CIBLE DE SECURITE CSPN

UTL SCAiP PoE avec lecteurs transparents

EVOLUTION DE VERSION

3.7	08/04/2025	A MAIGA L MENARD S.PECOT	Suppression de données sensibles pour diffusion publique Suppression des références vers les spécifications cryptographiques. Suppression des références liés à la mise à jour firmware
3.6	03/04/2025	A.MAIGA	Remplacement des mentions de « système de contrôle d'accès » par « UTL »
3.5	29/03/2024	S.PECOT	Mise à jour des versions
3.4	25/03/2024	L. MENARD S.PECOT	Mise à jour des versions Corrections
3.3	17/10/2023	A HIPEAU A LEGER A MAIGA L MENARD S PECOT F BARRILLIET	Mise à jour document et prise en compte des remarques effectuées par Oppida
3.2	12/10/2021	A MAIGA S PECOT	Ajout d'un filtrage des communication IP Serveur – UTL Corrections clients Correction type de badge DESFire EV3
3.1	12/07/2021	A MAIGA	Modifications et corrections suites aux pré-tests CSPN
3.0	19/03/2021	A MAIGA	Correction et ajout carte option 6 x RS485, prise en compte des nouvelles demandes ANSSI
2.2	04/02/2020	A MAIGA	Modifications à la suite de la réunion ANSSI du 15/01/2020
2.1	13/01/2020	A MAIGA	Réorganisation et mise à jour à la suite de la rédaction des spécifications cryptographiques
2.0	03/09/2019	A MAIGA	Mise à jour suites au travail de Cameon
1.1	22/01/2019	A MAIGA	Mise à jour suites à la réunion avec OPPIDA
1.0	24/09/2018	A MAIGA	Première version
Indice	**Date**	**Personne**	**Nature des modifications**

DOCUMENTS DE REFERENCE

Source	Référence	Version	Liens
ANSSI	ANSSI-CSPNCER/P01/1.1	V1.1	www.ssi.gouv.fr
ANSSI	GUIDES-ANSSI	V1.2	Guide de sécurité des technologies sans-contact pour le contrôle des accès physiques
ANSSI	GUIDES-ANSSI	V2.0	Guide de sécurité des technologies sans-contact pour le contrôle des accès physiques
ANSSI	Référentiels Général de Sécurité	V2.0	RGS_v-2-0
ANSSI	Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN	V1.0	ANSSI-CSPN-NOTE-07 Méthodologie pour évaluation CSPN Contrôle d'accès_v1.0
APSAD	Référentiel	D83	Contrôle d'accès-Documents techniques pour la conception et l'installation

--- Sommaire ---

1 Introduction

1.1 Identification de la cible de sécurité

Ce document constitue la cible de sécurité pour une évaluation CSPN dans la catégorie 6 : Identification, authentification pour le contrôle des accès physiques.

1.2 Identification du produit

- **Nom du produit** : UTL SCAiP (**S**ystème de **C**ontrôle d'**A**ccès **iP)** PoE, commercialisé sous les marques FDI, CASTEL, GOLMAR)
- **Version logicielle UTL** : fV2005
- **Version logicielle Lecteur** : fV2003
- **Composition** :
    - UTL (Contrôle d'accès IP de 6 PORTES)
    - Lecteurs et claviers-lecteurs de la gamme Multi technologie de FDI
    - Serveur terrain iP Manager

- **Constructeur** : FDI MATELEC
    - Site Web : https://www.fdi-access.com/
- **Fabrication** : Site de FDI MATELEC à Cholet, France
- **Utilisation** : contrôle d'accès sécurisés de sites administratifs, industriels et tertiaires

1.3 Références et désignations

Eléments	Désignation	Description
Application métier	iP Manager	
Equipement	FD-125-906	UTL iP POE ANSSI 2-smart RS485 6 PORTES
Equipement	FD-020-924*	Lecteur d'accès RFID P40 ANSSI 2-smart RS485
Equipement	FD-020-925*	Lecteur d'accès RFID P80 ANSSI 2-smart RS485
Equipement	FD-020-926*	Lecteur d'accès RFID PK80 ANSSI avec Clavier digital 2-smart RS485
Badges	DESFire	DES Fast innovative reliable enhanced (NXP)
Hard/Soft	Serveur	Machine host hébergeant des applications et des données
Software	VM	Virtual Machine
Software	AES 128	Advanced Encrypted Standard, clé 128 bits
Software	DH	Diffie Hellmann
Software	ECC	Elliptic Curve Cryptography
Software	TLS	Transport Layer Security
Protocole	2-smart	2-smart : Bus 2 Fils (propriétaire FDI Hardware et Software)
Protocole	RS485	Bus RS485 (propriétaire FDI software)
Hardware	OCo	Ouverture Coffret
Hardware	OCa	Ouverture Capot
Hardware	PHY	PHYceiver Ethernet
Hard/soft	CiP6P	Centrale Contrôle d'accès 6 portes
Hard/soft	UTL	Unité de Traitement Local
Code (donnée)	PIN	Personal Identification Number
Code (donnée)	ID	Identifiant
Système	SI	Système d'Information

Système	GAC	Centre de Gestion des contrôles d'accès
Système	SCAiP	Système de Contrôle d'Accès IP sécurisé
Personne	RSSI	Responsable Sécurité Système d'Information

(*) Les produits (même hardwares et même softwares) étant commercialisés sous différentes marques, les initiales « FD » peuvent être remplacées par « CA » ou « GE ». Le tableau ci-dessous résume les différentes références en fonction des marques de commercialisation.

Marque de Commercialisation	**Références UTL et versions logicielles**	**Références Lecteurs P40 et versions logicielles**	**Références Lecteurs P80 et versions logicielles**	**Référence clavier-lecteur PK80 et versions logicielles**
FDI	FD-125-906, version fV2005	FD-020-924, version FV2003	FD-020-925, version FV2003	FD-020-926, version FV2003
CASTEL	CA-125-906, version fV2005	CA-020-924, version FV2003	CA-020-925, version FV2003	CA-020-926, version FV2003
GOLMAR	GE-125-906, version fV2005	GE-020-924, version FV2003	GE-020-925, version FV2003	GE-020-926, version FV2003

Tableau 1 : Références commerciales des produits de la solution

Dans la suite du document, nous ferons référence aux versions FDI des produits pour faciliter la lecture.

1.4 Configuration d'évaluation du produit

Composant du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
GAC	Système d'exploitation		Linux Ubuntu 22.04	
	Applicatifs		Propriétaire, version logicielle v01.19.00	
	Fonctions cryptographiques		TLS1.3 ; SHA256 ; RSA2048 ; RSA-PSS ;	
	Bases de données et annuaires		MariaDB 10.6.16	
UTL	Système d'exploitation	Free RTOS : 10.5.1 LTS (Long time supported)		
	Applicatifs	Propriétaire version logicielle fV2005		
	Références	XX-125-906 (XX = FD pour FDI CA pour Castel et GE pour Golmar)		
	Fonctions cryptographiques	TLS 1.3 ; SHA 256 ; AES ; ECDSA ; HMAC-SHA256 ; RSA-2048 ; RSA-PSS ; CMAC, HKDF-SHA384		
	SAM	Mifare SAM AV3, MF4SAM3X84, NXP		
Lecteurs simples ou Lecteurs-clavier	Système d'exploitation	Sans OS		
	Applicatifs	Propriétaire version logicielle fV2003		
	Références	XX-020-924/925/926 (XX = FD pour FDI CA pour Castel et GE pour Golmar)		
	Fonctions cryptographiques	CMAC, HKDF-SHA384, AES		
	SAM	aucun		
Badges			Mifare DESFire EV3	

Tableau 2 : Configuration et périmètre d'évaluation du produit

2 Argumentaire du produit

2.1 Description générale du produit

2.1.1 Architecture de la solution d'accès

La solution SCAiP correspond à une solution sécurisée, simple et intégrée pour une gestion centralisée de contrôle d'accès physiques.
Elle est composée :

- D'une partie appelée « Serveur » intégrant les applications, les bases de données et le serveur de terrain,
- D'une partie appelée « Matériel » intégrant les équipements de terrain : UTL, lecteurs, claviers et badges Mifare DESFire.

Le système est architecturé autour des équipements représentés ci-dessous et a pour objectif de filtrer les flux d'individus (usagers) autorisés ou non à pénétrer sur un site, un bâtiment ou des locaux. Pour assurer les contrôles sur les accès, le système d'accès remplit les fonctions suivantes :

- Identification par badge RFID (sans contact) et authentification par code PIN
- Traitements des droits d'accès au niveau de l'UTL
- Automatisme d'accès (déverrouillage, séquencement d'opérations de contrôle de l'ouvrant, état de l'accès physique)

La solution SCAiP peut être implantée dans différents secteurs tels que les administrations, l'industrie et le tertiaire.

2.1.2 Schéma type

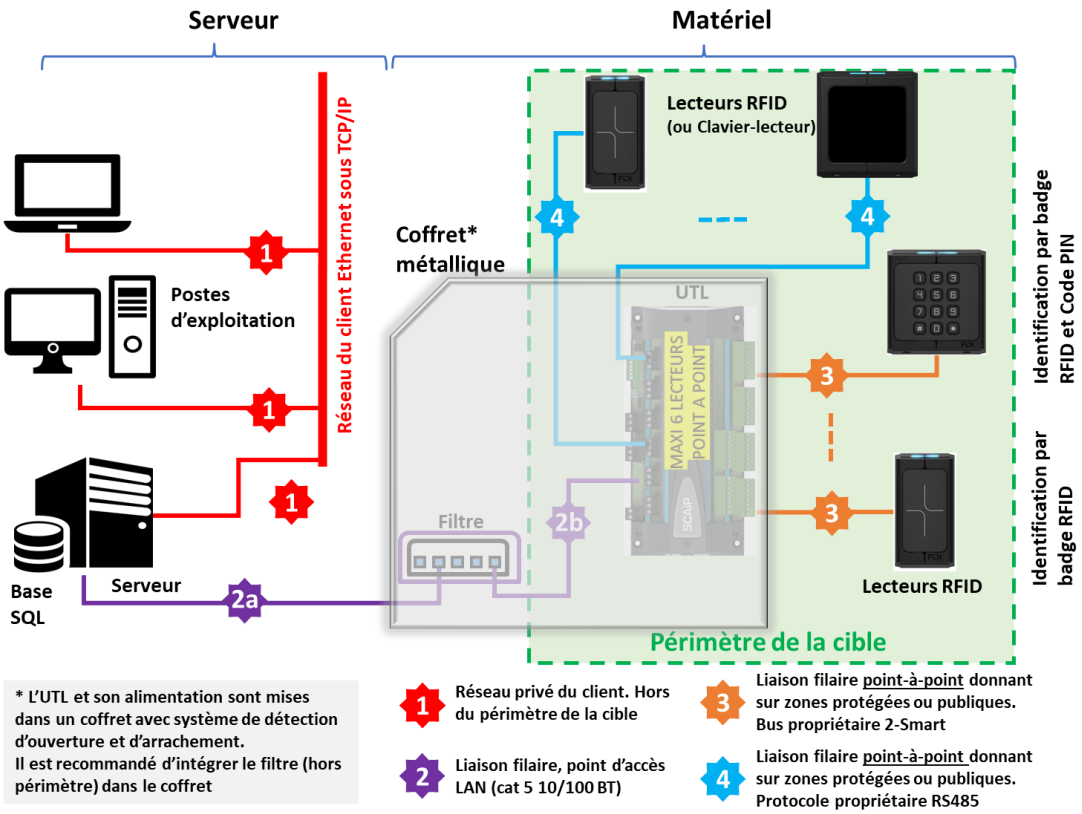

Figure 1 Solution SCAiP

2.1.3 Description fonctionnelle et utilisation

La solution SCAiP de FDI permet une gestion centralisée et en temps réel des accès physiques. Elle permet d'administrer d'une manière intuitive les paramètres des points d'accès d'une entreprise, les droits individuels des salariés suivant les services, et les droits des visiteurs. Les fonctions d'accès sont gérées depuis le serveur « métier » nommé iP Manager et développées par FDI MATELEC.
Ce serveur est utilisé (via l'application Web), chez le client final, par des responsables de sécurité (des administrateurs ou exploitants préalablement formés) qui gèrent toutes les fonctions d'accès à des zones sécurisées ou protégées via des moyens d'identification d'usagers afin de leur attribuer des droits d'accès. Les droits d'accès sont préalablement définis par le client pour la sécurisation des sites.
Cette application, ergonomique et simple d'utilisation, permet une personnalisation des droits et des autorisations d'accès, permet la traçabilité des événements du système afin de réaliser un suivi personnalisé des accès.

Le serveur est entièrement sous le contrôle de responsable(s) de sécurité (client final, RSSI).
Cette application répond aux problématiques classiques du Contrôle d'Accès « QUI, QUAND, OU, QUOI, COMMENT » et permet de :

- Définir tous les types d'accès physiques,
- Référencer de façon unique les usagers dans la base de données du Serveur,
- Donner des droits d'accès aux usagers et aux visiteurs,
- Définir les réflexes (les actions à effectuer par le système en fonction de certains évènements)
- Référencer les éléments de sécurité SI (droits d'administration, droits d'accès au SI, clés de sécurité, …).

Pour répondre à ces besoins, la solution SCAiP repose sur les équipements suivants :

- Un Serveur de terrain avec « application métier » et base de données.
- Des postes d'exploitation
- Des UTL avec leur système d'alimentation en énergie (l'UTL est alimentée en POE par les switchs du client. L'alimentation du switch doit être secourue). Chaque UTL peut gérer jusqu'à 6 portes.
- Des lecteurs (ou clavier-lecteurs) de badges RFID (gamme Multitechno). Ces lecteurs dialoguent en point-à-point avec les UTL de contrôles d'accès via le bus propriétaire 2-smart noté 3 sur la Figure 1 ou via le bus RS485 noté 4.
- Le bus 2-smart (data + alimentation) peut fonctionner jusqu'à une distance de 100 mètres alors que le bus RS485 (data) peut fonctionner jusqu'à une distance de 1000 mètres.
- Une UTL peut gérer au maximum 6 lecteurs, en liaison point à point, suivants les configurations ci-dessous :
  - 6 lecteurs sur le bus 2-smart
  - 6 lecteurs sur le bus RS485
  - 5 lecteurs sur le bus 2-smart et 1 lecteurs sur le bus RS485
  - 4 lecteurs sur le bus 2-smart et 2 lecteurs sur le bus RS485
  - 3 lecteurs sur le bus 2-smart et 3 lecteurs sur le bus RS485
  - 2 lecteurs sur le bus 2-smart et 4 lecteurs sur le bus RS485
  - 1 lecteurs sur le bus 2-smart et 5 lecteurs sur le bus RS485

- Des badges d'accès (basés sur la technologie Mifare® DESFire de NXP en version EV3)

L'accès à une zone protégée ou sécurisée nécessite une identification préalable qui peut être parfois complétée d'une authentification via code PIN (code personnel). Cela nécessite donc d'utiliser un clavier-lecteur RFID.

Note : La notion d'authentification par Code PIN correspond à la fonction d'accès qui consiste à traiter un élément complémentaire (voir ANNEXE 2 : niveau de sûreté IV) à l'identification tel que défini par l'ANSSI.

2.1.4 Raccordements & réseaux

Le serveur et les postes d'exploitation sont raccordés au réseau du client. Ces postes d'exploitation communiquent en https et en WSS (webSocket sécurisé) avec le serveur.
Ce réseau est généralement un réseau Ethernet en IPV4 qui est établi, maintenu et entièrement administré par le client final.
Ce réseau constitue le réseau fédérateur qui assure les interfaces entre les différents équipements comme le serveur de terrain et les postes d'exploitation. Plusieurs postes d'exploitation peuvent être installés sur ce réseau.
Notes :

- Le réseau du client est hors du périmètre de l'évaluation CSPN. Ce réseau est repéré 1 sur la Figure 1.
- Les postes d'exploitation ne dialoguent pas avec l'UTL

Le réseau **LAN du client assure** les échanges entre le Serveur et les UTL. Les données échangées entre le Serveur et l'UTL, via ce réseau sont chiffrées (authentification et chiffrement TLS1.3). Le segment de réseau qui aboutit à l'UTL correspond à une liaison filaire LAN cat 5 en 10/100 BT qui est dédiée par le client au contrôle d'accès.

Le point d'accès réseau, repéré 2b sur la Figure 1, fait partie du périmètre d'évaluation.

L'interface IP de l'UTL est protégée par un dispositif de filtrage (pare-feu, VLAN asymétrique ou autre), n'autorisant que les flux de communications avec le serveur.

2.1.5 Filtre (pare-feu) hors périmètre de la cible

Le dispositif de filtrage installé entre l'UTL et le serveur est un pare-feu qui a été configuré pour ouvrir seulement les ports de connexion utilisés par l'UTL et le serveur et limiter la bande passante. Ce dispositif de filtrage est intégré dans le coffret avec l'UTL mais ne fait pas partie du périmètre d'évaluation. FDI préconise à ses clients l'utilisation d'un firewall pour limiter les surfaces d'attaques sur l'UTL dans le cas d'une cyberattaque.

2.1.6 Réseaux dédiés

Les réseaux dédiés correspondent à des liaisons filaires utilisées exclusivement pour les installations de contrôles d'accès physiques. Ces réseaux dédiés ne sont pas partagés avec d'autres équipements que ceux présentés dans la cible d'évaluation.

La solution SCAiP offre deux possibilités de liaisons des lecteurs ou claviers lecteurs à l'UTL :

- Chaque lecteur (ou clavier-lecteur) RFID peut être directement relié à l'UTL par un bus propriétaire 2-smart et supportant un protocole également propriétaire.
- Chaque lecteur peut également être relié à l'UTL par un bus terrain RS485 (à travers un protocole propriétaire).

Ces bus de terrain correspondent à des liaisons filaires donnant généralement sur des zones publiques. Ce cas n'est pas systématique car ces liaisons peuvent aussi être en zone protégée.

Ces bus assurent des communications sécurisées entre les UTL et les lecteurs (ou claviers-lecteurs) RFID. Sous les commandes de l'UTL (en tant que maitresse de la communication), les échanges sur ces bus se font en temps réel et de manière permanente. Les données circulant sur ce bus sont chiffrées en AES128.

Note : Les bus de terrain 2-smart et RS485 sont respectivement repérés en 3 et 4 sur la Figure 1 et font partie du périmètre d'évaluation.

2.1.7 Partie Serveur hors du périmètre de la cible

2.1.7.1 Serveur d'accès

Rôle : Serveur applicatif pour une gestion centralisée de toutes les fonctions d'accès.
Le serveur peut être constitué d'un poste informatique sous Linux et est doté d'une base de données sous MariaDB. L'installation et la mise à jour des différents composants devra être réalisées par l'administrateur système. Ce serveur peut aussi être hébergé sous forme de VM dans l'infrastructure du client. Dans ce cas, la VM est implantée/hébergée dans un serveur.
Le Serveur dispose de trois fonctionnalités :

- Configuration : Celle-ci permet de définir l'architecture avec les différents équipements déployés sur site(s) (UTL/Lecteurs) au travers d'échanges temps réel et centralisés.
- Exploitation : Celle-ci permet la gestion des accès, des droits des usagers, des alarmes, des événements.
- Supervision : Permet la gestion des alarmes, des événements.

Cette interface permet, sous condition de droits d'administration, de charger, modifier des informations dans la base de données.

2.1.7.2 Postes d'exploitation

Rôle : Station de programmation et d'exploitation. Le logiciel est accessible via un explorateur web (Firefox, Chrome, Edge). Les postes d'exploitation et les certificats, permettant la communication sécurisée entre le serveur et les explorateurs web, devront être fournis par le client, et installés, et maintenus par l'administrateur système.

2.1.8 Partie matérielle dans le périmètre de la cible

2.1.8.1 UTL

Rôle : L'UTL gère jusqu'à 6 lecteurs (ou clavier-lecteurs). Elle est composée d'une carte mère (**Erreur ! Source du renvoi introuvable.** : gestion de 4 lecteurs dans le cadre du bus 2-smart) et d'une carte fille (**Erreur ! Source du renvoi introuvable.** : gestion de 2 lecteurs dans le cadre du bus 2-smart ou 6 lecteurs dans le cadre du RS485). Elle dispose des caractéristiques suivantes :

- Point d'accès LAN pour l'architecture de terrain
- Base locale de 50000 titres d'identification
- Gestion d'évènements et d'alarmes
- Alimentation des lecteurs (ou clavier-lecteurs) par les bus 2-smart

L'UTL embarque un module Mifare SAM AV3 (certifié EAL6+ au niveau hardware pour les attaques physiques) pour le stockage des éléments de sécurité, la génération de clés de chiffrement, la génération d'aléas et aussi pour des calculs cryptographiques. Ce module SAM est également utilisé pour gérer les transactions directement avec les badges MIFARE DESFire. A noter que le module SAM utilisé est sous format SIM, ce qui laisse la possibilité au client de conserver ses clés, par exemple en cas de SAV sur l'UTL.

L'UTL dispose d'une capacité de gestion autonome en cas de rupture de sa connexion LAN avec le serveur.

Cette capacité repose sur la gestion temps réel des usagers, des droits d'accès, des alarmes et de l'historisation des événements.

L'UTL possède une horloge temps réel sauvegardée par pile lithium. Celle-ci permet d'horodater les événements même lorsque l'UTL est déconnectée du réseau.

L'UTL est intégrée dans un boitier contenant un système de capteurs pour détecter l'ouverture, l'arrachement ou l'intrusion. Permettant le cas échéant de générer un évènement.

Caractéristiques techniques de l'UTL :

Composant	Description (exemple référence FDI)
Désignation	UTL SCAIP IPASSAN POE 6 PORTES ANSSI
Référence produit	FD-125-906
Version logicielle	fV2005 (mise à jour sécurisée depuis le serveur)
Emplacement	Zone sécurisée
Microcontrôleur	32 bits, 120 MHz
OS embarqué	OS Free RTOS
Base locale	Base propriétaire
Données	Données névralgiques : Module SAM Données en Flash (binaire)
OCo	Détection d'Ouverture Coffret et d'arrachement

Liaisons & sécurisations :

L'UTL :

- est en lien avec le serveur par le réseau IP (repère 2a)
- est en lien avec les lecteurs (claviers-lecteurs) RFID via les bus 2-smart (repère 3) ou via les bus RS485 (repère 4). L'UTL gère l'alimentation des lecteurs dans le cadre du bus 2-smart.
- Peut gérer jusqu'à 6 lecteurs ou claviers-lecteurs avec un seul lecteur par bus (repère 3 et 4).
- dispose de clés usines et d'un identifiant hard unique (MAC)
- embarque des algorithmes de chiffrement en cryptographie symétrique et asymétrique
- embarque des algorithmes de hachage.
- embarque un module Mifare SAM AV3 pour le stockage d'éléments de sécurité et les calculs cryptographiques symétriques et asymétriques.
- utilise des protocoles d'échange de clés avec le serveur et les lecteurs

2.1.8.2 Lecteur de badges d'accès (format P40)

Rôle : Identification de badges RFID en mode transparent

Caractéristiques techniques du lecteur :

Composant	Description (exemple référence FDI)
Désignation	Lecteur RFID

Référence produit	FD-020-924
Version logicielle	fV2003 (mise à jour sécurisée uniquement par l'UTL)
Emplacement	Zone publique ou zone protégée
Microcontrôleur	32 bits, 64 MHz
OS embarqué	Sans OS
Autre	Détection d'arrachement et d'ouverture.

2.1.8.3 Lecteur de badges d'accès (format P80)

Rôle : Identification de badges RFID en mode transparent

Caractéristiques techniques du lecteur :

Composant	Description (exemple référence FDI)
Désignation	Lecteur RFID
Référence produit	FD-020-925
Version logicielle	FV2003 (mise à jour sécurisée uniquement par l'UTL)
Emplacement	Zone publique ou zone protégée
Microcontrôleur	32 bits, 64 MHz
OS embarqué	Sans OS
Autre	Détection d'arrachement et d'ouverture.

2.1.8.4 Clavier-Lecteur de badges d'accès

Rôle : Identification RFID mode transparent et authentification par Code PIN (double identification).

Caractéristiques techniques du Clavier-lecteur :

Composant	Description (exemple référence FDI)
Désignation	Clavier-Lecteur RFID
Référence produit	FD-020-926
Version logicielle	FV2003(mise à jour sécurisée par l'UTL)
Emplacement	Zone publique ou zone protégée
Microcontrôleur	32 bits, 64 MHz
OS embarqué	Sans OS
Autre	Détection d'arrachement et d'ouverture.

Liaisons & sécurisations :
Le lecteur (ou clavier-lecteur) RFID :

- est en lien avec l'UTL via le bus 2-smart (repère 3) ou le bus RS485 (repère 4).
- négocie la clé d'authentification avec l'UTL à l'installation
- dispose d'une clé usine et d'un identifiant hardware unique
- embarque des algorithmes de chiffrement en cryptographie symétrique (AES) et de hachage.
- utilise un protocole d'échange de clés avec l'UTL

2.2 Descriptions des fonctions d'accès

2.2.1 Identification RFID

Les badges d'accès ont plusieurs origines possibles :

- Fournisseur spécialisé et retenu pour des marchés gouvernementaux (par exemple : un ministère)
- Achat par le client final. Solution badge multi applicatifs
- Fournisseur FDI MATELEC. Dans ce cas, la sécurité du support est assurée par un code de gravure ou un marquage au verso. Ce marquage permet d'assurer la traçabilité des lots de badges livrés au client. Il n'existe aucun lien entre les données internes aux badges et les codes de gravure.

2.2.2 Identification avec confirmation par Code PIN

Cette fonction est paramétrable depuis le serveur et conditionne la fonction de contrôle de l'accès au niveau de l'UTL (Badge + code PIN).

2.2.3 Documents en référence

- Notice IP manager ANSSI
- Notices et guides d'installation des UTL et lecteurs pour SCAiP

2.3 Description du périmètre d'évaluation

La cible de sécurité prévoit l'évaluation de la sécurité des fonctions de contrôle d'accès gérées par les équipements suivants (Figure 2) :

- L'UTL dans son coffret
- Les lecteurs (claviers-lecteurs) RFID

Un serveur est installé mais ne fait pas partie du périmètre d'évaluation.
Le dispositif de filtrage est installé mais ne fait pas partie du périmètre d'évaluation.

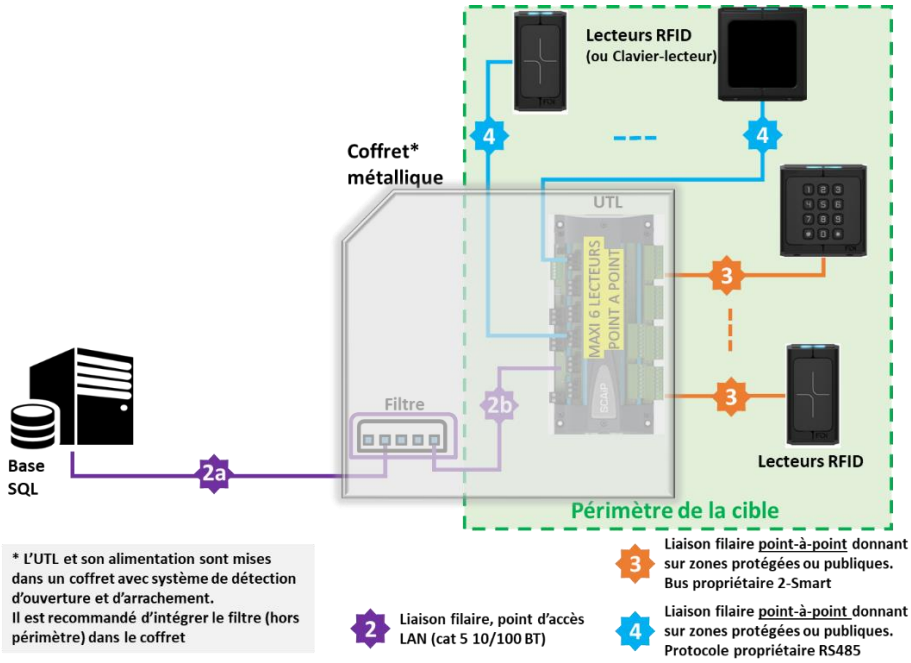

Figure 2 : Périmètre d'évaluation

2.4 Synthèse des différents échanges

- Sur les liaisons 2a et 2b : Sur le réseau Ethernet peut subsister des communications Serveur <–> UTLs. Les communications entre le serveur de terrain et les UTLs sont chiffrées (chiffrement et authentification TLS1.3).

- Sur la liaison 3 : L'UTL connait les ID des lecteurs qui doivent être branchés en point à point.
  - Les communications sur les bus propriétaire 2-smart (hardware et software) entre les lecteurs (ou claviers-lecteurs) et l'UTL sont chiffrées (chiffrement et authentification).
  - Les communications entre le badge et l'UTL s'appuient sur le mode transparent via les communications chiffrées sur le bus.
  - Pour le clavier-lecteur, les codes PIN sont hachés et envoyés à l'UTL sur le bus sécurisé.
- Sur la liaison 4 : L'UTL connait les ID des lecteurs qui doivent être branchés en point à point.
  - Les communications sur le bus RS485 entre les lecteurs (ou claviers-lecteurs) et l'UTL sont chiffrées (chiffrement et authentification).
  - Les communications entre le badge et l'UTL s'appuient sur le mode transparent via les communications chiffrées sur le bus.
  - Pour le clavier-lecteur, les codes PIN sont hachés et envoyés à l'UTL sur le bus sécurisé.

3 Description de l'environnement d'utilisation du produit

3.1 L'environnement d'utilisation du produit

Pour répondre aux besoins actuels du marché de contrôles d'accès physiques et sécurisés par badges RFID basés sur la technologie Mifare® DESFire de NXP avec mécanismes de chiffrements, nous prenons en considération les bases suivantes :

- Chiffrements de l'interface entre le badge d'accès et le lecteur RFID : technologie Mifare DESFire de NXP.
- Mode opératoire du lecteur RFID : Transparent
- Présence de clés de sécurité dans le lecteur RFID : Aucune clé permettant de déchiffrer les badges dans le lecteur. Le lecteur possède 2 clés diversifiées pour sa communication sécurisée avec l'UTL. Ces clés diversifiées sont générées par le module SAM dans l'UTL.
- Traitement des fonctions sécurisées des badges dans l'UTL : toutes les fonctions sécurisées en lectures (*)
- Données névralgiques et clés : Téléchargées dans l'UTL depuis le serveur (après authentification et chiffrement TLS1.3). La procédure de mise en sécurité, nécessitant à certains endroits une intervention manuelle, est décrite dans la notice.

Le mode transparent correspond au schéma de l'architecture hautement recommandée par l'ANSSI (voir Figure 3). Cette architecture regroupe le canal sans fil (Interface RF avec le badge) et la liaison filaire avec l'UTL.

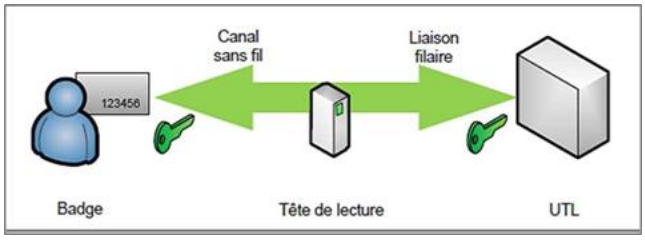

Figure 3 : Architecture hautement recommandée par l'ANSSI : tête de lecture transparente, authentification de bout en bout

(*) Ces fonctions sont celles du Tableau 2 du document ANSSI « Guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques ». Ce tableau est renseigné en ANNEXE 2 de ce document.

Les données névralgiques et les clés sont protégées au niveau de l'UTL dans le module SAM. Le processus d'identification d'un badge DESFire en mode transparent est donnée dans la Figure 4

Lorsqu'un badge DESFire est détecté, à la demande de l'UTL, des commandes sont envoyées au lecteur pour récupérer l'identifiant du badge qui servira de diversifiant pour générer la clé sécrète permettant de lire le contenu du badge.
La liaison entre l'UTL et le badge est sécurisée avec une clé de session mise en place entre les deux équipements. La lecture et le déchiffrement du contenu du badge se fait au travers de dialogues sécurisés entre le module SAM et le badge grâce au protocole Mifare DESFire. Les données d'accès contenues dans le badge et déchiffrées par le module SAM sont transférées à l'UTL qui décide de l'action adéquate à réaliser.

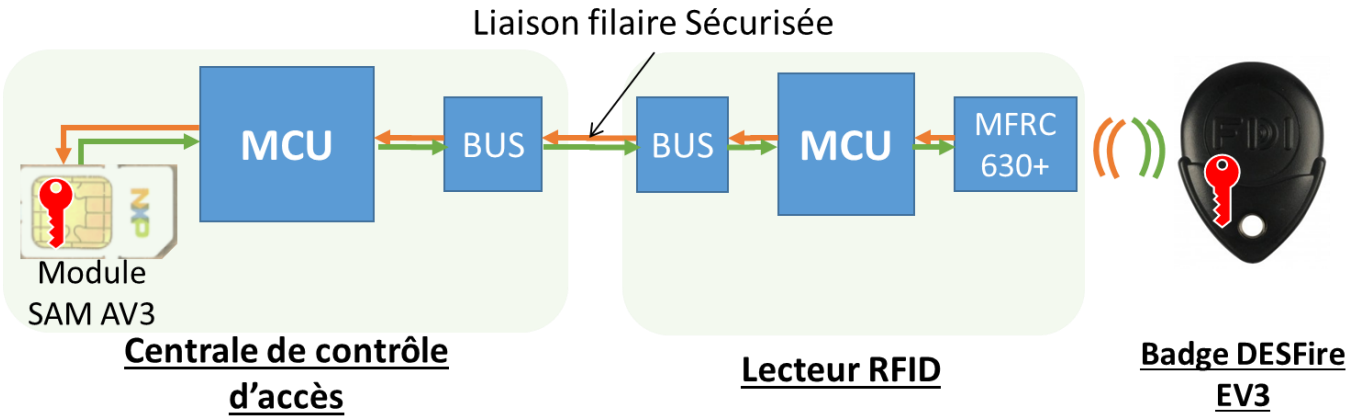

Figure 4 : Lecture d'un badge DESFire en mode transparent

- Le réseau fédérateur est le réseau LAN du client. Ce réseau est sous contrôle d'un DSI (plan d'adressage, configuration des switches et des routeurs).
- L'UTL a la charge d'effectuer les lectures sécurisées des badges d'accès et l'acquisition des codes PIN en cas de double identification.
- L'UTL récupère les clés d'accès mère par téléchargement depuis le serveur, après authentification et chiffrement TLS1.3.

3.2 Hypothèses sur l'environnement du produit

Le système de contrôle d'accès est un système d'informations (SI) à part entière. Il doit donc être sécurisé comme tout SI et ce, d'autant plus qu'il traite des informations personnelles sensibles (Source ANSSI pour le contrôle des accès physiques).
La solution SCAiP fait partie du SI du client final. Dans ce sens, elle hérite des protections mises en place. Dans certains cas, un audit préalable de sûreté est conduit par des autorités compétentes et ce, avant la mise en service d'une solution d'accès sécurisée. Cet audit porte sur la sécurisation des locaux et sur la sécurisation du SI (voir le document D83 de l'APSAD).

La phase d'initialisation du système, permettant la mise en service de l'ensemble des équipements, doit être réalisée par une personne de confiance dans un environnement de confiance après s'être au préalable assuré qu'aucune personne ni matériel n'est en écoute sur les différentes liaisons filaires (Ethernet, 2-smart, RS485).
Lors d'une phase de remplacement de matériels, les mêmes précautions doivent être appliquées.

3.2.1 Hypothèses sur le centre de gestion des accès contrôlés (GAC)

Le GAC est installé dans un local hautement sécurisé. Les utilisateurs du logiciel sont considérés de confiance et les administrateurs du serveur sont considérés de confiance.

3.2.1.1 Hypothèses sur le système d'exploitation

- Les mises à jour de sécurités doivent être installées sur le système d'exploitation ainsi que les différents composants (apache, java)

- Le réseau de centrale et le réseau pour les postes internet doivent être séparés
- Un firewall doit être installé et configuré pour autoriser seulement les postes et les centrales sur les ports concernés
- La prise de poste se fait via une session Windows/Linux avec politique des mots de passe/certificat (mots de passe sécurisés, changements périodiques des mots de passe, …).
- Les navigateurs internet sont installés avec les dernières mises à jour.
- Pour le serveur web, afin de répondre à l'url souhaitée, un certificat valide doit être fourni par le client afin d'assurer la connexion https entre les postes et le serveur. Le certificat sera installé sur le serveur par une personne de confiance. Ce certificat devra être conforme aux recommandations de l'ANSSI (date de validités, conforme à la norme X.509, utilisation de CRL ou OCSP).

3.2.1.2 Hypothèses sur les applicatifs

- L'applicatif doit être mise à jour avec les dernières évolutions de sécurité.

3.2.1.3 Hypothèses sur les fonctions cryptographiques

- Les librairies utilisées pour les fonctions cryptographiques doivent être mises à jour (à travers les dernières évolutions de l'applicatif et les mises à jour java)

3.2.1.4 Hypothèses sur les bases de données et annuaires

- Le moteur de bases de données doit être à jour avec les derniers correctifs.
- La base de données doit être accessible que par l'applicatif par identifiant et mot de passe sécurisé (sécurisation du port via moteur de base de données et firewall)

3.2.2 Hypothèses sur l'environnement physique du produit

3.2.2.1 Installation du serveur

Il est supposé que le serveur soit installé dans un local informatique sécurisé dont l'accès est strictement limité aux personnels habilités.

3.2.2.2 Installation des postes d'exploitation

Les équipements d'administration, ainsi que tous supports contenant des données sensibles (papier, disquettes ou clés USB, sauvegardes, ...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

3.2.2.3 Installation de l'UTL

L'UTL ainsi que le système d'alimentation secourue sont installés dans un local technique sécurisé dont l'accès est limité. Le système d'alimentation secourue est géré par le client.

3.2.2.4 Installation des lecteurs (claviers-lecteurs)

Les lecteurs (et claviers-lecteurs) RFID sont installés pour les usagers de façon bien visible.
Pour un accès à partir d'une zone publique, les lecteurs assurent une protection anti-vandale d'au moins IK08 suivant le modèle.
Aucun câble, ni aucun équipement ne sont posés/installés en zone non protégée, à l'exception du lecteur de badge ou clavier-lecteur.
Le câble de raccordement des lecteurs de badge doit être traversant (le câble sort directement de la zone protégée sur le lecteur). Il ne doit pas courir le long de la porte en zone non protégée, même au travers d'une goulotte ou d'un tube de protection.
Le câblage de l'ensemble des équipements constituant les environnements de porte est direct, point à point.
La prise en compte du lecteur par l'UTL nécessite une opération au niveau du serveur.

3.2.3 Hypothèses sur l'environnement technique du produit

Le serveur intègre différentes fonctionnalités.

- Il fonctionne dans un environnement Linux qui est protégé des virus et ne permet pas l'exécution de code malveillant.
- Les mises à jour de sécurité et les outils Linux sont installés.
- Le niveau de protection du canal d'échange entre le Serveur et l'UTL est décrit dans les spécifications cryptographiques.
- Il existe un compte administrateur, doté de tous les privilèges de configuration et d'exploitation.
- Il existe un compte exploitant, doté de privilèges restreints, et réservé à l'utilisation courante du système.

3.2.3.1 Les réseaux

Le réseau du client et les réseaux dédiés (bus 2-smart et/ou RS485) sont physiquement et logiquement séparés.
Aucune passerelle, informatique ou de transmission de données, ne peut être mise en œuvre entre ces deux réseaux.
Les échanges de données entre les deux réseaux passent systématiquement par l'UTL. Dans le cas de téléchargements depuis le serveur vers les périphériques lecteurs ou claviers-lecteurs, les données sont routées via le bus 2-smart ou RS485 via un protocole d'échanges propriétaire de FDI MATELEC.

3.2.3.2 Protection en transmission de l'identifiant d'accès (ID)

L'ID (identifiant personnel) d'un usager est encodé dans un fichier d'une application de son badge d'accès (application d'accès dans un badge DESFire EV3).
Cet ID est protégé en lecture par un chiffrement en AES 128 bits avec clé AES 128 bits diversifiée (niveau III).
La confidentialité, lors de la transmission dans l'interface air (badge/lecteur) et jusqu'à l'UTL, est assurée par les mécanismes d'échanges Mifare® DESFire.

3.2.3.3 Sécurisation du réseau LAN

Le réseau LAN du client est placé en zone protégée et technique.
L'interface IP de l'UTL est protégée par un dispositif de filtrage considéré comme sûr et fonctionnel, n'autorisant que les flux de communication entre le serveur et l'UTL.

3.2.3.4 Sécurisation des postes

Les postes d'exploitation sont placés en zone sécurisée.
La prise de poste se fait via une session Windows/Linux avec politique des mots de passe (mots de passe sécurisés, changements périodiques des mots de passe, …).
Les mises à jour de sécurité et les outils Windows/Linux sont installés. Les navigateurs internet sont installés avec les dernières mises à jour.

3.3 Hypothèses sur les acteurs du produit

Un ou plusieurs exploitants peuvent agir sur le serveur IP Manager, avec des niveaux de droit différents.
Dans tous les cas, l'exploitant reçoit une formation sur le système. D'autre part, le ou les exploitant(s) dispose(nt) des prérogatives déterminées par le responsable sûreté qui limite les droits d'accès au système. La Figure 5 donne une vue d'ensemble des principaux acteurs du système. Un acteur peut avoir plusieurs rôles.

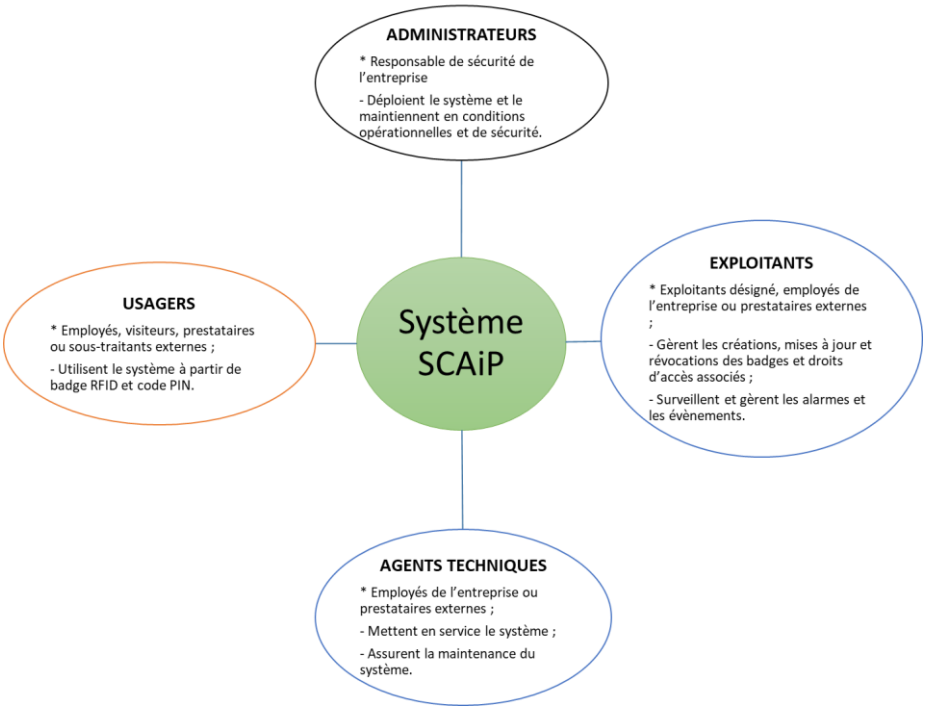

Figure 5 : Les acteurs du système SCAiP

3.3.1 Les administrateurs

Le système SCAiP est entièrement sous le contrôle de responsable(s) de sécurité (client final, RSSI).
L'administrateur, **présumé de confiance**, dispose des moyens de contrôler la configuration matérielle et logicielle de l'ensemble du dispositif. Il a la charge de déployer le système et de le maintenir en conditions opérationnelles et de sécurité.
Des sauvegardes régulières des configurations et de la base de données sont vivement recommandées.

Il doit également veiller à maintenir le système d'exploitation à jour et configurer dans ses différentes versions (exemple : Ubuntu 22.04, Windows 11).
Il doit s'assurer que les accès aux différents composants tels que la base de données, les drivers, les paramétrages des connexions, ne sont accessibles qu'aux seuls utilisateurs autorisés.

3.3.2 Les exploitants

La solution d'accès SCAiP nécessite une exploitation permettant entre autres la gestion des postes de surveillance, les gestions des alarmes en temps réel ; l'ajout et la suppression d'usagers ; la gestion des exceptions ; etc.
Un exploitant est, soit un employé du client, soit un employé d'une société de service en contrat avec le client. Il est également **présumé de confiance**.
L'exploitant a pour fonction de configurer et d'adapter au quotidien les différentes fonctions du système qui concourent à attribuer des autorisations d'accès sur l'ensemble des portes et obstacles physiques contrôlés.
Toute connexion des exploitants au système de gestion est tracée dans l'historique des événements.

3.3.3 Les agents techniques

Les agents techniques, **sans présomption de confiance**, sont des personnes intervenant dans le cadre des opérations de mise en service (déploiements) et de maintenance (techniciens).
Ils ne possèdent aucune prérogative de gestion des droits d'accès.

Toute connexion à l'UTL est tracée dans l'historique des événements. Cette connexion se fait obligatoirement par le biais du serveur.

3.3.4 Les usagers

Les usagers, **sans présomption de confiance**, sont les utilisateurs finaux de la solution SCAiP. Pour accéder aux zones protégées ou aux zones sécurisées, ils disposent de badges sans contact (RFID) DESFire et éventuellement de code PIN personnel supplémentaire. Le code PIN seul ne suffit pas comme moyen d'accès.

Trois populations d'usagers sont concernées par les accès avec badges RFID :

- Employés ou résidents,
- Visiteurs,
- Prestataires, intervenants ou stagiaires.

Le système de contrôle d'accès mis en place doit permettre à chacun de ces intervenants de remplir la tâche qui lui incombe, simplement, d'une manière sécurisée, et sans le pénaliser dans l'exécution normale de sa mission.

Pour les accès véhicule, un seul cas est à considérer :

- Gestion de badges de proximité et sécurisés, niveaux II et III du tableau 2 en ANNEXE 2.

Notes :

La solution SCAiP permet au responsable de la sécurité d'affecter à ces différents types d'usagers des badges sans contact avec le même niveau de sécurité. Ces niveaux correspondent aux Niveaux II ou III du Tableau 4 en Annexe 2 : Tableau 2 ANSSI - Niveaux de sûreté et niveaux de résistance aux attaques.

Pour les sites sécurisés, la technologie Mifare® DESFire (EV3) est vivement recommandée.

Le code PIN personnel est attribué par le responsable de la sécurité et selon une logique de référencement des usagers. Le serveur permet de renouveler les codes PIN tous les 60 jours par défaut. Cette valeur est paramétrable dans l'application.

Les règles de sécurité sont censées être appliquées (bonnes pratiques) :

- Pas de prêt d'un badge.
- Ouverture de porte pour passage uniquement.
- Ces porteurs sont supposés ne réaliser de demande d'accès que pour leur usage personnel et ne pas permettre l'accès à tout autre personne (tiers et collègues inclus).
- Ils sont supposés ne pas confier leur badge, ni communiquer leur code PIN personnel.

4 Description de l'environnement technique de fonctionnement

4.1 Dispositif d'accès

La gestion de l'environnement d'accès nécessite la disposition des équipements minimums suivants :

- Détecteur d'ouverture de porte (état de la porte) / contact de verrouillage.
- Contact sec de confirmation de passage pour les obstacles physiques
- Sortie libre par bouton poussoir (commande de sortie)
- Sortie par lecture de badge (lecteur en sortie)
- Organe de serrurerie condamnant l'accès (commande par contact sec et alimentation secourue)

4.2 Dispositifs de raccordements et alimentations

Les raccordements des équipements entre eux sont donnés et numérotés dans le schéma de la cible de sécurité (voir Figure 2).
S'y ajoutent :

- Les raccordements des équipements mentionnés au paragraphe 4.1 ci-dessus.
- Les alimentations (secourues par les équipements du client).

4.3 Postes informatiques

- Serveur iP Manager (Configuration & Exploitation) :
  - Unix/Linux
    - Linux Ubuntu
  - Base de données MariaDB
  - Java Runtime Environnement
  - Apache/PHP
- Postes d'exploitation :
  - Système d'exploitation avec navigateur à jour.

4.4 Badges

Les badges d'accès sécurisés sont basés sur la technologie NXP Mifare® DESFire (EV3) :

- Badges livrés pré-encodés selon les différents niveaux de sécurité
- Badges encodés à partir de l'application Web iP Manager

Dans tous les cas, les badges correspondront aux niveaux II et III du tableau des niveaux de sûreté présenté en Annexe 2 : Tableau 2 ANSSI - Niveaux de sûreté et niveaux de résistance aux attaques.

Note : Les fonctions de lectures, sécurisées avec clés diversifiées, font appel à différents algorithmes de calculs de clés. Pour répondre aux différents besoins liés aux calculs des clés, ces fonctions sont traitées au niveau de l'UTL à l'aide d'un module SAM AV3.

4.5 Le module SAM

Le module SAM (en format carte micro SIM) est livré préprogrammées avec les clés de communications des lecteurs et de déchiffrement du firmware.

5 Mesures de l'environnement

La solution SCAiP s'intègre dans l'environnement du client final. En tant que solution d'accès, elle s'intègre ou est couplée au SI du client.

- Pour répondre aux exigences de sécurité, les équipements doivent être installés en respectant les emplacements donnés dans la Figure 6. A noter que les équipements d'accès (lecteurs et clavier-lecteurs) peuvent être installés en zones vertes ou oranges ou rouge dans le cas de lecteur de sortie de ladite zone.
- Dans certains cas, un audit de sécurité est établi afin de vérifier les zones et la sécurisation du SI (voir le document D83 de l'APSAD).

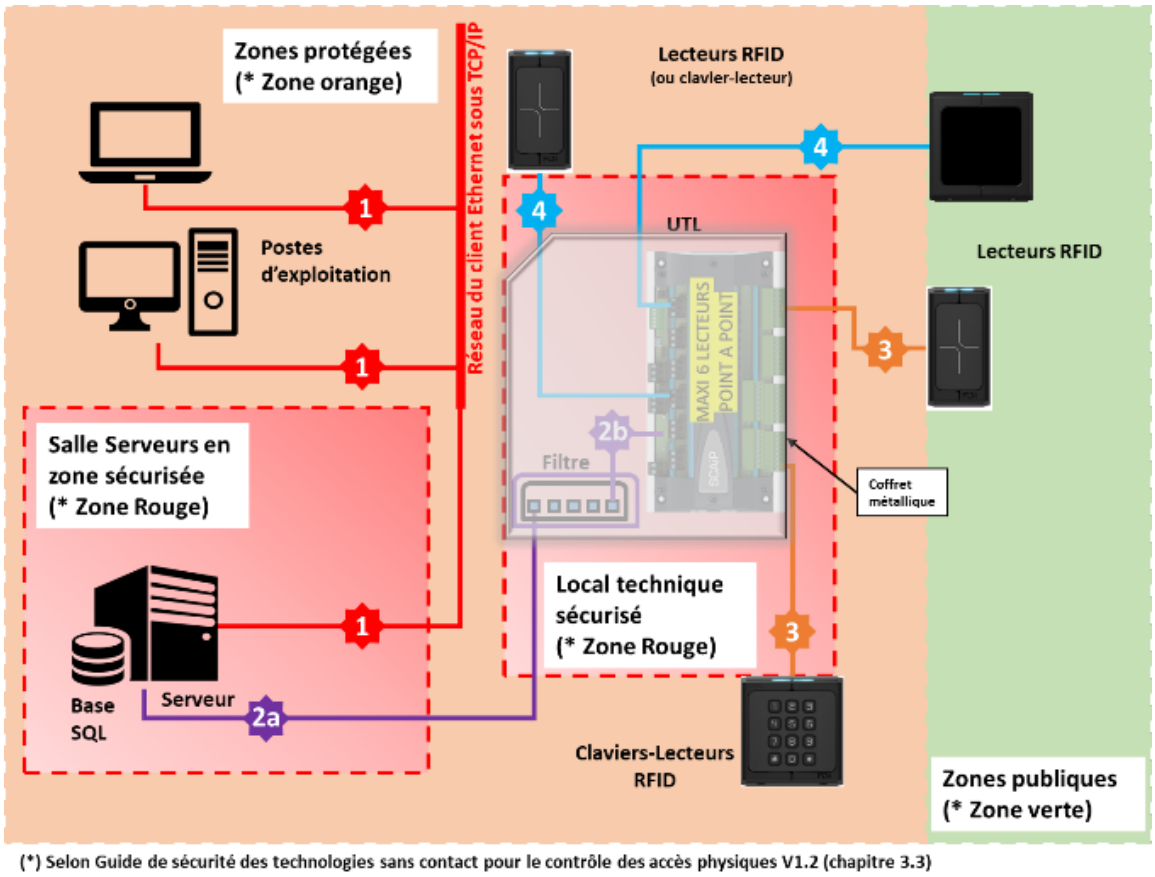

Figure 6 : Example de zones à respecter pour l'installation des équipements de la solution SCAiP

5.1 Organisations

La solution SCAiP est une solution centralisée qui nécessite un minimum d'organisation :

- Responsable sûreté avec des droits d'administration
- RSSI (topologie du réseau, plan d'adressage, mises à jour des logiciels, gestion des mots de passe)
- Opérateur(s) (surveillance des écrans sur les postes, prise en compte des alarmes, gestion/signalement des incidents)

5.2 Mesures de sécurité

Sur un plan organisationnel, les mesures de sécurité font partie des « bonnes pratiques ». Elles doivent être portées à la connaissance des personnes en charge de la sécurité des sites.
Selon l'organisation du client, ces mesures sont diffusées via intranet ou sous forme papier (circulaire, notes, documents confidentiels).

- La remise des clés ou « cérémonie des clés » fait partie des mesures sécuritaires :

- Elle consiste à insérer les différentes clés dans le système.

- Les consignes font partie des mesures sécuritaires :
  - Cas de perte ou de vol d'un badge
  - Cas d'un oubli d'un badge ou d'un code PIN
  - Cas des interventions sur les équipements de la cible de sécurité
  - Cas des alarmes techniques (coupure d'alimentation, autoprotections, défaut de communications).
- Les mises à jour régulières font partie des mesures sécuritaires :
  - Suppression d'un usager et de ses droits
  - Suppression d'un badge
  - Ajout d'un usager avec son badge
  - Vérifications régulières de l'unicité des couples (ID, PIN)

6 Biens sensibles

6.1 Identification des biens sensibles

Les données sensibles qui sont protégées par la solution SCAiP regroupent plusieurs types d'informations

6.1.1 Les clés secrètes utilisées par le système

L'intégrité et la confidentialité des clés utilisées par le système sont garanties, ce qui inclut les clés de diversifications gérées par le module SAM de l'UTL ainsi que les clés secrètes permettant le chiffrement des communications entre les différents équipements.

6.1.2 Les certificats utilisés par le système

L'intégrité des certificats utilisées par le système sont garanties, ce qui inclut le certificat de l'autorité, la liste des certificats et des révocations.

6.1.3 Les crédits et identifiants d'accès

L'intégrité et la confidentialité des crédits et identifiants d'accès sont garanties, ce qui inclut les ID et informations contenus dans le badge Mifare DESFire®, les codes PIN.

6.1.4 Les droits d'accès et profils des utilisateurs

L'intégrité et la confidentialité des données de gestion des utilisateurs du système sont garanties, ce qui inclut les droits d'accès créés, gérés et révoqués par les exploitants ainsi que les données associées à leur profil et permettant de les relier personnellement au badge qui leur est assigné.

6.1.5 La configuration des équipements

L'intégrité et la confidentialité de la configuration des équipements sont garanties, ce qui inclut celle des UTL, des lecteurs connectés, des serveurs et des postes d'exploitation.

6.1.6 Les firmwares

L'intégrité, la confidentialité et l'authenticité des firmwares de mise à jour des équipements de la cible d'évaluation sont garanties.

6.2 Gestion des biens sensibles par le système

		Clés secrètes		Certificats	Informations des utilisateurs			Configuration	Firmware
		Clés de zones de sécurités (Clés DESFire)	Clés de chiffrement des échanges	Clés privées des certificats	ID DESFire	Journaux	Codes PIN	Profils / droits d'accès	Configuration des équipements	Clés de déchiffrement des firmwares
La TOE	Tête de lecture		X*							
	UTL	X	X	X	X	X	X	X	X	X
Environnement de la TOE (hors du périmètre)	Badges Mifare DESFire®	X*			X					
	Serveur iP Manager	X		X	X	X	X	X	X	

* Ces clés sont diversifiées

7 Description des menaces

7.1 Profil des attaquants

Les attaquants potentiels retenus sont les suivants :

7.1.1 Profil 1

Un attaquant à l'extérieur de la zone sensible. Il existe des risques d'attaque physique sur les têtes de lecture (scénario d'arrachement ou d'ouverture de capot), il peut dans ce cas perpétrer des attaques logiques sur les liaisons 2-smart ou RS485 entre la tête de lecture et l'UTL.

7.1.2 Profil 2

Un attaquant ayant accès à la zone sensible mais pas à la zone protégeant l'UTL ; Il peut dans ce cas perpétrer des attaques physiques sur les câbles et logiques sur les liens IP, 2-smart et RS485:

- Liaison IP entre le serveur et l'UTL.
- Liaison 2-smart entre la tête de lecture et l'UTL
- Liaison RS485 entre la tête de lecture et l'UTL

7.1.3 Profil 3

Un attaquant ayant accès à la zone protégeant l'UTL ; il peut perpétrer des attaques :

- logiques (liens IP, 2-smart et RS485) et physiques sur l'UTL par le biais de la liaison IP entre le filtre et le serveur (repères 2a)ainsi que par le biais des liaisons 2-smart ou RS485 entre l'UTL avec les têtes de lecture.
- physique par le biais de la lecture /ecriture des mémoires.

7.2 Intrusion sur la liaison entre l'UTL et le serveur

Cette intrusion concerne le réseau LAN Ethernet TCP/IP (repères 2a : sur la Figure 1) et correspond à une Intrusion sur le réseau LAN du client.
Les **attaques logiques** portent sur l'interception de données sensibles ou d'injection de données /commandes.
L'attaquant dispose de moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes.
Selon le « Guide de sécurité des technologies sans contact pour le contrôle des accès physiques » (Chapitre 3.4), l'intrusion correspond au :

- Niveau III avec franchissement par attaque logique simple. L'attaquant dispose de matériels ou maquette électronique spécifique facilement réalisable.
- Niveau IV avec franchissement par attaque logique sophistiquée. L'attaquant dispose de matériels comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place

Ecoute transactions échangées sur le LAN	**Menaces**
Ecoute d'une transaction contenant l'ID	Copie du badge
Ecoute d'une transaction contenant le Code PIN	Usurpation d'identité (Authentification PIN par le malveillant)
Ecoute d'une transaction contenant les plages horaires	Elargir des périodes d'accès
Ecoute d'une transaction contenant l'affectation des droits	Modifier/étendre des droits

Ecoute d'une transaction contenant des commandes	Ouverture d'un accès
Ecoute des transactions avec le serveur	Emulation d'une UTL

7.3 Intrusion sur le bus dédié 2-smart

Cette intrusion concerne la topologie des bus 2-smart (repères 3 sur la Figure 1) et correspond à une intrusion sur des infrastructures filaires (bus).
Les attaques logiques portent sur l'interception de données sensibles ou d'injection de données /commandes.
L'attaquant dispose de moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes.
Selon le « Guide de sécurité des technologies sans contact pour le contrôle des accès physiques » (Chapitre 3.4), l'intrusion correspond au :

- Niveau III avec franchissement par attaque logique simple. L'attaquant dispose de matériels ou maquette électronique spécifique facilement réalisable.
- Niveau IV avec franchissement par attaque logique sophistiquée. L'attaquant dispose de matériels comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place

Transaction /échanges	**Menaces**
Ecoute d'une transaction contenant l'ID	Copie du badge
Ecoute d'une transaction contenant le Code PIN	Usurpation d'identité (Authentification PIN par le malveillant)
Ecoute des transactions avec l'UTL	Emulation d'un ou plusieurs lecteurs afin de rejouer des trames valides ou d'effectuer une attaque DOS (Denial of Service)

7.4 Intrusion sur le bus dédié RS485

Cette intrusion concerne la topologie des bus RS485 (repère 4 sur la Figure 1) et correspond à une intrusion sur des infrastructures filaires (bus).
Les attaques logiques portent sur l'interception de données sensibles ou d'injection de données /commandes.
L'attaquant dispose de moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes.
Selon le « Guide de sécurité des technologies sans contact pour le contrôle des accès physiques » (Chapitre 3.4), l'intrusion correspond au :

- Niveau III avec franchissement par attaque logique simple. L'attaquant dispose de matériels ou maquette électronique spécifique facilement réalisable.
- Niveau IV avec franchissement par attaque logique sophistiquée. L'attaquant dispose de matériels comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place

Transaction /échanges	**Menaces**
Ecoute d'une transaction contenant l'ID	Copie du badge
Ecoute d'une transaction contenant le Code PIN	Usurpation d'identité (Authentification PIN par le malveillant)
Ecoute des transactions avec l'UTL	Emulation d'un ou plusieurs lecteurs afin de rejouer des trames valides ou

	d'effectuer une attaque DOS (Denial of Service)

7.5 Attaque physique sur l'UTL

- Tentative de cryptanalyse et lecture du code exécutable, de la base de données ou des clés sécrètes.
- Substitution d'une UTL

7.6 Attaque physique sur le lecteur ou clavier-lecteur RFID

Un attaquant arrache ou ouvre la tête de lecture de son support de fixation.

- Tentative de remplacement du lecteur ou des clés sécrètes.
- Substitution d'une tête de lecture

7.7 Corruption du firmware

L'attaquant parvient à injecter et faire exécuter un firmware corrompu sur l'UTL. L'injection de code peut être temporaire ou permanente et ceci inclut donc toute exécution de code non prévue ou non autorisée.
L'attaquant peut également réussir à substituer une mise à jour corrompue à une mise à jour légitime. Un utilisateur pourra alors tenter d'installer cette mise à jour dans l'UTL par des moyens légitimes.
Enfin, l'attaquant peut également tenter d'installer une ancienne version légitime du firmware sans en avoir le droit.
Les mises à jour par les opérateurs légitimes ne sont pas considérées comme des attaquants car ce sont eux qui s'assurent de la provenance du firmware avant l'installation.

8 Description des fonctions de sécurité

8.1 Fonctions de sécurité

La fonctionnalité principale de la solution SCAiP est de fournir au client la capacité de mettre en œuvre une solution d'accès sécurisée dans sa propre infrastructure. Cette mise en œuvre passe par :

- La définition des sites, des zones et leur niveau de sécurité, des points d'accès (locaux ou portes)
- La définition d'une architecture adaptée au contrôle des flux (transfert d'informations)
- L'adoption d'une politique de sécurité cohérente et non ambiguë par rapport aux moyens organisationnels
- L'application d'une politique d'identification (identifiant unique et code PIN pour chaque usager)
- L'exploitation des audits analyse/consultation des historiques
- La mise en place d'une politique de sécurité pour les clés (génération, protection, mise à la clé des UTL)

8.1.1 Les protections :

8.1.1.1 P1 : Protection des données échangées entre le Serveur et l'UTL

Cette protection passe par l'établissement d'un canal de communication TLS1.3, les deux parties ayant ouvert une session avec une authentification mutuelle au préalable. C'est l'UTL qui initie la connexion TLS vers le serveur, aucune connexion entrante n'est possible. Lors de cette connexion,

le serveur et l'UTL s'authentifient. Cette application ne permet pas de se connecter directement sur l'UTL pour prendre la main sur cette dernière.
Une fois la connexion initiée, le serveur et l'UTL ont une clé commune de session. Cette clé est à renouveler tous les jours.
Les commandes et les transactions échangées entre le serveur et l'UTL sont protégées en confidentialité.
Pour les tentatives de rejeu, la protection passe par la mise en œuvre des mécanismes cryptographiques.

8.1.1.2 P2 : Sécurisation de l'UTL

Les UTL sont protégées des attaques physiques par installation dans une zone protégée uniquement accessible aux administrateurs de confiance.
De plus, l'UTL est intégrée dans un coffret protégé par un tamper et un système basé sur des capteurs permettant de détecter l'ouverture et l'intrusion dans le coffret.
Les éléments de sécurité sont stockés dans un module SAM (Mifare SAM AV3 de niveau CC EAL6+).
Les interfaces de débogage (JTAG, USB, port série) sont désactivées.
Les données sensibles dans les mémoires flash sont protégées en intégrité, confidentialité et authenticité.

Les composants sensibles (microcontrôleur, mémoires flash) sont poncés et cachés sous une résine en époxy rigide.
La détection de défauts génère systématiquement des alarmes techniques vers le serveur.
Cette détection les types de défaut suivants :

- OCo (Ouverture Coffret) ou intrusion coffret.
- Défaut de communication du bus 2-smart (repère 3 de la Figure 1). Le défaut de communication est analysé par le serveur.
- Défaut de communication du bus RS485 (repère 4 de la Figure 1). Le défaut de communication est analysé par le serveur.
- Défaut de communication du LAN (repères 2a et 2b la Figure 1). Le défaut de communication est analysé par le serveur.

8.1.1.3 P3 : Protection des données échangées entre l'UTL et les lecteurs (avec ou sans clavier)

Les identifiants de tous les lecteurs (avec ou sans clavier) qui doivent être connectés à l'UTL sont rentrés dans le serveur et envoyés de façon sécurisée à l'UTL. Seules ces lecteurs peuvent dialoguer avec l'UTL de façon sécurisée à l'aide d'un chiffrement des données en AES 128-bit.
Le lecteur RFID (avec ou sans clavier) se comporte en mode transparent lors de la présentation d'un badge et ne contient donc aucune donnée sensible. C'est donc le badge qui s'authentifie directement auprès du module SAM embarqué dans l'UTL.

Un code PIN accentue la sécurité de l'accès. Il est saisi sur le lecteur équipé d'un clavier. Ce code est transmis haché à l'UTL via la liaison sécurisée.

Le lecteur (avec ou sans clavier) utilise deux clés de session déterminées lors de l'échange initial de clés avec l'UTL.
Les lecteurs utilisent des clés diversifiées fournies par l'UTL. Ces clés sont uniques par UTL et par lecteur.

- A l'installation, une clé d'authentification et une clé de chiffrement sont négociées entre l'UTL et chaque lecteur (avec ou sans clavier) : il y a appairage.
- En cas de substitution d'un lecteur (avec ou sans clavier) :
  - La communication avec l'UTL ne permet de ne plus prendre en compte le badge ou le code pin présenté
  - Un « défaut authentification lecteur » (avec ou sans clavier) est remonté vers le serveur
- Pour débloquer la prise en compte d'un badge ou d'un code pin devant le lecteur (avec ou sans clavier) (cas d'un échange d'un clavier-lecteur en maintenance par exemple), une intervention d'une personne habilitée doit être réalisée au niveau du serveur.

8.1.1.4 P4 : Protection du code PIN

Certains accès se font sur la présentation d'un badge et un code pin. Les codes pins sont stockés dans le serveur et l'UTL, en utilisant une fonction de hachage.

8.1.1.5 P5 : Sécurisation du lecteur (avec ou sans clavier)

Le lecteur (avec ou sans clavier) RFID est placé en zone publique.
La tête de lecture, au format P40, possède un capteur d'arrachement et d'ouverture de capot, directement connecté au microcontrôleur.
La tête de lecture, au format P80 ou PK80, possède un capteur d'arrachement et d'ouverture de capot, directement connecté au microcontrôleur.
En cas de déclenchement, le microcontrôleur, si l'option de paramétrage est activée, efface les clés critiques qui sont dans la Flash.
La détection de défauts génère systématiquement des alarmes techniques vers le serveur.
Cette détection concerne principalement la détection d'arrachement du lecteur. Le défaut est analysé par l'UTL, qui la remonte au serveur.

8.1.1.6 P6 : Sécurisation des mises à jour firmware

Les fichiers firmware sont générés, chiffrés et signés par FDI MATELEC.

À chaque installation d'un nouveau firmware :

- une première vérification sommaire est faite par le serveur mais celui-ci n'ai pas capable de vérifier l'authenticité du fichier.
- l'intégrité et l'authenticité sont vérifiées par l'UTL juste après avoir reçu le dernier paquet du nouveau firmware (avant sa prise en compte effective). Si une de ces deux vérifications est incorrectes, alors le nouveau firmware est rejeté. L'installation d'une ancienne version de firmware n'est pas possible.

8.1.1.7 P7 : Sécurisation contre les attaques relais

Un mécanisme de protection contre les attaques de relais est mis en place dans l'UTL. Pour contrer cette attaque, un minuteur mesurant la durée de la transaction permet de refuser l'accès lorsque les temps de communications sont trop longs.

8.1.1.8 P8 : Protection des attaques par déni de service

Un filtre (type firewall) est préconisé dans le système dans le but de filtrer les messages émis sur le réseau et de transmettre uniquement les messages à destination de l'UTL. Ceci a pour objectif, d'éviter que l'UTL subisse des ralentissements lors de son fonctionnement.

De plus, l'UTL contrôle également le nombre de paquet reçus afin de détecter une attaque par déni de service. Un nombre trop important de paquet reçus sur une période donnée aboutit à une

coupure du PHY ce qui équivaut à un débranchement du câble Ethernet. Un évènement est journalisé et celui-ci peut être récupéré sur le serveur avec une opération manuelle.
Après coupure du PHY, la communication est réactivée au bout de 60 secondes. L'évènement journalisé peut alors être récupéré.

8.2 Justification de couverture des menaces par les fonctions de sécurité

Protections / Menaces	P1 Protection des échanges entre l'UTL et le serveur	P2 Protection de l'accès physique à l'UTL	P3 Protection des échanges entre la tête de lecture et l'UTL	P4 Protection du code PIN	P5 Détection de l'arrachement d'une tête de lecture	P6 Protection du firmware	P7 Protection contre les attaques relais	P8 Protection contre les attaques par déni de service
Attaque des échanges entre l'UTL et le serveur	X	X						
Attaque des échanges entre l'UTL et les têtes de lecture		X	X	X				
Arrachement de la tête de lecture					X			
Corruption du firmware						X		
Attaque relais							X	
Déni de service								X

9 Annexes

9.1 Informations sur les menaces et la sûreté

Le tableau ci-dessous est extrait du « Guide de sécurité des technologies sans contact pour le contrôle des accès physiques » (Chapitre 3.4) :

Menaces potentielles			Niveaux de sûreté
Qui ?	**Quels moyens**	**Quelles connaissances ?**	
Franchissement par attaque mécanique et/ou logique « simple »			
Pénétrations préméditées de personnes faiblement équipées	Matériel et méthode obtenus dans le commerce ou sur Internet.	Connaissance basique du système acquise au travers de documents publicitaires ou technico-commerciaux émis par le fabricant ou les distributeurs.	**II**
Franchissement par attaque mécanique et/ou logique « évoluée »			
Pénétrations préméditées de personnes initiées et équipées.	Matériel ou maquette électronique spécifique facilement réalisable.	Connaissances recueillies à partir de l'examen d'un dispositif.	**III**
Franchissement par attaque mécanique et/ou logique « sophistiquée »			
Pénétrations préméditées de personnes initiées, fortement équipées et renseignées.	Matériel comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place.	Connaissances sur la conception et l'exploitation du système. Ceci implique d'avoir accès à des informations confidentielles du fabricant.	**IV**

Tableau 3 : Principales menaces en fonction du niveau de sûreté

Ce tableau regroupe les principales menaces avec les informations suivantes :

- **Pour le niveau II** : la solution SCAiP est une solution professionnelle avec une communication sous contrôle. De ce fait, les connaissances du produit sont non diffuses et s'adressent uniquement à des professionnels. Les outils d'aide à la mise en œuvre ne sont communiqués qu'aux clients de la solution. Elles ne sont pas mises en ligne via internet.
- **Pour le niveau III** : la solution SCAiP permet de générer des alarmes en cas de ruptures momentanées des liaisons (ex : alarmes défauts de communications) ; de substitution d'un équipement [ex : remplacement d'une UTL ou d'un lecteur (ou clavier-lecteur) par une maquette spécifique].
  Ces alarmes peuvent générer des alertes vers l'extérieur.
- **Pour le niveau IV** : les utilisateurs devront s'assurer que les mécanismes cryptographiques, mis en œuvre sur les réseaux LAN et dédiés, sont activés et conformes aux recommandations d'utilisation du produit.

9.2 Annexe 2 : Tableau 2 ANSSI - Niveaux de sûreté et niveaux de résistance aux attaques

Niveau de sûreté	Résistance aux attaques logiques	Méthode	Technologie	Caractéristiques	Mises en œuvre sur SCAiP
I	-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés, cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.	Facilement clonable	**NON**
II	L1	Authentification du badge.	Carte ISO 14443, authentification à cryptographie symétrique	Authentification reposant sur une clef commune ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).	**OUI en AES**
III	L2	Authentification du badge, clefs dérivées recommandées.	Carte ISO 14443, authentification à cryptographie symétrique	Authentification reposant sur une clef dérivée d'une clef maîtresse ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).	**OUI en AES**
IV	L3	Authentification du badge et du porteur par un second facteur (information mémorisée ou élément biométrique). Clefs dérivées.	Carte ISO 14443, authentification à cryptographie symétrique. Saisie d'un code mémorisé ou d'un élément biométrique.	Authentification reposant sur une clef dérivée d'une clef maitresse ; Algorithmes et protocoles d'authentification connus et réputés (3DES, AES).	**OUI en AES et double identification avec code PIN**

Tableau 4 : Correspondance entre le niveau de sûreté et la résistance aux attaques logiques

Source ANSSI : « Guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques »

9.3 Annexe 3 : Badges d'accès

Les badges d'accès basés sur la technologie NXP Mifare® DESFire (EV3) sont hors périmètre de l'évaluation.

Pour comprendre la façon dont ces badges sont lus par les UTL, la Figure 7 représente la structure des applications et des fichiers dans le Mifare® DESFire EV3. L'organisation de la mémoire de MIFARE DESFire EV3 est flexible et peut être dynamiquement structuré pour s'adapter à toutes les exigences de l'application. Chaque dossier d'application est un conteneur de fichiers de données utilisables dans un certaines applications du monde réel (par exemple, la billetterie de transport). Il y a 5 types de fichiers disponibles pour le stockage de données et 1 type de fichier pour stocker le MAC (Message Authentification Code) de la transaction. Dans le dossier de l'application, il existe un ensemble de clés et de paramètres de configuration dédiés à l'application. Le propriétaire de l'application peut organiser librement la structure des fichiers et les paramètres de sécurité dans son application. Une application adjacente n'aura pas accès à ses fichiers tant qu'ils ne possèdent pas les droits de sécurité appropriés. Au niveau PICC, il existe un autre jeu de clés et de paramètres de sécurité pour le propriétaire du PICC. Ce dernier aura le droit de créer ou de supprimer toute application, mais il n'aura pas accès aux fichiers de l'application, à moins qu'il ne connaisse également les clés de l'application.

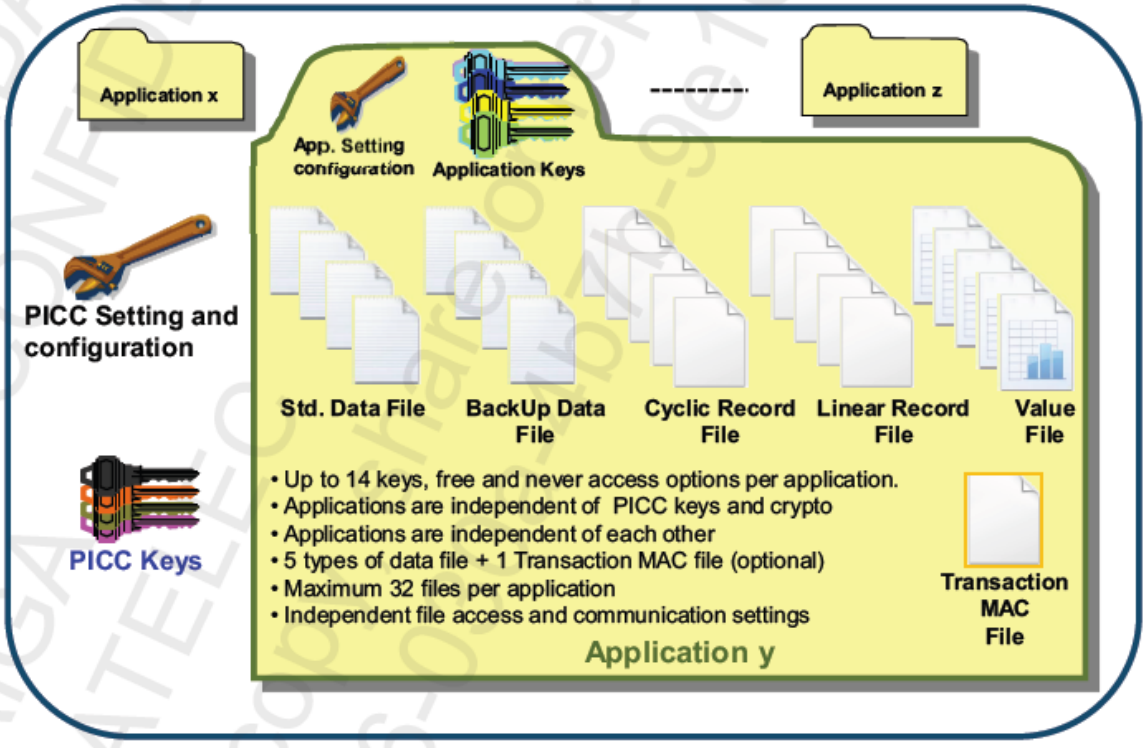

Figure 7 : Structure Mifare® DESFire

1. Le badge reçoit une personnalisation électrique :
   - Cette opération est réalisée au niveau d'un poste d'encodage. Ce poste est sous contrôle d'un responsable sûreté, habilité et qui est gardien des secrets.
   - La fonction d'encodage est soit intégré au serveur (ex : badges encodés par le client), soit complètement externalisé (ex : badges encodés par une société tierce).
2. La lecture sécurisée des badges par les lecteurs d'accès passe par un mécanisme d'authentification mutuelle entre le badge et l'UTL. Cette authentification se fait au niveau de l'application d'accès du badge.

3. La lecture dépend de la façon dont le badge a été administré au niveau root et au niveau application. Il est à noter que les fonctions de lectures sécurisées avec clés diversifiées font appel à différents algorithmes de calculs de clés possibles.
4. Cette lecture peut être réalisée de deux façons :
    - Avec une clé de lecture commune correspondant au niveau II (*)
    - Avec une clé diversifiée qui est une clé unique et correspondant au niveau III (*)

(*) Dans tous les cas, les badges correspondront aux niveaux II et III du tableau des niveaux de sûreté.

Note : Pour répondre aux différents besoins liés aux calculs des clés, ces fonctions sont traitées au niveau de l'UTL et à partir d'algorithmes reconnus tels que AES, AES CBC, AESCMAC.