS-POE secured permet de corriger ces failles de sécurité majeures en optant pour un lecteur totalement transparent. Le lecteur n'embarque plus aucune logique applicative et n'agit que comme un dispositif de lecture et de transport d'information. Le scénario de lecture du badge devient alors :

1. La centrale s'authentifie auprès de la puce,
2. La centrale lit les données qui l'intéressent depuis la puce, via le lecteur transparent (le lecteur ne fait que transmettre les informations, aucune opération cryptographique n'est effectuée par ce dernier).

Les failles de sécurité précédentes sont comblées :

- Les clés d'authentification sont désormais situées au niveau de la centrale, donc à l'intérieur de la zone sécurisée, voire dans une zone encore plus sécurisée (armoire technique protégée),
- La transaction s'effectuant en temps réel avec la puce, aucune injection arbitraire et aucun rejeu n'est possible.

Une carte SAM peut également être utilisée pour renforcer la sécurité sur le contrôle des clés de chiffrement.

La centrale peut être connectée à des lecteurs de portes en RS485 ou en Ethernet (TCP/IP).

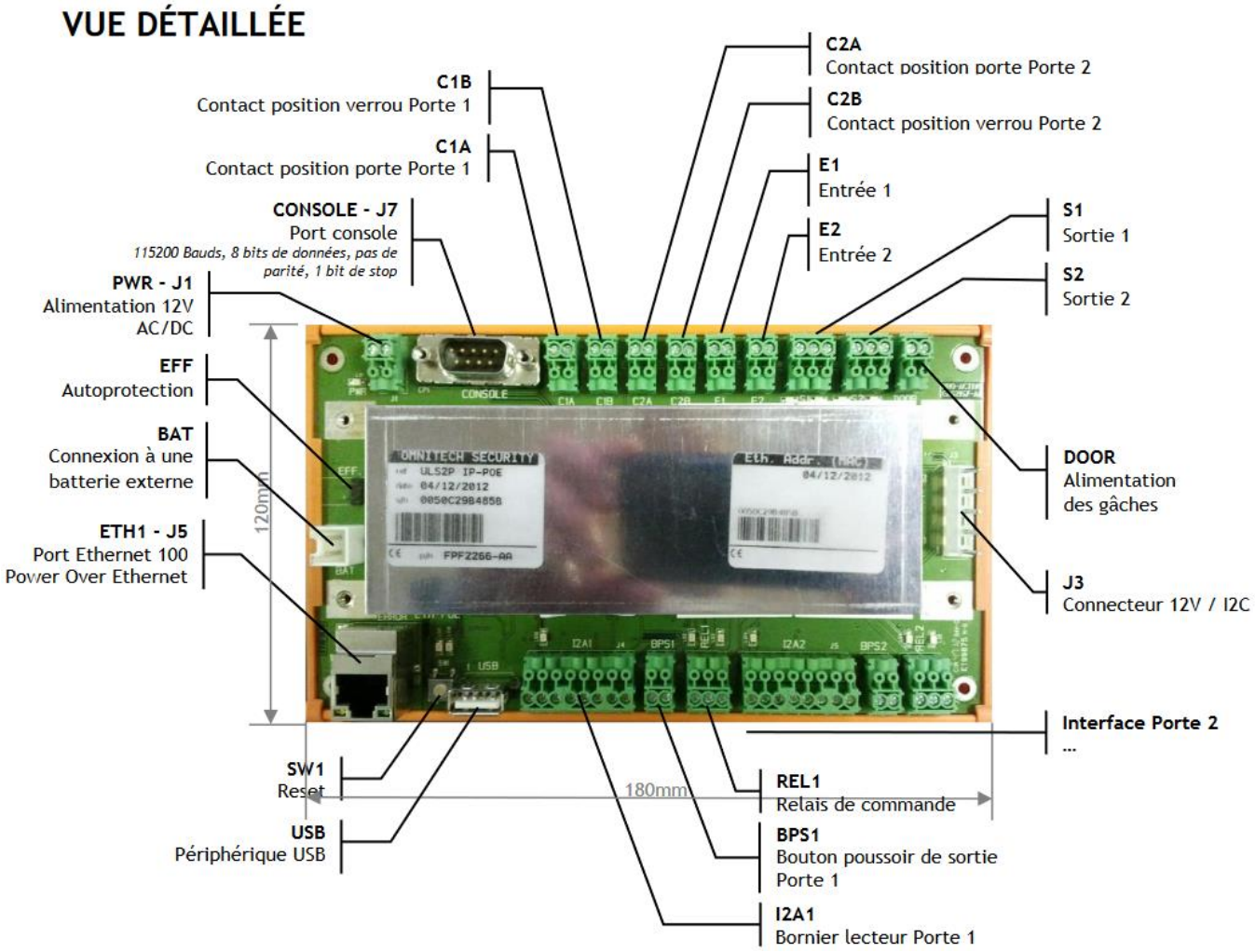


Figure 1 : Vue d'une centrale ULS-POE secured

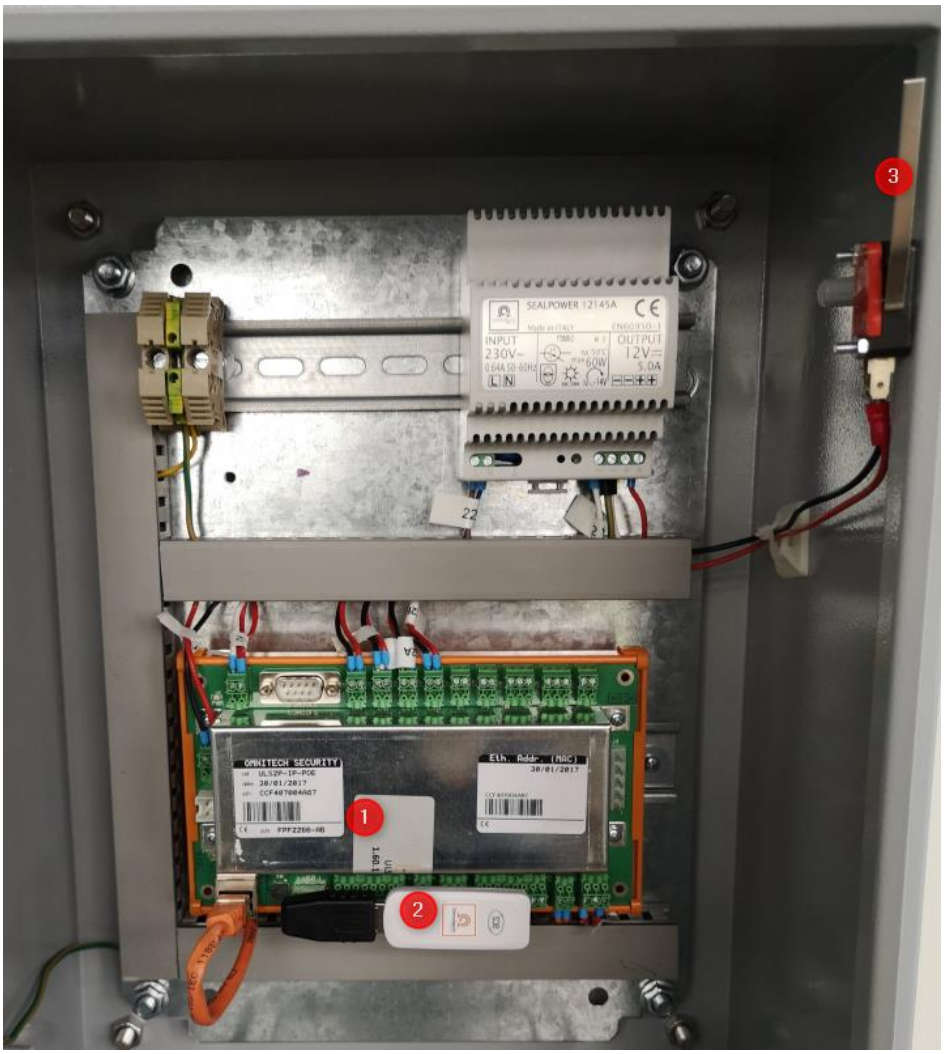


Figure 2 : Centrale ULS-POE secured en situation ; (1) étiquette VOID collée sur le capot et le PCB mentionnant « ULS-POE secured » et sa version de firmware ; (2) lecteur de carte SAM ; (3) contact anti-effraction sur l'ouverture du coffret contenu l'ULS-POE.

2.2 Mise en œuvre dans une architecture complète

2.2.1 Omnitech Security, sécurité et sûreté

Filiale du groupe français DOM Security depuis Novembre 2014, OMNITECH Security est éditeur de logiciel de Sureté et fabricant de matériel de contrôle d'accès depuis 2005.

OMNITECH Security, est une filiale du groupe DOM Security créé en 1993, construite autour de 4 métiers :

- Éditeur de solutions logicielles de sûreté ouvertes

Notre progiciel d'Hypervision SEAL s'adapte à tous vos contextes complexes, de vidéosurveillance, contrôle d'accès, intrusion, périmétrie et gère aujourd'hui les plus grands sites européens.

- Constructeur de matériels de contrôle d'accès

Nos produits industriels, conçus et fabriqués en France, sont entièrement IP. L'architecture basée sur la technologie LON™ vous garantit des déploiements rapides et économiques. Notre filiale SpringCard nous confère une très grande expertise dans le domaine du RFID et l'identification des personnes.

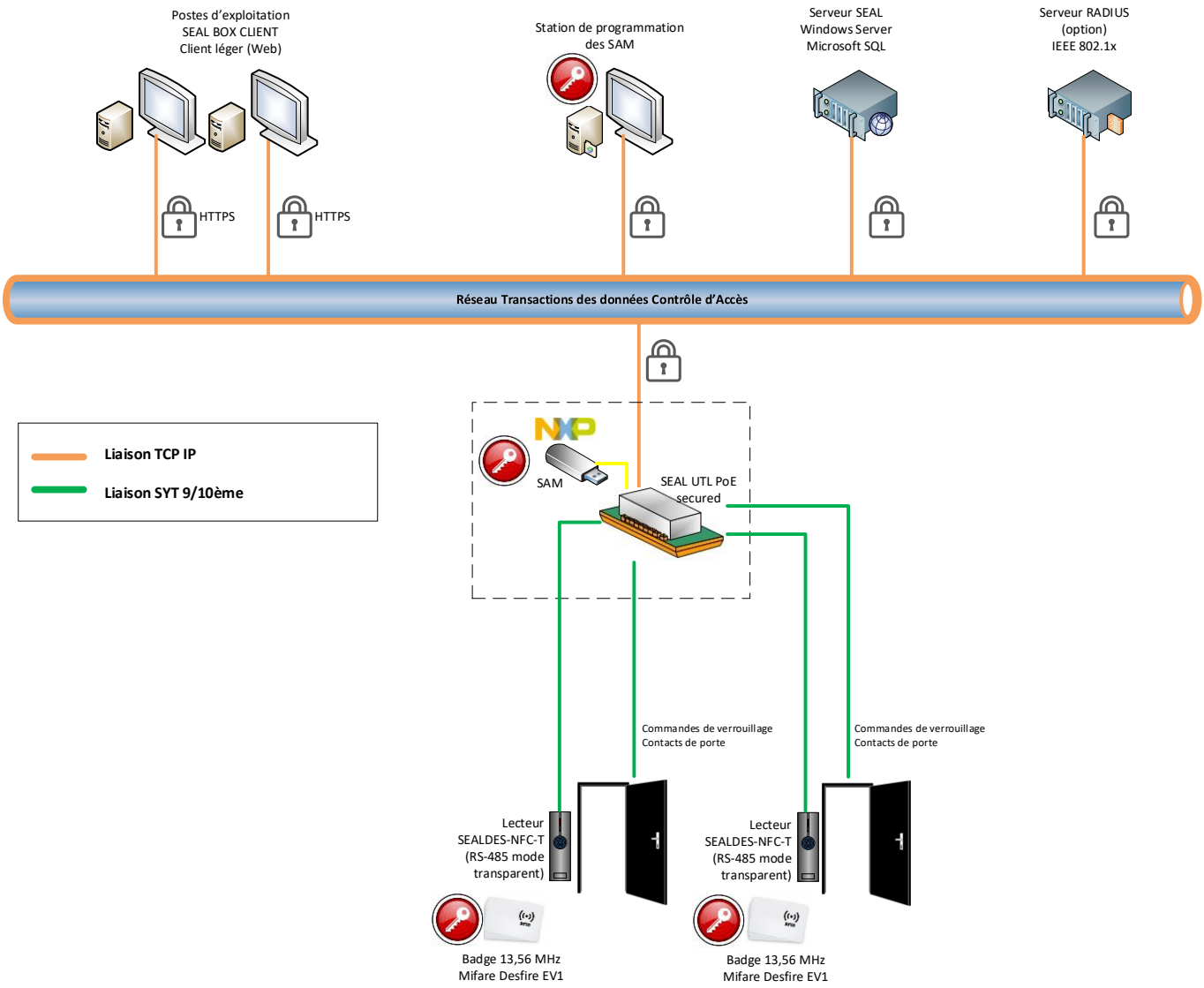
- Solution sur mesure

Nous travaillons en étroite collaboration en mode projet avec nos clients installateurs et clients finaux.

- Maintenance et support

Nous sommes reconnus pour notre savoir-faire et notre réactivité, et disposons d'une plate-forme de maintenance et support technique permettant de gérer des contrats H24. Notre contrat SEAL Care personnalisé garantit à nos clients des taux de disponibilité des installations proches de 100%.

2.2.2 Architecture exemple



2.2.3 La sécurité de bout en bout

2.2.3.1 Communications Serveur ←→ UTL

Les UTL « ULS-POE secured » disposent nativement de ports Ethernet intégrés (pas de cartes ou d'interfaces) pour communiquer avec le serveur de gestion SEAL en protocole TCP/IP

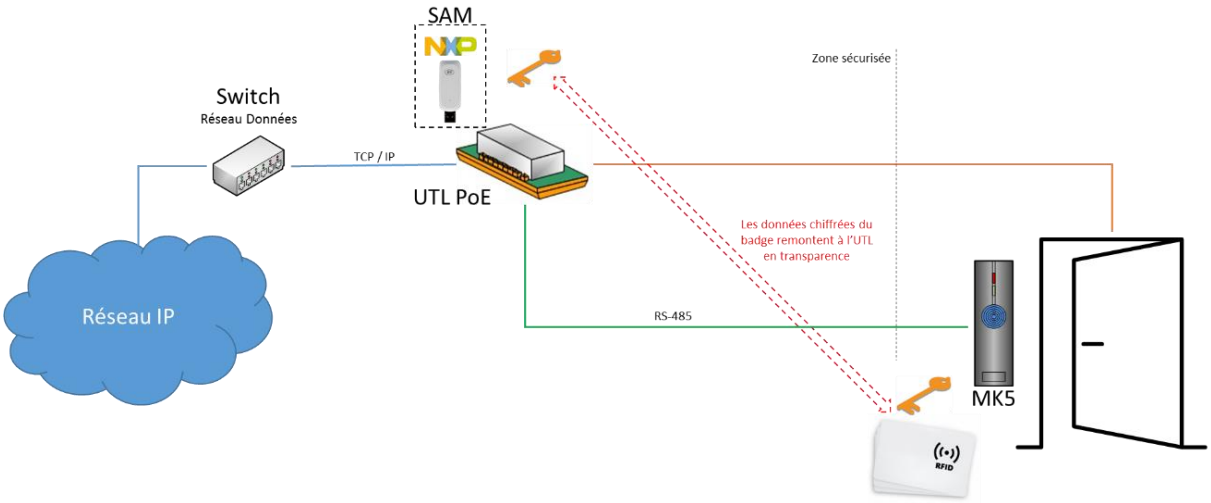
L'interface IP de l'UTL « ULS-POE secured » est protégée par un dispositif de filtrage (pare-feu, VLAN asymétrique ou autre), n'autorisant que les flux des lecteurs de badges vers UTL, et des communications du serveur SEAL vers UTL. Ces deux types flux sont séparés l'un de l'autre.

Algorithme utilisé pour la confidentialité des communications Serveur ←→ UTL : AES128-CBC + HMAC-SHA256.

2.2.3.2 Communication UTL ←→ Badge

Les liens physiques entre les lecteurs de badge et l'UTL « ULS-POE secured » sont des câbles RS485 et Ethernet. Les éléments qui transitent sur le réseau RS-485 ou IP entre le lecteur

et l'UTL sont exactement les mêmes que ceux qui transitent dans l'air entre le lecteur et la puce sans contact, il n'y a donc pas de sécurisation particulière à mettre en place.



Ce réseau de communication n'introduit pas de vulnérabilité, la sécurité s'établissant entre les deux extrémités de la chaîne.

Il n'est donc pas nécessaire de sécuriser la communication entre le lecteur transparent et l'UTL « ULS-POE secured » :

- Cela permet d'optimiser les performances en supprimant les latences ou les temps de traitement introduits par une couche cryptographique supplémentaire
- Cela permet d'analyser objectivement la sécurité de la transaction et de l'optimiser de bout en bout, sans avoir à compter sur des mécanismes cryptographiques intermédiaires.

2.2.4 La carte SAM

Le système avec lecteur transparent qui vient d'être décrit reste perfectible sur un point : les clés d'authentifications situées dans l'UTL « ULS-POE secured » peuvent encore faire l'objet d'une attaque, soit à travers le réseau informatique, soit en dérobant une UTL pour en analyser le contenu.

Pour résoudre cette faille, les clés d'authentification sont protégées par un dispositif dont le niveau de sécurité est prouvé, à savoir une carte SAM (Secure Access Module), c'est-à-dire une carte à puce dédiée à la cryptographie, qui pourra effectuer les calculs cryptographiques pour le compte de l'UTL sans jamais révéler les clés qu'elle contient.

Les ULS-POE secured OMNITECH Security disposent d'une carte SAM qui est insérée dans un adaptateur mini-SIM vers USB lui-même raccordé sur le port USB des UTL.

La carte SAM retenue est la NXP MIFARE DESFire EV1. Il s'agit d'un circuit pour carte sans contact 100% conforme à la norme ISO/IEC 14443A, qui assure les fonctions de stockage de données et de communication sécurisée.

Les mécanismes de sécurité (authentification et chiffrement) reposent sur les algorithmes AES. La carte SAM implémente tous les mécanismes de sécurité de la puce DESFire EV1, ainsi que l'algorithme RSA pour la vérification (ou la création) de signatures numériques. Elle est aussi capable de diversifier les clés en fonction de l'UID de la puce DESFire qui lui est présentée, et peut stocker 3 versions de chaque clé, ce qui autorise la rotation.

La carte SAM est verrouillée à chaque démarrage.

Capacités et limites des SAM NXP AV2

Les SAM NXP AV2 disposent des caractéristiques suivantes :

- 128 entrées pour stocker des clés d'authentification (avec 3 versions de clé dans chaque entrée). 1 entrée est réservée pour le déverrouillage, 1 autre pour la clé d'administration du SAM, ce qui laisse 126 entrées disponibles.
- 3 entrées pour stocker des clés RSA. Les entrées 0 et 1 peuvent contenir une paire RSA complète et seront donc utilisées de préférence pour la génération de signatures, l'entrée 2 ne peut contenir qu'une clé publique et sera donc utilisée de préférence en vérification.

Compte tenu de ces caractéristiques, le facteur limitant est le nombre de clés RSA. Une UTL implémentant complètement le comportement décrit dans ce document pourra supporter jusqu'à 3 « templates » de lecture de cartes DESFire EV1.

2.2.5 Station de configuration des cartes SAM (salle blanche)

La station de programmation des SAM permet l'encodage des SAM (SAM NXP AV2) implantées dans les UTL, protégeant les données sensibles.

Cette station permettra la création et l'initialisation de nouvelles SAM de lecture à intégrer dans les UTL.

Cette station doit être mise en place dans une salle « blanche » sécurisée et ne pas être connectée au réseau de sûreté.

2.2.6 Station de création des badges (salle blanche)

La station de création des badges permet l'encodage des badges de contrôle d'accès des usagers. Cette station comporte une SAM d'écriture pour inscrire dans des badges vierges les données de sécurité.

Cette station permettra la création et l'initialisation de nouveaux badges.

Cette station doit être mise en place dans une salle « blanche » sécurisée et ne pas être connectée au réseau de sûreté.

2.2.7 Serveur SEAL

Le serveur applicatif SEAL assure l'Hypervision globale de la solution de sûreté.

SEAL est une solution d'exploitation unifiée, elle est constituée d'un serveur central applicatif accessible depuis tous les postes raccordés au réseau de sureté et disposant des droits, mode de fonctionnement client / serveur.

SEAL présente une IHM ergonomique et simple d'utilisation accessible en client léger Web qui organise et hiérarchise les informations disponibles

Le serveur SEAL est constitué d'un serveur sous environnement Microsoft Windows serveur et une base de données Microsoft SQL Server, ouverte et non propriétaire.

2.2.8 Postes d'exploitation

Depuis les postes d'exploitation, les opérateurs accèdent à l'IHM SEAL pour le traitement, la programmation et la gestion des accès.

Cette gestion complète et centralisée permet également les échanges avec les contrôleurs déployés sur le terrain et la programmation de toutes les informations de configurations pour les usagers, les droits d'accès et les événements / alarmes horodatés dans une base de données.

2.2.9 Serveur Radius (non déployé par OMNITECH Security)

Le serveur RADIUS a pour objectif d'identifier tous les équipements se connectant sur le réseau transactionnel, ce qui garantit contre toute connexion physique non autorisée. Les équipements actifs de type « switch » réalisent une isolation physique du port sur lequel l'équipement non identifié est connecté.

2.3 Description de la manière d'utiliser le produit

La centrale ULS-POE secured comporte une base de données interne listant les badges autorisés et les périodes d'autorisation. Cette base est alimentée via un SDK communiquant via TCP/IP avec la centrale sur le port 4001. Cette alimentation se fait via un serveur SEAL.

Le firmware de la centrale peut être mis à jour via un port série présent sur la console.

La centrale est configurée hors réseau, et connecté sur le réseau final une fois proprement configurée.

Les badges sont créés en salle blanche, coupée de tout réseau extérieur, en utilisant la clé de lecture de l'ULS. Cette clé de lecture, et la clé d'écriture associée nécessaire pour la création du badge, sont la propriété du client final.

Le client final a la responsabilité de ne diffuser cette clé que par des moyens sécurisés, et aux seules personnes habilitées. Ainsi, Omnitech Security recommande que la salle blanche pour la création des badges soit physiquement coupée de tout réseau informatique, et accessible aux seules personnes habilitées à la création des badges.

Si le client final souhaite installer plusieurs de ces salles blanches – par exemple, sur des sites différents – il pourra choisir de cloisonner les sites en utilisant des clés différenciées.

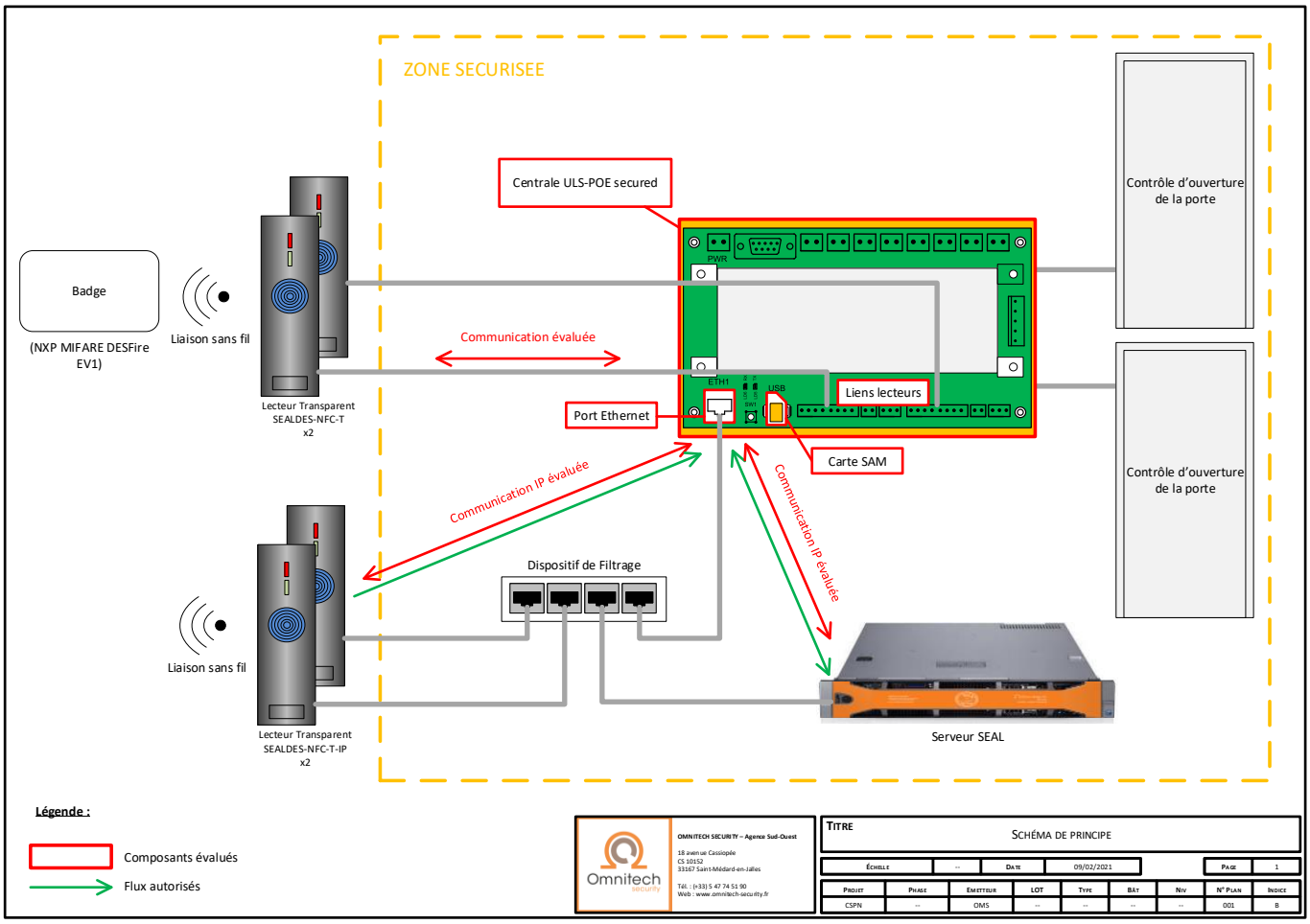
De même, l'application DESFire est une *application réservée aux lecteurs de contrôle d'accès*, et possède une clé dédiée différente des éventuelles autres applications encodées dans les badges. Dans la mesure du possible, afin de limiter le nombre d'entités ayant connaissance de la clé de lecture, Omnitech Security recommande de limiter la distribution de la clé, même sous forme sécurisée, aux seules personnes nominativement identifiées ayant la responsabilité de la préparation du matériel à installer ou à mettre à jour.

Le client final doit disposer d'un règlement régissant la distribution, l'utilisation et la récupération des badges. Ce règlement précise par exemple qu'un badge est remis à son porteur contre une décharge, conservée par le client final ; que lorsqu'un badge perdu est retrouvé, il est détruit ; etc.

Par devoir de conseil et par souci d'accompagnement, Omnitech Security rappelle l'ensemble de ces bonnes pratiques à ses clients finaux. En particulier, lorsqu'une disposition particulière prise par le client n'apparaît pas en adéquation avec le niveau de sécurité envisagé, Omnitech Security en informe le client.

3 Définition du périmètre

3.1 Périmètre évalué



Seule la centrale ULS-POE secured et ses interfaces sont incluses dans le périmètre de l'évaluation. La centrale est dotée d'une carte SAM, dont la sécurité intrinsèque ne fait pas partie de l'évaluation.

Le lien entre la centrale et le mécanisme d'ouverture de la porte est considéré comme sûr et n'est pas évalué, de même que le mécanisme d'ouverture de la porte.

En revanche, les lecteurs de badge ne sont pas considérés comme sûrs, et l'interface (câble RS485 et Ethernet) entre ces lecteurs et la centrale ULS-POE secured fait partie du périmètre de l'évaluation.

L'interface IP de la centrale est protégée par un dispositif de filtrage, hors périmètre de l'évaluation, considéré comme sûr et fonctionnel, n'autorisant que les flux lecteur IP vers centrale, et serveur SEAL vers centrale. Les lecteurs IP n'ont accès qu'au port nécessaire à leur fonctionnement sur la centrale.

Le serveur SEAL permettant de modifier les droits d'accès n'est pas inclus dans la cible. Seule la communication entre la centrale et les lecteurs de badge est considérée.

Les échanges avec le badge (requêtes et réponses) sont chiffrés, et impliquent systématiquement le SAM.

Les badges et leur sécurité intrinsèque (extraction des clés de chiffrement) ne sont pas inclus dans la cible.

3.2 Configuration évaluée

La centrale est considérée comme proprement installée. Son interface de configuration réseau FTP est désactivée, ainsi que son interface http ; la configuration initiale à la mise en service se fait en console par le port série.

Les liens entre les lecteurs de badge et la centrale sont des câbles RS485 et Ethernet.

La centrale dispose d'une carte SAM (NXP MIFARE SAM AV2.).

Les badges utilisent des puces NXP MIFARE DESFire EV1, et les lecteurs de badge sont des FunkyGate-DW PC/SC et leur équivalent IP (FunkyGate-IP PC/SC).

Précisément, les lecteurs de badge sont préparés en mode transparent, sous la référence SEALDES-NFC-T 2.37.1 (version série ; modèle technique FunkyGate-DW RDR NFC ; firmware « lecteur transparent » v2.37.1 ; étiquette VOID) et SEALDES-NFC-T-IP 2.37.1 (version IP ; modèle technique FunkyGate-IP RDR NFC ; firmware « lecteur transparent » v2.37.1 ; étiquette VOID).

Un serveur SEAL est installé, mais ne fait pas partie du périmètre d'évaluation.

Le dispositif de filtrage installé entre la centrale, les lecteurs IP et le serveur SEAL est un switch sur lequel a notamment été paramétré un VLAN asymétrique. Seuls sont autorisés les flux nécessaires au fonctionnement du produit : flux entrants sur la centrale, TCP depuis les lecteurs de badge, TCP et UDP depuis le serveur SEAL, et flux UDP sortant de la centrale vers le serveur SEAL. En particulier : les lecteurs de badge n'ont pas accès à l'interface d'administration de la centrale, qui nécessite une connexion sur la console de la centrale, ni au serveur SEAL lui-même. Ce dispositif de filtrage est en zone sécurisée.

La matrice des flux IP autorisés est la suivante :

Source	**Cible**	**Nature du flux**
ULS-POE secured	Lecteur transparent IP	Bidirectionnel Routage de la communication entre l'ULS et le badge.
ULS-POE secured	Serveur SEAL	Unidirectionnel Événements (passages de badges, alarmes…)
Serveur SEAL	ULS-POE secured	Bidirectionnel Programmation de la centrale (droits d'accès, horaires…)
Serveur SEAL	ULS-POE secured	Unidirectionnel Commandes (ouverture à distance, libération ou blocage…)

3.3 Utilisateurs typiques

Il y a 2 catégories d'utilisateur :

- L'administrateur : crée les cartes d'accès, et configure le système, modifie les droits d'accès.
- Les porteurs de badge (usagers du système) : ces acteurs vont chercher à s'authentifier via leur badge auprès du contrôleur de porte pour déclencher l'ouverture d'une porte.

3.4 Agents menaçants

Les agents menaçants sont :

- L'attaquant cherchant à espionner la communication entre le badge et l'ULS ; cet agent cherchera typiquement à accéder au câble IP ou série situé derrière le lecteur ;
- L'attaquant essayant de se faire passer pour un porteur de badge ; cet agent procèdera par exemple par une attaque par relais.

3.5 Hypothèses sur l'environnement

1. Administrateur de confiance

Les administrateurs sont considérés comme de confiance, non hostiles et formés à l'utilisation du produit.

2. Centrale et dispositif de filtrage IP positionnés dans un environnement sécurisé

La centrale de contrôle ainsi que le dispositif de filtrage IP la protégeant sont placés dans une zone physique sécurisée, qui n'est accessible qu'aux administrateurs.

3. Dispositif de filtrage IP

Le dispositif de filtage IP protégeant la centrale est considéré comme bien configuré, efficace, correctement dimensionné. Seuls les flux minimums nécessaires et légitimes sont autorisés, et donc accessibles.

4. Lien sécurisé entre la centrale et le contrôleur de porte

La liaison entre la centrale et le contrôleur de porte est considérée comme sécurisée, par son environnement physique. Il n'est pas possible en particulier d'y injecter du trafic ou de modifier le trafic en cours d'échange.

5. Badges et carte SAM sûrs

a) Les badges et la carte SAM sont considérés comme sûrs : il n'est pas possible d'en extraire les clés de chiffrement.

b) Toutes les opérations internes aux puces des badges et de la carte SAM sont considérées comme sûres et correctement implémentées, et le générateur d'aléa de la carte SAM est un TRNG, conformément aux déclarations du fabricant.

6. Badges personnels

Les porteurs de badge ne confient pas leur badge à un tiers, et ne permettent pas l'accès à un tiers grâce à leur badge. Les cas de badges volés ou perdus sont également écartés.

7. Bonne création des badges et clés par l'utilisateur du produit

Les badges sont fournis par l'utilisateur du produit. La sécurité de la centrale ULS-POE secured suppose que les badges ont été créés et sont gérés conformément à l'état de l'art

et aux recommandations d'utilisation du produit (chiffrement des applications et activation du RID entre autres), et en particulier au niveau de la gestion par l'utilisateur du produit des cartes contenant les clés cryptographiques et de la génération de ces clés.

L'hypothèse 5 concerne le fonctionnement interne des cartes, tandis que l'hypothèse 7 concerne l'utilisation qui est faite de ces cartes.

4 Biens sensibles à protéger

4.1 Biens sensibles de l'environnement

1. Déplacements de l'utilisateur / vie privée

Si un attaquant parvient à reconnaitre le passage d'un même badge à plusieurs endroits, il est en mesure de suivre les déplacements d'un utilisateur, ce qui constituerait une atteinte à sa confidentialité. De plus, l'attaquant ne doit pas pouvoir déterminer si un utilisateur donné a accès à une porte donnée (ne peut pas obtenir la matrice des accès). De manière générale, il n'est pas possible de savoir quel utilisateur vient d'ouvrir une porte.

4.2 Bien sensibles du produit

2. Authentification usagers

Seuls les usagers ayant droit doivent être en mesure d'ouvrir la porte protégée.

3. Secrets Cryptographiques

Des clefs de chiffrements sont utilisées afin de garantir la confidentialité des échanges et l'authenticité / intégrité de certaines données. Ces clés ne doivent pas être divulguées.

4. Configuration

La configuration des équipements contient des données sensibles, comme la liste des usagers ayant droit d'accéder aux zones protégées.

5. Logs

Les logs des accès aux zones peuvent permettre de tracer les déplacements d'un utilisateur et porter atteinte à sa confidentialité. Ces logs se présentent sous la forme d'évènements, transmis sur le réseau en UDP, exclusivement dans la zone sécurisée.

4.3 Caractéristiques de sécurité des biens

Bien sensible	Confidentialité	Intégrité	Authenticité	Disponibilité
1. Déplacements de l'utilisateur / vie privé	X	X	X	
2. Authentification des usagers		X	X	X
3. Secrets Cryptographiques	X	X		X
4. Configuration	X	X		
5. Logs	X	X		

5 Menaces sur le système

5.1 Vecteurs d'attaque

1. Modification du lecteur de badge

Un attaquant peut tenter de démonter un lecteur de badge et modifier son fonctionnement nominal afin d'obtenir de la centrale l'ouverture de la porte.

2. Faux badge

Un attaquant peut tenter de créer un faux badge afin d'obtenir les accès à des zones autrement interdites.

5.2 Identification des menaces

1. Obtention non autorisée de l'accès

Un utilisateur, légitime ou non, obtient l'ouverture d'une porte à laquelle les contrôles en place sont supposés lui interdire l'accès.

2. Divulgation des déplacements d'un utilisateur

Un attaquant parvient à obtenir la liste des portes ouvertes ou tentatives d'ouverture d'un utilisateur, arrivant ainsi à suivre ses déplacements, en attaquant par exemple les logs d'accès de la centrale, ou en écoutant l'identifiant du badge au niveau du lecteur.

3. Divulgation des droits d'accès

Un attaquant obtient la liste des utilisateurs ayant le droit d'ouvrir une porte.

4. Modification de la configuration

Un attaquant parvient à modifier la configuration d'un équipement, pouvant par exemple retirer à un utilisateur légitime ses droits d'accès à une porte ou rajouter un utilisateur autorisé.

6 Fonctions de sécurité

6.1 Liste des fonctions de sécurité

1. Authentification des utilisateurs et badges

Les administrateurs sont authentifiés sur le système. L'authentification des badges est vérifiée avant l'ouverture de la porte.

2. Chiffrement des échanges sans fils entre le badge et la centrale

Les échanges entre la carte d'accès et la centrale de contrôle sont chiffrés par des clés partagées dérivées en clés de session. La carte SAM effectue les calculs cryptographiques pour la centrale. Au démarrage des échanges, le badge présente un RID.

3. Communications d'administration sécurisées

Les échanges effectués sur le port Ethernet avec le serveur SEAL (administration de la centrale ULS-POE secured) sont sécurisés. La configuration initiale de la centrale se fait par connexion directe sur la console de la centrale.

4. Protection de la configuration

La configuration et la liste des accès autorisés n'est modifiable que par les administrateurs.

5. Protection des logs

Les logs ne sont accessibles qu'aux personnes autorisées (les administrateurs).

6. Anti-arrachement des lecteurs de badges

En cas d'arrachement du lecteur de badge, ou en cas d'ouverture de son capot, le lecteur émet un bip sonore répété, se désactive, et un événement est émis vers la centrale ULS-POE secured.

7. Anti-effraction du coffret de l'ULS-POE secured

Le contact anti-effraction du coffret de l'ULS-POE secured est branché sur la centrale, qui émet un événement en cas d'ouverture du coffret.

6.2 Couverture des besoins de sécurité

6.2.1 Menaces - biens sensibles

	Déplacements de l'utilisateur / vie privé	**Authentification des utilisateurs**	**Secrets Cryptographiques**	**Configuration**	**Logs**
Menaces	**Biens sensibles**				
Obtention non autorisée de l'accès		X	X	X	
Divulgation des déplacements	X				X
Divulgation des droits d'accès				X	
Modification de la configuration		X		X	

6.2.2 Fonctions de sécurité - menaces

	Menaces			
	Obtention non autorisée de l' accès	**Divulgation des déplacements**	**Divulgation des droits d' accès**	**Modification de la configuration**
Fonctions de sécurité				
Authentification des utilisateurs et badges	X		X	X
Chiffrement des échanges sans fils entre le badge et la centrale	X	X	X	
Communications d'administration sécurisées			X	X
Protection de la configuration			X	X
Protection des logs		X	X	
Anti-arrachement des lecteurs de badges	X	X	X	
Anti-effraction du coffret de l'ULS-POE secured				X
Hypothèses				
Administrateur de confiance	X		X	X
Centrale et dispositif de filtrage IP positionnés dans un environnement sécurisé	X			X
Dispositif de filtrage IP sécurisé				X
Lien sécurisé entre la centrale et le contrôleur de porte	X			
Badges et carte SAM sûrs	X			
Badges personnels	X		X	
Bonne création des badges et clés par l'utilisateur du produit	X			

✦

Omnitech Security
18 avenue Cassiopée – CS 10152
33167 Saint-Médard-en-Jalles – FRANCE
Tél. +33 547 745 190
https://www.omnitech-security.fr

« Ensemble, construisons l'@venir » ®