Environnement de contrôle d'accès SEAL System avec ULS4

Cible de sécurité - CSPN

OMNITECH SECURITY
18 avenue Cassiopée – CS 10152
33167 Saint-Médard-en-Jalles
FRANCE

Tél : +33 547 745 190

http://www.omnitech-security.fr

SAS au capital de 250 000 €
R.C.S. BORDEAUX 482 646 015
APE 7112B

Tableau des versions

Date	Version	Motif	Rédacteur
19/05/2023	0.9	Version initiale	Alexandre BALLET
04/09/2023	1.0	Version modifiée à la suite de la première lecture du CESTI OPPIDA	Pierre BORDES
11/04/2024	1.1	Correction d'une référence documentaire incorrecte. Correction de la Figure 6 (évaluation du lecteur). Actualisation des photos de l'ULS et du MCS.	Pierre BORDES
24/09/2024	1.2	Ajustement des versions des éléments de la ToE	Pierre BORDES
23/07/2025	1.3	Modifications suites aux retours de l'évaluateur	Pierre BORDES
14/10/2025	1.4	Définition des zones publiques, protégées, névralgiques et mise à jour de la Figure 6.	Pierre BORDES
30/04/2026	1.5	L'évaluation a porté sur la révision 40.	Pierre GÉLARD
30/04/2026	1.5-pub	Pour diffusion publique (versions des dépendances masquées).	Pierre GÉLARD

Liste de diffusion

Nom	Prénom	Société	Contact
-	-	ANSSI/CCN	certification.anssi@ssi.gouv.fr
-	-	ANSSI/BQA	Bureau de Qualification de l'ANSSI, qualification@ssi.gouv.fr

Liste de relecture

Nom	Prénom	Société	Rôle
Bordes	Pierre	INVISSYS	Auteur
Grand	Michael	TRUST N GO	Relecteur
Gélard	Pierre	OMNITECH Security	Approbateur

TABLE DES MATIÈRES

TABLE DES FIGURES

TABLE DES TABLEAUX

RÉFÉRENCES DOCUMENTAIRES

Source	Référence	Version	Titre
ANSSI	**[NOTE 7]**	2.0	Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN
ANSSI	**[GUIDE]**	2.0	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection
ANSSI	**[WEB]**	1.1	Recommandations pour la sécurisation des sites web, https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Securite_Web_NoteTech.pdf
NXP	**[MF4SAM3]**	3.1	MIFARE secure access module SAM AV3
OMNITECH SECURITY	**[PREPA]**	1.2	ULS secured – preparation atelier
OMNITECH SECURITY	**[MES]**	1.2	ULS secured – mise en service
OMNITECH SECURITY	**[PME CSPN]**	39.0	Procédures de maintenance et d'exploitation d'une installation CSPN
OMNITECH SECURITY	**[GUIDE EXP]**	39.0	Guide de l'exploitant SEAL
OMNITECH SECURITY	**[CRYPTO]**	1.6	Environnement de contrôle d'accès SEAL System avec ULS4 – Spécifications crypto CSPN

ACRONYMES

AID	Identifiant d'application d'un badge DESFire (Application IDentifier).
Badge	Dans le cadre de ce document, tout support physique hébergeant une puce DESFire.
DESFire	Technologie de badge sans contact, propriété de NXP.
EID	Identifiant de badge encodé dans le badge (Encoded IDentifier). L'unicité au sein de l'installation est garantie par le GAC.
GAC	Gestion des Accès Contrôlés.
MCS	Module de Contrôle SEAL. Désignation commerciale d'un module d'extension composant l'environnement de contrôle d'accès d'Omnitech Security, en charge du raccord des organes de la porte et du lecteur de badge.
RS485	Interface de communication série basée sur une paire torsadée + écran. Permet des échanges point à point ou en bus.
SAM	Carte se présentant physiquement comme une carte SIM et proposant des fonctions de sécurité cryptographiques.
TRNG	Générateur de nombres aléatoires matériel (True Random Number Generator)
UCS	Unité de Contrôle SEAL. Ancien nom du MCS d'Omnitech Security.
UID	Identifiant unique de badge fourni par le fabricant du badge (Unique IDentifier).
ULS	Unité Locale SEAL. Désignation commerciale du module de base constituant l'environnement de contrôle d'accès d'Omnitech Security.
UTL	Unité de Traitement Local. L'ULS4 est une UTL d'Omnitech Security.

1 IDENTIFICATION

1.1 Identification du document

Ce document décrit la cible de sécurité relative à la solution de contrôle d'accès d'Omnitech Security, comprenant les composants suivants :

- le progiciel SEAL System,
- une ou plusieurs ULS4, en charge du traitement local des autorisations d'accès,
- un ou plusieurs modules MCS4 permettant de relier chaque ULS4 aux organes de porte et aux lecteurs de badges,

en vue de l'obtention d'une certification de sécurité de premier niveau des technologies de l'information (CSPN).

1.2 Identification du produit

Éditeur	OMNITECH Security
Site de l'éditeur	https://www.omnitech-security.fr/
Nom commercial du produit	ULS4 et SEAL System
Identification technique	Système de contrôle d'accès composé de : GAC : SEAL System UTL : ULS4 MCS4
Version évaluée	SEAL Exploitation 2025.2 (40) ULS4 – Firmware 2.38 MCS4 – Firmware 2.11
Catégorie de produit	Identification, authentification et contrôle d'accès

2 ARGUMENTAIRE DU PRODUIT

2.1 Description générale du produit

2.1.1 Introduction

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. Le groupe DOM Security a été créé en 1993.

Omnitech Security recouvre 4 métiers :

- Éditeur de solutions logicielles de sûreté

L'Hyperviseur SEAL SYSTEM fonctionne en architecture ouverte et communique avec des solutions de contrôle d'accès, de vidéoprotection, d'alarme intrusion et de détection périmétrique, d'IoT, d'interphonie, de sonorisation, etc....

- Constructeur de matériels de contrôle d'accès

Les produits industriels de la gamme, conçus et fabriqués en France, garantissent des déploiements rapides et économiques. Au sein du groupe DOM Security, la société DOM confère à Omnitech Security une très grande expertise dans le domaine de l'identification par radiofréquence (RFID) et l'identification des personnes. La filiale INVISSYS permet d'élargir ce spectre de compétences avec un savoir-faire dans le domaine de l'électronique, la connectivité et l'IoT.

En mars 2021, l'ANSSI a délivré une certification CSPN à l'ULS3-PoE Secured (1.79) d'Omnitech Security, venant ainsi renforcer la gamme des produits de contrôle d'accès filaires et radios traditionnels. L'ULS4 est la nouvelle génération d'ULS.

- Solution sur mesure

Omnitech Security accompagne ses clients dans la réalisation de leurs projets de sûreté en adaptant les solutions de sûreté aux métiers et besoins précis des utilisateurs.

- Maintenance et support

Le savoir-faire et la réactivité de la société sont reconnus. Omnitech Security dispose d'une plateforme de maintenance et support technique permettant de gérer des contrats H24. Le contrat SEAL Care personnalisé garantit aux clients des taux de disponibilité des installations proches de 100%.

- Centre de formation Omnitech Academy

Le centre de formation Omnitech Academy propose un catalogue de formations certifiantes, en présentiel ou distanciel via une plateforme d'e-learning, couvrant notamment l'exploitation et l'administration de l'Hyperviseur SEAL, l'installation et la mise en service des équipements de sûreté et la maintenance.

2.1.2 État de l'art et innovation

L'ULS4 est la nouvelle génération d'ULS. Elle est conforme à l'état de l'art :

- lecture transparente des badges,
- utilisation d'un SAM (amovible) pour protéger les clés de lecture des badges, propriétés du client,
- autoprotections et sécurisation actualisée de tous les canaux de communication.

L'ULS4 reprend la sécurité moderne de l'ULS-PoE Secured et la modularité de l'ULS3, dont l'installation pouvait tirer parti d'un bus terrain à la topologie libre.

L'ULS4 innove en exploitant un nouveau bus de terrain facilitant la modernisation des câblages existants.

2.1.3 Schéma général d'architecture

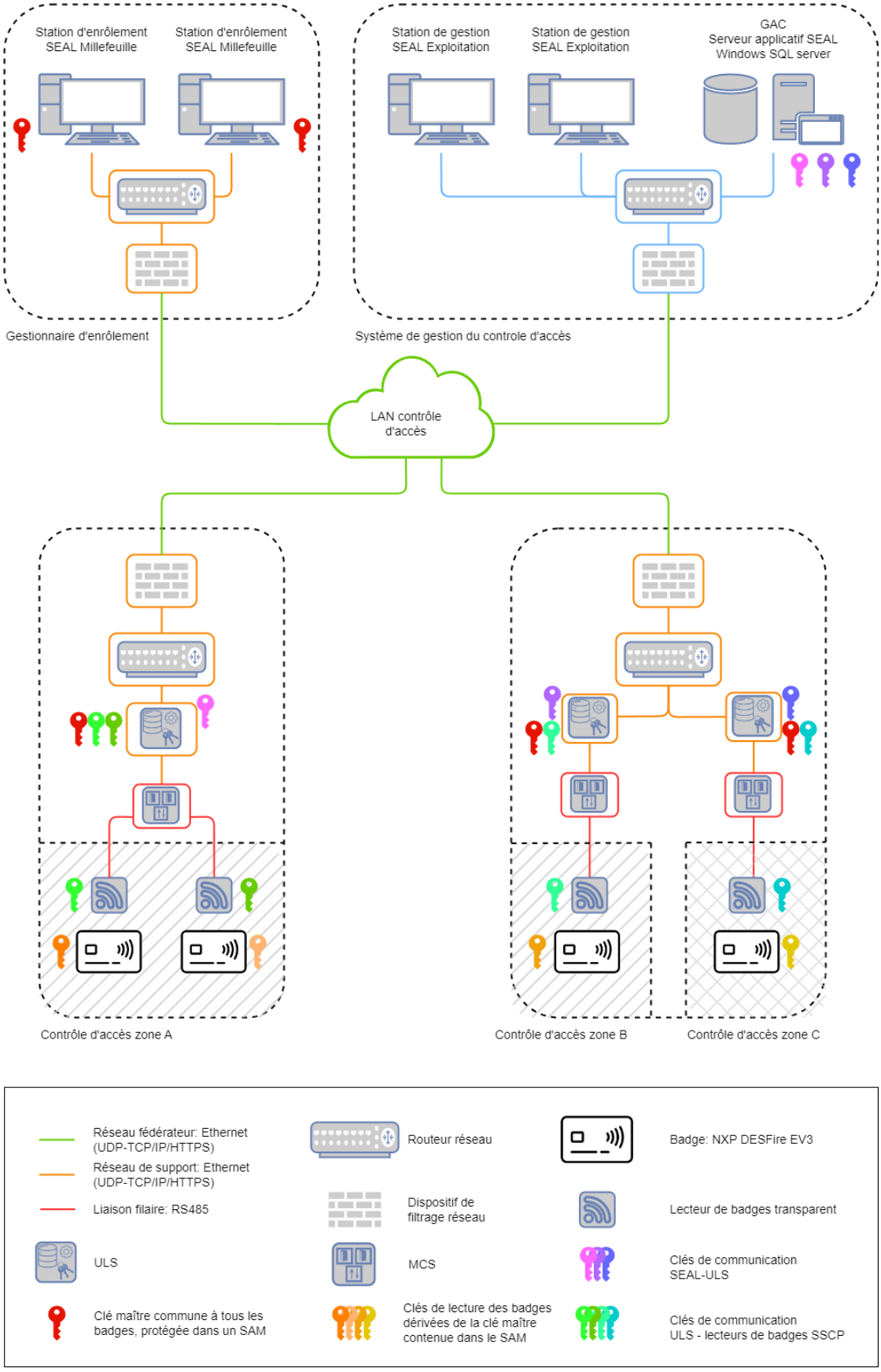

Figure 1 - Schéma général d'architecture

L'architecture générale du système présentée en Figure 1 se compose des éléments suivants :

- Un environnement d'enrôlement des badges (hors TOE)[1]
  - Un ou plusieurs postes, sur lequel est installé SEAL Millefeuille, logiciel d'enrôlement des badges
- Un environnement d'exploitation
  - Le serveur SEAL[2] (GAC)
  - Un ou plusieurs postes pouvant se connecter à SEAL Exploitation[2]
- Un ou plusieurs environnements de contrôle d'accès
  - Une ou plusieurs ULS[2],
  - Un SAM sur chaque ULS (hors TOE)[3],
  - Un ou plusieurs MCS[2]
  - Un ou plusieurs lecteurs de badges SEALDES-4[4],
  - Des badges NXP DESFire EV3 (hors TOE[5]), encodés avec les clés dérivées d'une clé maître connue des SAM, via l'environnement d'enrôlement.

L'ULS utilise le SAM pour calculer les clés dérivées des badges, et stocke de manière sécurisée les clés de communication avec ses lecteurs de badges et avec le serveur.

2.1.4 Descriptif des éléments constituants le système

2.1.4.1 Serveur SEAL

Le serveur applicatif SEAL est développé par Omnitech Security. Il assure l'Hypervision globale de la solution de sûreté. Il présente une interface web accessible depuis toutes les stations raccordées au réseau de sureté.

Le serveur SEAL est un serveur sous environnement Microsoft Windows Server, disposant d'une base de données Microsoft SQL Server, et exploitant le serveur web IIS.

[1] Dans la TOE, on procède à l'enrôlement des badges depuis SEAL Exploitation. Dans cette situation, les badges doivent être pré-encodés par un logiciel au choix, que le client doit doter d'un SAM disposant des mêmes clés que les SAM distribués aux ULS.
[2] Inclus dans la TOE.
[3] Le SAM est fabriqué et distribué par l'utilisateur (voir note 1)
[4] Le lecteur de badges est transparent. Il est néanmoins supervisé par le MCS.
[5] Le badge est pré-encodé par l'utilisateur (voir note 1)

2.1.4.2 ULS4

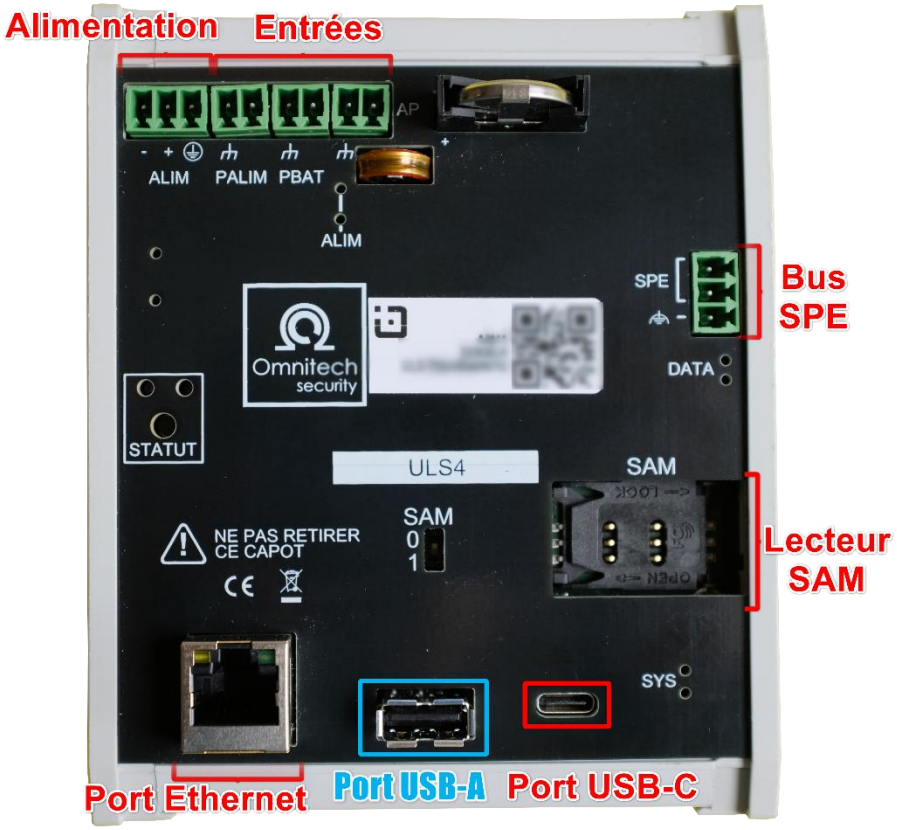

Figure 2 - Schématique de l'ULS4

Les ports utilisés pendant la mise en service sont en rouge.

L'ULS4 est une UTL développée par Omnitech Security, servant à restreindre l'accès à des zones sensibles. Elle assure l'identification et l'authentification des badges présentés aux lecteurs, puis autorise ou non le porteur de badge à franchir le point d'accès. L'ULS4 est reliée à un ou plusieurs modules appelés MCS4, en charge de l'interface physique avec les lecteurs de badges et le déverrouillage des portes. L'ULS4 peut ainsi piloter jusqu'à 32 portes.

L'ULS4 comporte une base de données interne listant les badges autorisés et les périodes d'autorisation. Cette base est alimentée par le serveur SEAL. Des mises à jour du firmware de l'ULS4 et du MCS4 sont publiées régulièrement par Omnitech Security.

L'ULS4 est pré-configurable en usine (par exemple, choix du nombre d'usager entre 100 000 et 500 000).

L'ULS4 sort d'usine avec un certificat d'identification signé par une autorité de confiance Omnitech Security.

2.1.4.3 MCS4

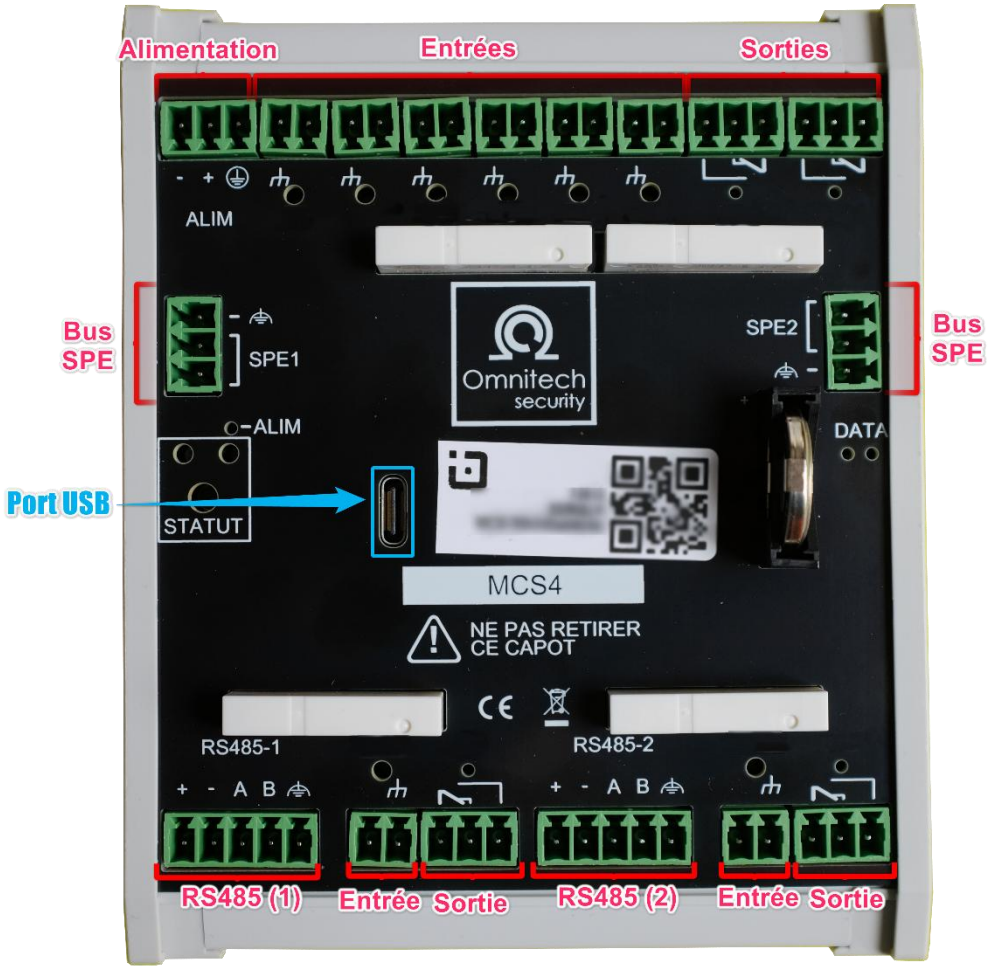

Figure 3 - Schématique du MCS4

Les ports utilisés pendant la mise en service sont en rouge. Les ports désactivés en sortie d'usine sont en bleu.

Le MCS4 est un équipement d'extension à l'ULS4, prévu pour faire office de passerelle entre l'ULS4 et les organes électromécaniques de contrôle d'accès (gâche électrique, pêne motorisé, ventouses… et lecteurs de badges).

Chaque MCS4 peut être connecté à 2 portes et 4 lecteurs (2 lecteurs par porte). Une ULS4 peut être reliée à 16 MCS4 maximum.

Chaque MCS4 dispose également de 8 entrées et 4 sorties, prévues pour déclencher des alarmes au niveau du GAC suivant les contacts configurés (un contact de porte ouverte actif trop longtemps entraîne une alarme, etc.).

2.1.4.4 La carte SAM

Les ULS4 d'Omnitech Security disposent d'un lecteur de carte SAM.

La carte SAM retenue est la NXP MIFARE DESFire AV3. Elle est certifiée EAL6+[6]. Il s'agit d'un circuit pour carte sans contact 100% conforme à la norme ISO/IEC 7816, c'est-à-dire en mesure d'établir un canal de communication chiffré de bout en bout avec un badge DESFire. Le SAM assure

[6] Voir documentation **[MF4SAM3]**

les fonctions de stockage des clés de communication, d'implémentation des algorithmes cryptographiques et des primitives DESFire EV3.

Les mécanismes de sécurité (authentification et chiffrement) reposent sur l'algorithme AES. La carte SAM implémente tous les mécanismes de sécurité de la puce DESFire (Secure Messaging, Proximity Check…) ainsi que des algorithmes RSA et ECC pour la vérification 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 déverrouillée à chaque démarrage.

2.1.4.5 Lecteur de badge SEALDES-4 transparent

Le lecteur de badge SEALDES-4 transparent ne sert que d'intermédiaire entre le badge DESFire et le SAM enfiché sur l'ULS4. Le lecteur est équipé d'une fonction de détection anti-arrachement exploitée par l'ULS4 pour déclencher une alarme.

Les lecteurs de badges communiquent avec le MCS4 par le biais d'un bus RS485 (1 bus pour 2 lecteurs). Les échanges sont sécurisés à l'aide du protocole SSCP v2.

Le lecteur de badge est transparent. Il maintient une communication directe entre la puce sans contact du badge et le SAM, permettant ainsi un chiffrement de bout en bout.

Des IHM visuelles et sonores sont également présentes sur le lecteur. Leur pilotage est réalisé par l'ULS4 de manière sécurisée grâce au protocole SSCP v2.

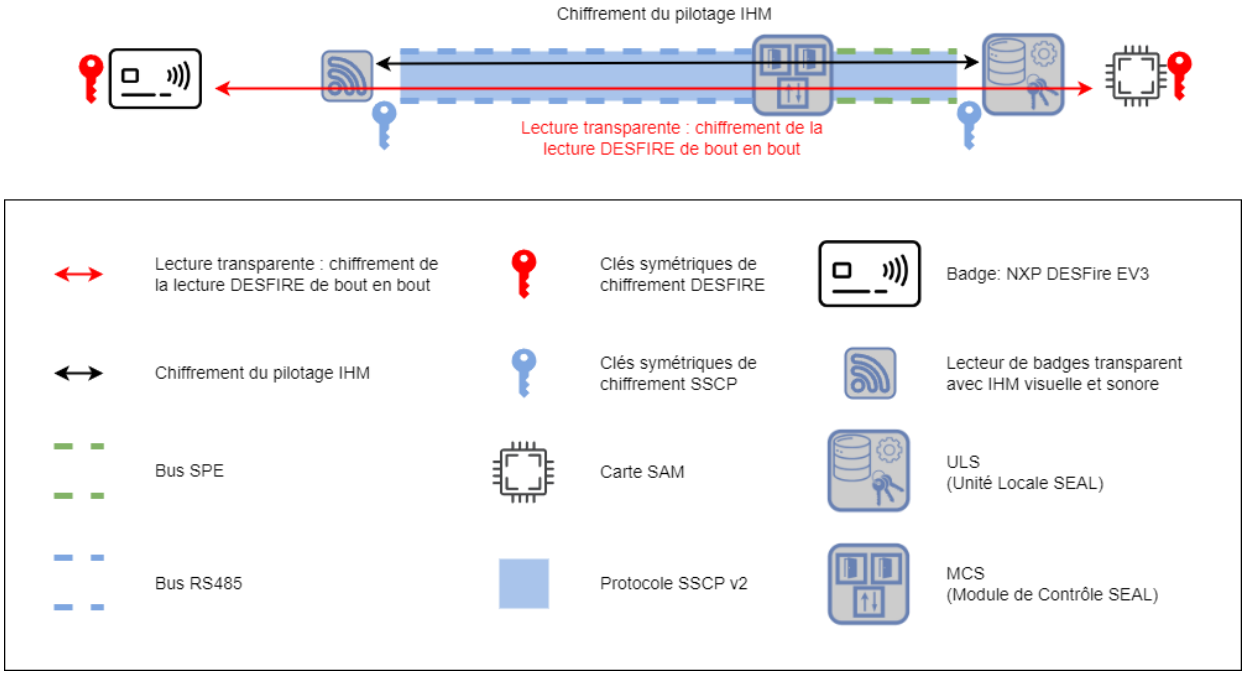

Figure 4 - Schéma de sécurisation de la communication badge/SAM

2.1.4.6 Badge DESFire EV3

Les badges DESFire EV3 utilisés sont fournis par la société NXP et seront encodés avec des clés dérivées d'une clé commune connue des SAM distribués dans les ULS. Une fois encodés, les badges sont enrôlés via SEAL Exploitation. Omnitech Security propose également une solution d'enrôlement avec le logiciel SEAL Millefeuille (hors TOE).

Les badges sont considérés comme de confiance, les puces DESFire EV3[7] étant certifiées Critères Communs EAL5+.

2.2 *Description de l'environnement d'utilisation du produit*

2.2.1 Utilisation usuelle

Les secrets sont générés dans une salle sécurisée, dédiée aux manipulations cryptographiques, coupée de tout réseau extérieur. Les clés de lecture utilisées par les ULS4, ainsi que les clés d'écriture associées nécessaires à la création du badge, sont la propriété du client final. Elles sont distribuées dans des SAM.

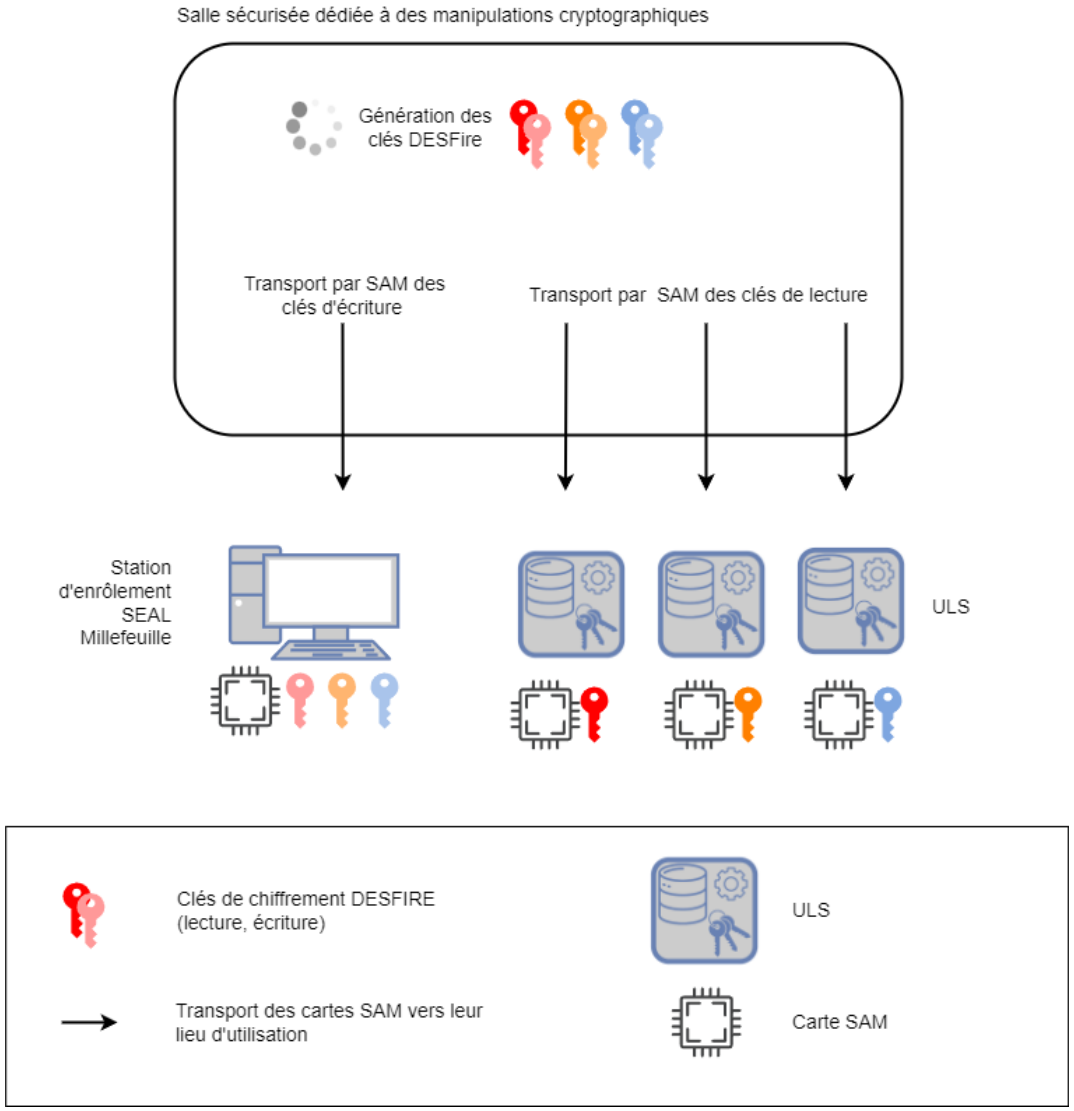

Figure 5 - Schéma de génération et transport des clés DESFire de manière sécurisée jusqu'au lieu d'utilisation

Le client final a la responsabilité de ne diffuser ce jeu de clés que par des moyens sécurisés, et aux seules personnes habilitées. Ainsi, Omnitech Security recommande que la salle sécurisée pour la

[7] https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/mifare-desfire-ev3-high-security-ic-for-contactless-smart-city-services:MF3DHx3

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 sécurisées – par exemple, sur des sites différents – il pourra choisir de cloisonner les sites en utilisant des jeux de clés différenciés. De même, l'application DESFire[8] est une application réservée aux lecteurs de contrôle d'accès, et possède une clé dédiée différente des éventuelles autres applications encodées dans les badges.

Afin de limiter le nombre d'entités ayant accès à la clé maître de lecture, Omnitech Security recommande de limiter la distribution des SAM et de leurs codes de déverrouillage aux seules personnes nominativement identifiées en charge de l'installation ou de la mise à jour du matériel.

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 toute perte doit être signalée ; que lorsqu'un badge perdu est retrouvé, il doit être 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.

En plus du module de contrôle d'accès, SEAL System propose un module vidéo, un module d'intrusion et un module de sonorisation. Dans le cadre de cette cible de sécurité, ces modules sont désactivés.

2.2.2 Description d'une procédure d'accès

Par l'intermédiaire d'un poste de gestion, un exploitant donne une nouvelle autorisation d'accès à un porteur de badge, déjà équipé d'un badge DESFire EV3, pour une porte et une période de validité donnée. Une fois validée, cette autorisation d'accès est journalisée dans le GAC. Le GAC transfère alors la mise à jour des autorisations d'accès à l'ULS4 en charge de la porte. Une fois la synchronisation effectuée, le badge peut être utilisé pour ouvrir la porte.

Le badge DESFire EV3 est présenté par le porteur de badge au lecteur de badge transparent associé à la porte. Le lecteur informe l'ULS4 de la présence d'un badge et l'ULS4 établit la liaison transparente entre le badge DESFire EV3 et le module SAM NXP AV3. Après une étape d'authentification mutuelle, l'ULS4 demande une lecture de l'identifiant du badge présenté (EID).

L'ULS4 peut alors rechercher cet identifiant dans sa base d'accès et procéder à la validation des caractéristiques de l'accès (horaires, période de validité…). Si l'ensemble des vérifications est conforme, l'ULS4 envoie un ordre d'ouverture à l'organe de pilotage de la porte. Un évènement est également sauvegardé quelle que soit l'issue des vérifications afin d'assurer une traçabilité de l'action. Il contient l'ensemble des données relatives à cette tentative d'ouverture. Cet évènement sera ensuite envoyé au GAC de manière asynchrone.

[8] Ces applications, utilisées par le protocole DESFire, correspondent à des zones mémoires d'un badge. Une application représente un usage, ou service, par exemple « contrôle d'accès zone sensible 1 ». Lorsqu'un badge héberge plusieurs applications, on parle de badge multi-service.

3 DESCRIPTION DES DÉPENDANCES

Cette section décrit les dépendances à des matériels et des logiciels du système non fournis avec le produit.

Le client a la responsabilité de fournir un serveur Microsoft fonctionnel avec les caractéristiques suivantes :

- Microsoft Windows Server 2022 (21H2) ou supérieur
- Annuaire Windows
- Service Web Microsoft IIS
- Microsoft SQL Server 2022 ou supérieur

Le client doit également fournir :

- Les cartes SAM destinées aux ULS, et préparées conformément aux spécifications mentionnées dans **[PME CSPN]**
- Les badges pré-encodés pour être lisibles par les ULS équipées des SAM

Bibliothèques tierces sur lesquelles reposent la TOE

Composant	Bibliothèque tierce utilisée
GAC	BCrypt (wincrypt)
ULS	Noyau Linux
ULS	Distribution Yocto
ULS	Mosquitto
ULS	OpenSSL
MCS	Distribution Zephyr
MCS	MbedTLS

4 DESCRIPTION DES UTILISATEURS TYPIQUES

4.1 Administrateurs

Les administrateurs gèrent les comptes d'accès au système via l'annuaire Windows. SEAL est configuré pour consulter cet annuaire afin de déterminer, à partir du groupe d'utilisateurs Windows, le profil utilisateur (Administrateur, Exploitant, Agent Technique).

4.2 Exploitants

Les exploitants créent les cartes d'accès, configurent le système, et modifient les droits d'accès. Ils disposent de comptes d'accès aux postes SEAL Exploitation et SEAL Millefeuille.

4.3 Agents techniques

Les agents techniques sont du personnel qualifié intervenant dans le cadre d'opérations de mise en service et de maintenance du système. Ces agents sont réputés de confiance et disposent de comptes d'accès dédiés aux postes SEAL Exploitation et SEAL Millefeuille. Ils sont en charge de la maintenance des ULS et de la mise en place des cartes SAM dans celles-ci.

4.4 Porteurs de badge

Les porteurs de badge (usagers du système) vont chercher à s'authentifier via leur badge auprès du contrôleur de porte pour déclencher l'ouverture d'une porte.

Les porteurs de badge n'ont pas de compte d'accès à SEAL Exploitation.

5 DESCRIPTION DU PÉRIMÈTRE DE L'ÉVALUATION

L'évaluation est réalisée pour :

- L'ULS4 (UTL) et son MCS4
- Le SEALDES-4 (Lecteur de badges)
- SEAL 2023.2 (GAC)
- Communication entre l'ULS4 et son MCS4
- Communication entre l'ULS4 et les lecteurs de badges SEALDES-4 transparents
- Communication entre le lecteur et le badge
- Communication entre l'ULS4 et SEAL 2023.2
- Communication entre SEAL 2023.2 et les stations de gestion

Tableau 1 - Caractérisation du périmètre d'évaluation

Composant du système		**Inclus dans la cible de l'évaluation** (TOE)	**Non évalué** (environnement de la TOE)	
			Supposé de confiance	Attaquant potentiel
GAC	**Système d'exploitation**		Microsoft Windows Server 2019	
	Applicatifs	SEAL 2025.2 (applicatif web + services Windows)		
	Fonctions cryptographiques		TLS 1.2 (primitives intégrées à Windows)	
	Bases de données et annuaire		Microsoft SQL server 2019	
ULS	**Système d'exploitation**	Linux 5.10.229		
	Applicatifs	Firmware ULS4 v2.38		
	Fonctions cryptographiques	OpenSSL v3.0.x		
	SAM		SAM NXP AV3	
MCS	**Système d'exploitation**	Zephyr 3.7.2		
	Applicatifs	Firmware MCS4 v2.11		
	Fonctions cryptographiques	mbedTLS v3.6.4		
Lecteurs		SEALDES-4		
Badges			NXP DESFire EV3	

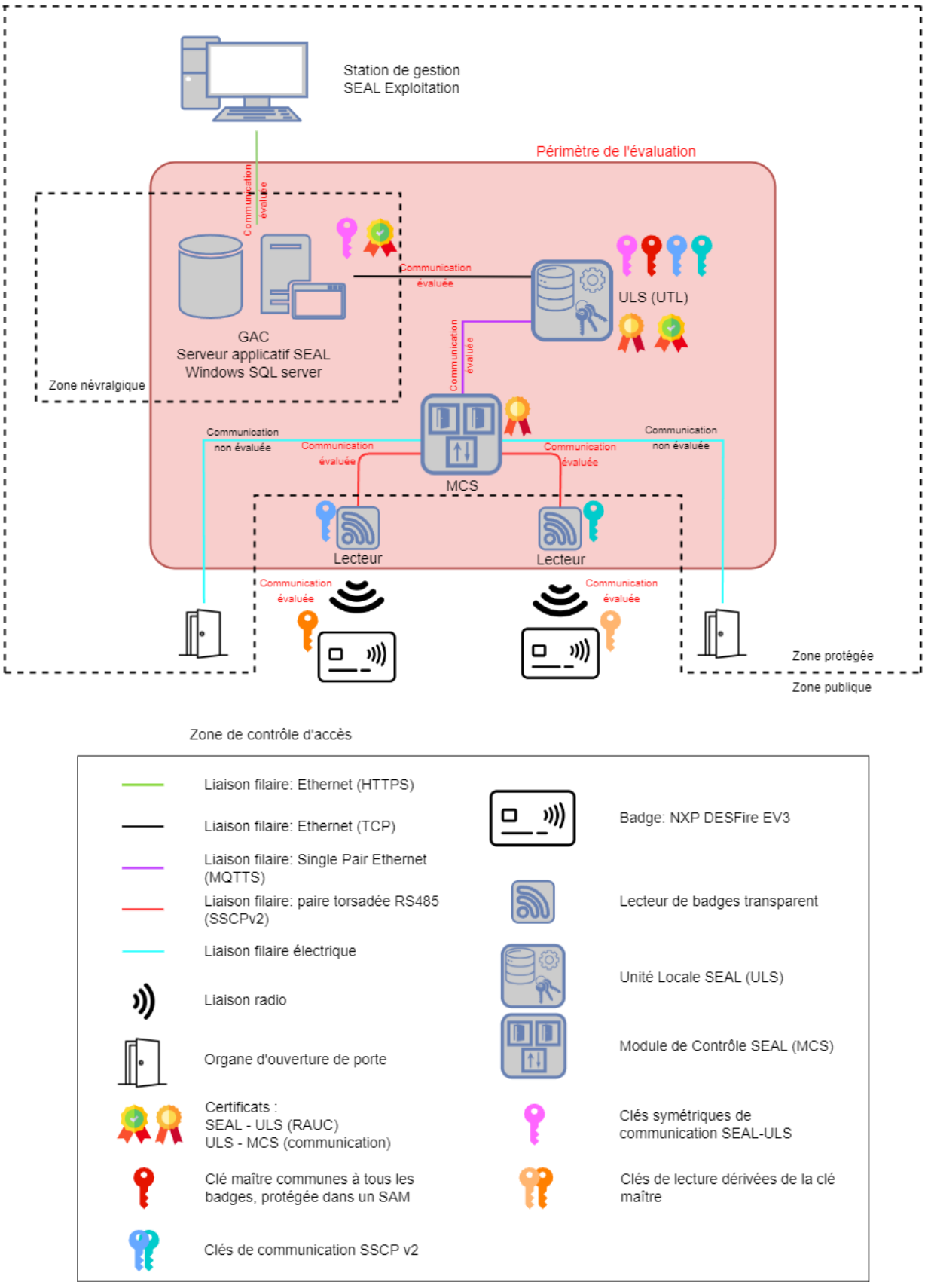

Figure 6 - Schéma d'architecture du périmètre d'évaluation

5.1 Zones d'accès

On distingue 3 types de zones d'accès dans ce document :

- **Zone publique** : zone accessible au public, sans contrôle d'accès.
- **Zone protégée** : zone accessible par contrôle d'accès uniquement pour les porteurs de badges avec une autorisation. Le local technique où se trouvent les coffrets de contrôle d'accès est une zone protégée autorisée uniquement aux techniciens de maintenance et administrateurs de confiance.
- **Zone névralgique** : zone restreinte, supposée sûre, dans laquelle se trouve le serveur de GAC.

5.2 Dispositifs d'accès

L'environnement de l'accès dispose *a minima* des équipements suivants :

- Détecteur d'ouverture (état de la porte)
- Bouton poussoir pour la sortie libre (commande de sortie)
- Mécanisme de verrouillage de l'accès (verrouillé par défaut)
- Lecteur de badge

5.3 Système informatique

Le serveur informatique est installé sous Windows Server 2019, les derniers correctifs de Windows à date du test sont déployés. Le serveur dispose également de SQL Server 2019, avec les derniers correctifs à date déployés. Le logiciel SEAL est installé sur ce serveur.

La station client est installée sous Windows 11, les derniers correctifs à date du test sont déployés. Les tests sont faits à partir d'un navigateur récent et à jour de ses correctifs de sécurité (Chrome, Edge, Firefox).

L'infrastructure réseau cloisonne le réseau de la station de gestion et le réseau de l'ULS. Le GAC sera accessible des deux réseaux. Cf fig. 4.8 de **[GUIDE]**.

5.4 Carte SAM

La carte SAM NXP AV3 de la société NXP contiendra la clé maître nécessaire à la diversification des clés des badges.

5.5 Badges

Un jeu de badges DESFire sera préparé avec les clés de lectures dérivées de la clé maître stockée dans le SAM. Les informations nécessaires à leur lecture seront paramétrées dans la configuration de l'ULS.

6 DESCRIPTION DES HYPOTHÈSES SUR L'ENVIRONNEMENT DU PRODUIT

6.1 Hypothèses sur la configuration de l'environnement

- **H1. Modules externes**

Les modules externes[9] (services, ports) non indispensables au bon fonctionnement du produit sont désactivés.

La liste de ces services et ports est détaillée dans les documents **[PREPA]**, **[MES]** et **[PME CSPN]**.

- **H2. Services d'authentification**

Les serveurs d'authentification hors de la TOE utilisés pour authentifier les utilisateurs sont sains et configurés correctement.

- **H3. Service de base de données**

Le serveur de bases de données SQL Server, situé en-dehors de la TOE, est sain et correctement configuré, conformément aux bonnes pratiques[10].

- **H4. Système d'exploitation du GAC**

Le système d'exploitation Windows, situé en-dehors de la TOE, portant le GAC, est considéré comme sain, sauf en cas de défaillance du GAC.

En particulier, le service Microsoft IIS, considéré comme partie de Windows, situé en-dehors de la TOE, est sain, à jour des correctifs de sécurité, et est correctement configuré.

6.2 Hypothèses sur l'environnement physique du produit

- **H5. Conformité de l'installation physique du système**

Les règles d'installation fournies par Omnitech Security dans le document **[PME CSPN]** ont été respectées lors de l'installation physique du système.

- **H6. Serveur installé dans un environnement sécurisé et contrôlé**

Le serveur SEAL est placé dans la zone névralgique, qui n'est accessible qu'au personnel habilité.

- **H7. Postes d'administration et d'exploitation installés dans des environnements sécurisés et contrôlés**

Les stations d'administration et d'exploitation sont placés dans une zone protégée, qui n'est accessible qu'au personnel habilité.

[9] Un module externe est un élément logiciel apportant de nouvelles fonctionnalités à la TOE mais qui n'est pas indispensable à son fonctionnement.
[10] https://learn.microsoft.com/fr-fr/sql/relational-databases/security/securing-sql-server?view=sql-server-ver16

♦ **H8. ULS et MCS installés dans des environnements sécurisés**

Les ULS sont placées dans des zones physiques sécurisées (local technique avec accès par badge), qui ne sont accessibles qu'aux agents techniques. Elles sont installées conformément aux recommandations d'Omnitech Security décrites dans **[MES]**.

En particulier, elles sont placées dans un coffret avec détection d'ouverture et dédié à cet usage. Les MCS sont placés dans le même coffret, ou dans un coffret similaire à distance de l'ULS, toujours à l'intérieur de la zone sécurisée par le contrôle d'accès (zone protégée). Les liaisons filaires de l'ULS vers les MCS et les lecteurs de badges courent dans des gaines non apparentes à l'intérieur de la zone protégée.

♦ **H9. Lecteurs de badges installés avec câbles traversants**

Le raccordement de la tête de lecture doit être traversant de manière que la détection d'arrachement ne puisse être contournée simplement, les liaisons filaires pénétrant immédiatement en zone protégée.

6.3 Hypothèses sur l'environnement technique du produit

♦ **H10. Badges et cartes 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.

6.4 Hypothèses sur les utilisateurs du produit

♦ **H11. Administrateurs et opérateurs de confiance**

Les administrateurs, les exploitants et les agents techniques sont considérés comme étant de confiance, non hostiles et formés à l'utilisation du produit.

♦ **H12. 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 badges volés ou perdus font l'objet d'une procédure spécifique rendant impossible toute utilisation du badge en question dans un court délai.

♦ **H13. Bonne création des badges, des SAM et des clés par l'utilisateur du produit**

Les badges et les SAM sont fournis par l'utilisateur du produit, qui les a créés et les gère en respectant les recommandations de sécurité du produit utilisé à cette fin. En particulier en ce qui concerne le chiffrement des applications DESFire et la génération de leurs clés.

Remarque : l'hypothèse **H10** concerne le fonctionnement interne des cartes, tandis que l'hypothèse **H13** concerne l'utilisation qui est faite de ces cartes.

♦ **H14. Suivi de la documentation de sécurité**

Les utilisateurs respectent les préconisations provenant de la documentation de sécurité de la TOE (**[PME CSPN]**, et **[GUIDE EXP]**).

- **H15. Consultation des journaux**

Les exploitants consultent régulièrement les journaux locaux et centralisés, générés par la TOE.

7 BIENS SENSIBLES À PROTÉGER

- **B1. Droit d'accès des porteurs de badge**

Les droits d'accès des porteurs de badge sont constitués de l'ensemble des informations permettant de vérifier qu'un porteur possède les autorisations d'accès à une zone. Selon ces droits, l'action de badger peut mener ou non à l'autorisation d'accès à la zone concernée.

La TOE maintient une cohérence de ces droits à l'échelle du système. Ces droits sont protégés en confidentialité et en intégrité.

- **B2. Données d'exploitation des ULS**

Les données d'exploitation sont constituées de l'ensemble des informations utiles au bon fonctionnement du système de contrôle d'accès en phase opérationnelle. Cet ensemble comprend notamment des valeurs instantanées (état actuel de la porte), des données de configuration (mode de fonctionnement de la porte), des commandes (ouverture à distance) …

L'accès à ces données est régi par la politique de droit de la TOE.

Ces données sont protégées en intégrité et en authenticité.

- **B3. Échanges entre les ULS et SEAL**

SEAL pilote les ULS et assure une transmission périodique de la base de données nécessaire au traitement local des demandes d'accès.

Ces flux sont protégés en intégrité, confidentialité et authenticité.

- **B4. Échanges entre les MCS et les ULS**

Les MCS assurent le lien entre leur ULS (UTL), les lecteurs de badges et les organes d'ouverture de portes. Ce sont les états des entrées de MCS qui permettent à l'ULS d'en déduire des informations d'alarmes éventuelles.

Ces flux sont protégés en intégrité, confidentialité et authenticité.

- **B5. Échanges entre le lecteur de badge et l'ULS**

Les ULS assurent la gestion de toutes les demandes d'accès en provenance des têtes de lecture qui lui sont rattachées.

Ces flux sont protégés en intégrité, confidentialité et authenticité.

- **B6.A Mécanisme d'authentification des utilisateurs**

Les agents techniques s'authentifient sur les ULS pour la mise en service ou la maintenance via un compte d'administration local à l'ULS.

Les administrateurs, exploitants et agents techniques s'authentifient sur le site web du GAC via un compte Windows.

Le mécanisme est protégé en intégrité et en authenticité.

- **B6.B Mécanisme d'authentification des usagers**

Les porteurs de badges s'authentifient avec leur badge sur les SAM par l'intermédiaire de l'ULS.

Le mécanisme (le firmware et sa configuration) est protégé en intégrité et en authenticité.

- **B7.A Secrets de connexion des utilisateurs**

Les comptes sur les ULS et les comptes Windows permettant d'accéder à SEAL sont protégés par les systèmes d'exploitation des ULS et du serveur hébergeant SEAL, en intégrité et en confidentialité.

- **B7.B Secrets de connexion des équipements**

Les clés de connexion des ULS avec les MCS, les lecteurs de badges et le serveur SEAL sont protégées en intégrité et en confidentialité.

- **B8. Clés des badges DESFire**

Les clés des badges sont protégées par les SAM, en intégrité et en confidentialité.

- **B9. Politique de gestion des droits**

Chaque utilisateur du GAC possède un des quatre rôles décrits en section 4, assigné par un administrateur du système.

Cette politique est protégée en intégrité.

- **B10. Micrologiciel (*firmware*)**

Afin d'assurer correctement ses fonctions, le micrologiciel (*firmware*) de l'ULS et du MCS doit être intègre et authentique.

- **B11. Fonction de journalisation locale de l'ULS**

L'ULS dispose d'une fonction de journalisation locale qui, une fois configurée, doit rester opérationnelle.

- **B12. Fonction de journalisation centralisée de l'ULS**

L'ULS transmet ses journaux à SEAL. Cette fonction de journalisation centralisée, une fois configurée, doit rester opérationnelle.

- **B13. Journaux d'évènements locaux de l'ULS**

Les journaux des accès aux zones se présentent sous la forme d'évènements stockés dans l'ULS.

Ils sont protégés en intégrité et en authenticité.

- **B14. Journaux d'évènements centralisés de l'ULS**

Les événements sont transmis au serveur SEAL de manière sécurisée.

Ils sont protégés en intégrité, en authenticité.

Le serveur est également capable de détecter une perte d'événement pendant la transmission (par exemple à la suite d'une coupure).

Tableau 2 - Caractéristiques de sécurité des biens sensibles

	Confidentialité	Intégrité	Authenticité	Disponibilité
B1. Droit d'accès des porteurs de badge	X	X		
B2. Données d'exploitation de l'ULS		X	X	
B3. Échanges entre les ULS et SEAL	X	X	X	
B4. Échanges entre le MCS et l'ULS	X	X	X	
B5. Échanges entre le lecteur de badge et l'ULS	X	X	X	
B6.A Mécanisme d'authentification des utilisateurs		X	X	
B6.B Mécanisme d'authentification des usagers		X	X	
B7.A Secrets de connexion des utilisateurs	X	X		
B7.B Secrets de connexion des équipements	X	X		
B8. Clés des badges DESFire	X	X		
B9. Politique de gestion des droits		X		
B10. Micrologiciel (firmware)		X	X	
B11. Fonction de journalisation locale				X
B12. Fonction de journalisation centralisée				X
B13. Journaux d'évènements locaux		X	X	
B14. Journaux d'évènements centralisés		X	X	

8 DESCRIPTION DES MENACES

Ce chapitre détaille les scénarios de menace pouvant entrainer les risques définis par la **[NOTE 07]** :

- **R1**. Entrée non autorisée dans les locaux ;
- **R2**. Dissimulation (non-détection par le système) d'une entrée dans les locaux.

8.1 Agents menaçants

Pour cette évaluation les attaquants suivants sont considérés :

- Attaquant à l'extérieur du bâtiment protégé, c'est-à-dire ayant accès uniquement aux lecteurs transparents et aux badges (zone publique) ;
- Attaquant ayant accès au réseau du centre de gestion des accès contrôlés, sur lequel communiquent le serveur SEAL avec les ULS et avec les stations de gestion SEAL Exploitation ;
- Attaquant ayant accès au réseau terrain, sur lequel communique l'ULS avec les MCS et les lecteurs de badges (réseau dédié SPE entre l'ULS et les MCS et réseau dédié RS485 entre les MCS et les lecteurs de badges).

8.2 Liste des menaces

Les attaques couvertes par une hypothèse d'environnement évidente ne sont pas explicitées, par exemple le vol d'un badge, couvert par l'hypothèse **H12**.

8.2.1 Attaques sur le système Lecteur – MCS – ULS

- **M1. Attaques radio entre le badge et le lecteur**

L'attaquant intercepte les communications entre le lecteur et le badge dans le but de :

- Usurper l'identité ;
- Demander l'ouverture d'un accès/porte ;

- **M2. Vol des clés des badges DESFire**

L'attaquant parvient à accéder aux clé DESFire des badges, lui permettant de lire ou de créer ses propres badges.

- **M3. Modification du comportement du lecteur**

L'attaquant parvient à tromper le porteur de badge en modifiant le comportement des voyants lumineux et du buzzer.

L'attaquant parvient à tromper l'exploitant en simulant des passages de badge, en écoutant et en modifiant les communications entre le badge et l'ULS.

- **M4. Altération des transactions MCS – lecteur**

L'attaquant écoute les transactions dans le but de :

- Copier le badge ;
- Usurper l'identité ;
- Demander l'ouverture d'un accès/porte ;
- Piloter la LED RGB ainsi que le buzzer du lecteur de badge.

♦ **M5. Altération des transactions ULS – MCS**

L'attaquant écoute les transactions dans le but de :

- Demander l'ouverture d'un accès/porte ;
- Piloter la LED RGB ainsi que le buzzer du lecteur de badge ;
- Déclencher des alarmes ;

♦ **M6. Déni de service sur le MCS**

L'attaquant empêche le MCS d'assurer la communication entre l'ULS et le lecteur sans que l'ULS ne s'en aperçoive (c'est-à-dire sans interrompre le signal de vie).

En utilisant des requêtes malformées, l'attaquant cherche à :

- Altérer la configuration du MCS ;
- Piloter la porte sans que l'ULS ne l'ait autorisé ;
- Empêcher le MCS de remonter à l'ULS les informations en provenance de la porte (ouverture autorisée ou non).

♦ **M7. Déni de service sur l'ULS**

L'attaquant empêche l'ULS de remonter ses journaux à SEAL en temps réel sans que SEAL ne s'en aperçoive (c'est-à-dire sans interrompre le signal de vie).

En utilisant des requêtes malformées, l'attaquant cherche à :

- Altérer la configuration de l'ULS ;
- Forcer l'ULS à ouvrir ou non la porte indépendamment du badge présenté ;
- Empêcher l'ULS de tracer les autorisations, les refus d'accès et les alarmes de fonctionnement dans son journal local.

♦ **M8.A Altération de la base de données stockée dans l'ULS**

L'attaquant obtient la liste des porteurs de badge ayant accès aux zones protégées, dans le but de :

- Élargir des périodes d'accès ;
- Modifier/étendre des droits ;
- Réaliser des modifications de droits d'un badge existant afin de lui mettre des autorisations étendues ;
- Transférer les droits d'accès d'une personne sur le badge d'une autre personne ;

♦ **M8.B Altération du journal d'évènements stocké dans l'ULS**

L'attaquant obtient le journal d'évènements locaux de l'ULS et peut l'altérer dans le but de détruire la trace de son entrée dans les zones protégées.

♦ **M9. Corruption du micrologiciel**

L'attaquant parvient à modifier la logique de fonctionnement de l'ULS ou du MCS, par exemple en faveur d'une intrusion non-détectée, ou d'accéder au reste du système.

8.2.2 Attaques sur le système ULS – SEAL – Poste opérateur de gestion

♦ **M10. Altération des transactions SEAL – ULS**

L'attaquant écoute les transactions entre le serveur SEAL et l'ULS dans le but de :

- Rejouer une transaction modifiée pour réaliser des modifications de droits d'un badge existant afin de lui mettre des autorisations étendues ;
- Rejouer une transaction pour modifier la plage horaire ;
- Rejouer une transaction modifiée pour transférer les droits d'accès d'une personne sur le badge d'une autre personne ;
- Créer ou supprimer une trace d'activité dans les journaux centralisés ;
- Rejouer une commande d'ouverture de porte.

♦ **M11. Déni de service sur SEAL (GAC)**

L'attaquant empêche SEAL d'assurer la configuration des droits d'accès et la visualisation des alarmes par les exploitants.

L'attaquant procède en utilisant des requêtes malformées pour chercher à :

- Empêcher l'affichage des alarmes sur le bandeau des alarmes ;
- Empêcher la saisie et le contrôle des droits d'accès accordés aux porteurs de badge.

♦ **M12. Altération des transactions Serveur SEAL – Stations SEAL Exploitation**

L'attaquant écoute les transactions entre le serveur SEAL et les stations SEAL Exploitation dans les mêmes buts que **M10**, mais en agissant au niveau des données du serveur central au lieu d'agir au niveau des données de l'ULS.

♦ **M13. Contournement de l'authentification sur SEAL (GAC)**

L'attaquant parvient à s'authentifier sans avoir les secrets de connexion.

♦ **M14. Contournement de la politique de droits**

L'attaquant parvient à effectuer une élévation de privilège, c'est-à-dire à obtenir des droits qui ne lui sont pas normalement dévolus. L'attaquant peut également tenter d'installer une version quelconque du micrologiciel (firmware) sans en avoir le droit.

♦ **M15. Vol des identifiants d'authentification sur SEAL (GAC)**

L'attaquant récupère le compte de l'exploitant, de l'agent technique ou de l'administrateur, afin d'usurper son rôle.

8.3 Bilan des menaces vis-à-vis des biens sensibles

Tableau 3 - Biens sensibles visés par les menaces

	M1. Attaques radio entre le badge et le lecteur	M2. Vol des clés des badges DESFire	M3. Modification du comportement du lecteur	M4. Altération des transactions MCS – lecteurs	M5. Altération des transaction ULS – MCS	M6. Déni de service sur le MCS	M7. Déni de service sur l' ULS	M8.A Altération de la base de données stockée dans l' ULS	M8.B Altération du journal d' évènements stocké dans l' ULS	M9. Corruption du micrologiciel	M10. Altération des transactions SEAL – ULS	M11. Déni de service sur SEAL (GAC)	M112. Altération des transactions Serveur SEAL – Stations SEAL Exploitation	M13. Contournement de l' authentification sur SEAL	M14. Contournement de la politique de droits	M15. Vol des identifiants d' authentification sur SEAL (GAC)
B1. Droit d'accès des porteurs de badge								X		X	X		X			
B2. Données d'exploitation de l'ULS							X	X		X		X				
B3. Échanges entre les ULS et SEAL							X			X	X	X			X	
B4. Échanges entre les MCS et les ULS					X	X	X			X					X	
B5. Échanges entre le lecteur de badge et l'ULS	X		X	X	X	X	X			X						
B6.A Mécanisme d'authentification des utilisateurs														X	X	X
B6.B Mécanisme d'authentification des usagers	X									X						
B7.A Secrets de connexion des utilisateurs														X	X	X
B7.B Secrets de connexion des équipements			X	X	X					X	X					
B8. Clés des badges DESFire		X														
B9. Politique de gestion des droits										X			X	X	X	X
B10. Micrologiciel (firmware)						X	X			X					X	
B11. Fonction de journalisation locale							X			X						
B12. Fonction de journalisation centralisée										X		X				
B13. Journaux d'évènements locaux									X	X	X					
B14. Journaux d'évènements centralisés													X			

9 DESCRIPTION DES FONCTIONS DE SÉCURITÉ

- **F1. Authentification des badges**

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

- **F2. Lecture transparente entre le badge et la carte SAM**

L'ULS établit un canal sécurisé directement entre le badge et la carte SAM, qui détient les clés de chiffrement et effectue les calculs cryptographiques. Les badges sont encodés avec une clé dérivée.

- **F3. Dispositif anti-relais**

Le mécanisme d'authentification des usagers contrôlé par l'ULS inclus la fonction « proximity check » des badges DESFire EV3, afin de contrôler que le badge est bien à proximité de la tête de lecture.

Au cours de la communication entre un badge et un lecteur, les temps de communication sont mesurés. En fonction de ces mesures, le lecteur peut déterminer s'il s'agit d'un badge présenté au travers d'un relais ou du badge physiquement présenté devant lui.

Un calcul cryptographique détaillé dans le document **[CRYPTO]** est demandé afin de s'assurer d'une communication avec le badge au cours de la mesure.

- **F4. Protection de l'utilisation d'un SAM**

La protection contre le vol d'un SAM est assurée par deux éléments :

1) Au moment du vol du SAM, un évènement est envoyé vers le serveur SEAL afin de signaler le sabotage.
2) Les cartes SAM utilisées dans les ULS sont dotées d'un code de déverrouillage que seule l'ULS connait. Ainsi, un SAM volé ne peut pas être utilisé sans connaître le code de déverrouillage.

- **F5. Dispositif anti-arrachement de la tête de lecture**

La tête de lecture dispose d'un mécanisme de détection d'arrachement grâce à un accéléromètre situé sous le capot du lecteur. L'orientation de référence du lecteur est calculée à sa mise sous tension.

Pour détacher le lecteur du mur, il faut soulever le capot amovible ; l'accéléromètre détecte un changement d'orientation par rapport à une valeur de référence et déclenche un événement sur l'ULS, relayé vers le serveur. Aucune lecture de badge n'est alors possible sur le lecteur (refusé directement par l'ULS tant que l'arrachement est détecté).

- **F6. Communications sécurisées entre l'ULS et la tête de lecture**

L'ULS et la tête de lecture échangent via une communication chiffrée. Ceci assure que seule l'ULS est en mesure de piloter les voyants lumineux ainsi que le buzzer présents sur la tête de lecture.

La tête de lecture et l'ULS s'authentifient mutuellement. Il n'est pas possible de remplacer la tête de lecture appairée par un dispositif malveillant et que celui-ci communique avec l'ULS.

- **F7. Communications sécurisées entre l'ULS et le MCS**

L'ULS et le MCS échangent via une communication chiffrée. Cela permet au MCS de ne pouvoir être utilisé que par un matériel certifié par Omnitech Security.

- **F8. Communications sécurisées entre l'ULS et SEAL**

Les échanges effectués sur le port Ethernet de l'ULS avec le serveur SEAL sont sécurisés (programmation, pilotage et remontée des événements).

- **F9. Dispositif anti-effraction du coffret sécurisé**

Chaque équipement de contrôle d'accès (MCS et ULS) est fourni dans un coffret sécurisé équipé d'un détecteur d'ouverture (contact normalement fermé).

Un évènement est émis vers le serveur SEAL en cas d'ouverture du coffret. Aucune intervention sur l'ULS ou sur le MCS ne peut être effectuée sans que le serveur en soit informé. Le coffret lui-même est en zone protégée, typiquement dans un local technique protégé par contrôle d'accès.

Cette fonction est complétée par une protection contre le sabotage de l'ULS (**F16**) présentée ci-après.

- **F10. Protection de la configuration**

La configuration et la liste des accès autorisés n'est modifiable que par les administrateurs, les exploitants et les agents techniques, en fonction de leurs rôles respectifs.

- **F11. Protection des journaux locaux**

L'accès aux journaux locaux est contrôlé. Seul le firmware de l'ULS peut journaliser les accès par badges. Les entrées journalisées ne sont pas modifiables et sont conservées dans la limite des capacités de l'ULS.

- **F12. Signature du micrologiciel (firmware)**

Le micrologiciel contenu dans les ULS et dans les MCS est signé afin d'assurer son intégrité et son authenticité.

- **F13. Protection des journaux centralisés**

Les journaux locaux sont centralisés par messages authentifiés. Les pertes de messages sont détectées par le système et signalées. Une fois centralisés, les journaux ne sont pas modifiables, sauf par un administrateur de la base de données. Les entrées des journaux sont conservées dans la limite configurée dans SEAL.

- **F14. Communications sécurisées entre SEAL et la station SEAL Exploitation**

SEAL Exploitation utilise l'authentification Windows (intégrée lorsque le navigateur la supporte), sur une liaison https.

L'utilisation des postes SEAL Exploitation est cadrée par des sessions authentifiées et limitées dans le temps. Les jetons de sessions ne peuvent être réutilisés en-dehors de la fenêtre de temps de la session.

- **F15. Politique de droits**

Chaque compte utilisateur et élément du système se voit attribuer des droits restreints, ne lui permettant d'effectuer que les actions requises dans son périmètre de responsabilité. Trois rôles de base sont définis pour les utilisateurs de SEAL : administrateur, exploitant, agent technique.

- **F16. Stockage sécurisé des secrets dans l'ULS et le MCS**

Les secrets de communications des ULS et des MCS sont protégés par des *Secure Element* au sein des deux composants. Les *Secure Element* sont eux-mêmes verrouillés par un code PIN lors de l'appairage entre le SE et le MCU, en usine.

Chaque *Secure Element* est mis en place sous un capot de sécurité. Si ce capot est ouvert, un évènement de sabotage est envoyé vers le serveur et le module sur lequel est placé le *Secure Element* oublie le code PIN, rendant les informations contenues impossibles d'accès.

Deux cas sont possibles dans la fin de vie du produit :

- Le matériel est renvoyé en usine pour être réinitialisé au niveau du *Secure Element* et des données. Le matériel est ensuite détruit.
- Le matériel n'est pas renvoyé en usine mais détruit par le client. Il est demandé au client d'ouvrir le capot du tamper dans cette situation pour permettre la suppression de l'accès au *Secure Element*, permettant de garantir la non-divulgation des données.

Tableau 4 - Couverture des menaces par les fonctions de sécurité

	F1. Authentification des badges	F2. Lecture transparente entre le badge et la carte SAM	F3. Dispositif anti-relais	F4. Protection de l' utilisation d' un SAM	F5. Dispositif anti-arrachement de la tête de lecture	F6. Communications sécurisées entre l' ULS et la tête de lecture	F7. Communications sécurisées entre l' ULS et le MCS	F8. Communications sécurisées entre l' ULS et SEAL	F9. Dispositif anti-effraction du coffret sécurisé	F10. Protection de la configuration	F11. Protection des journaux locaux	F12. Signature du micrologiciel (firmware)	F13. Protection des journaux centralisés	F14. Communications sécurisées entre SEAL et la station	F15. Politique de droits	F16. Stockage sécurisé des secrets dans l' ULS et le MCS	Hypothèses
M1. Attaques radio entre le badge et le lecteur	X	X	X														
M2. Vol des clés des badges DESFire		X		X													
M3. Modification du comportement du lecteur					X	X											9 / 5
M4. Altération des transactions MCS – lecteurs					X	X										X	8 / 9
M5. Altération des transactions ULS – MCS						X	X									X	8 / 9
M6. Déni de service sur le MCS							X										8
M7. Déni de service sur l'ULS							X	X	X	X	X						8
M8.A Altération de la base de données stockée dans l'ULS								X	X	X							8
M8.B Altération du journal d'évènements stocké dans l'ULS								X	X		X						8
M9. Corruption du micrologiciel									X			X					8
M10. Altération des transactions SEAL – ULS								X					X			X	6 / 8
M11. Déni de service sur SEAL (GAC)								X						X			6/7
M12. Altération des transactions Serveur SEAL – Stations SEAL Exploitation														X			6 / 7
M13. Contournement de l'authentification sur SEAL (GAC)														X	X		6 / 7 / 11
M14. Contournement de la politique de droits															X		6 / 7 / 11
M15. Vol des identifiants d'authentification sur SEAL (GAC)														X			6 / 7 / 11

✦

Omnitech Security

18 avenue de Cassiopée – CS 10152

33167 Saint-Médard-en-Jalles – FRANCE

Tél. +33 547 745 190

https://www.omnitech-security.fr

« Ensemble, construisons l'@venir » ®