SUPERVISION ET CONTROLE DE SITES

Note Technique

Architecture cible de sécurité

Rév.	Date	Auteur	Vérificateur	Approbateur	Statut
A	27/06/2017	F. ROBEYN	J.P. HAENLIN	O. BERTHET-RAYNE	
B	19/04/2018	O. BERTHET-RAYNE	J.P. HAENLIN	F. ROBEYN	
C	30/01/2019	O. BERTHET-RAYNE	J.P. HAENLIN	F. ROBEYN	
D	28/01/2020	O. BERTHET-RAYNE	J.P. HAENLIN	F. ROBEYN	
E	05/11/2020	O. BERTHET-RAYNE	J.P. HAENLIN	F. ROBEYN	

Diffusion	Interne	
	Externe	

Nom du fichier	Référence document	Date d'impression	Page	Rev
Evolynx-NT-FR - Architecture cible de securité - E.doc	Evolynx-NT-FR	05/11/20	1 / 27	E

Historique des Modifications

Rév.	Chapitres	Pages	Objet de la modification
A0			Création du document
A			Première diffusion
B		13, 17, 21, 22, 24, 25	Prise en compte des remarques de l'ANSSI
C		5, 11, 12, 22	Mise à jour des versions et référence de document suite aux tests pré - CSPN
D			Mise à jour globale du document
E			Version publique

Sommaire

1 Présentation

1.1 Objectif

Ce document a pour objectif de décrire l'architecture cible de sécurité pour l'évaluation CSPN sur la solution EVOLYNX dans la catégorie « Identification, authentification pour le contrôle des accès physiques ».

1.2 Identification du produit

Nom du produit : EVOLYNX iPerflex
Version supervision : v8.2.1a4
Version firmware ITL/UED : v8.2.0c

Constructeur : Secure Systems & Services

Site web : https://www.secure-systems.fr

1.3 Document de référence

Réf	Document	Révision	Date
[Doc1]	Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques	1.0	19/11/2012
[Doc2]	ANSSI-CSPN-2015-02 Rapport de certification ANSSI-CSPN-2015/02		10/05/2015
[Doc3]	Evolynx-NT-FR - Mécanismes cryptographiques	D	28/01/2020

1.4 Règles de l'art

Algorithme	Version
TLS	1.2
AES	128 bits minimum / 192 voire 256
SHA	256

2 Argumentaire du produit

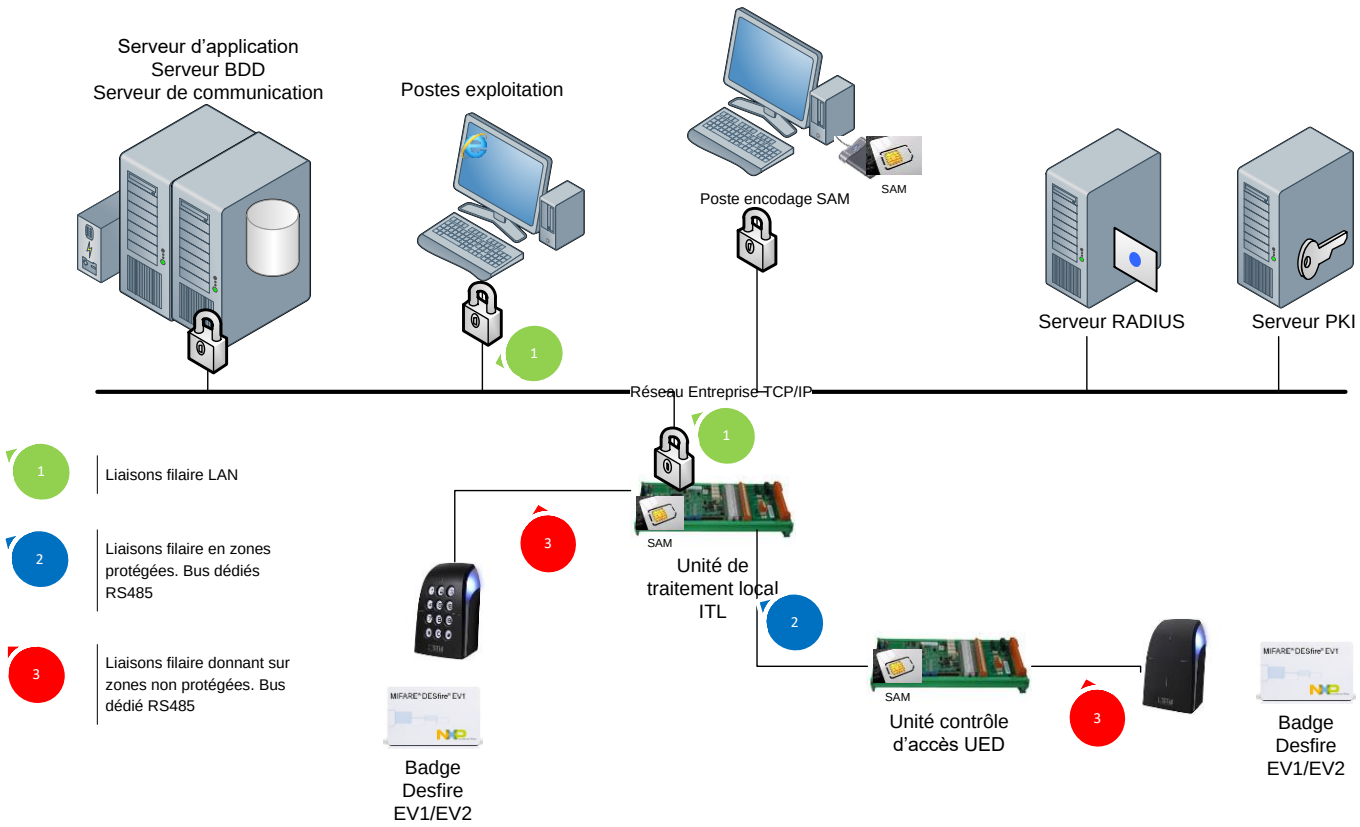
2.1 Description générale du produit

La solution de sureté iPerflex permet de gérer de façon centralisée les droits d'accès physique d'une population. Cette solution s'adapte aux infrastructures multi site.

Elle repose sur un ensemble de sous-systèmes :
- Serveur de base de données,
- Serveur d'application
- Frontal de communication,
- Equipements terrain ITL

Les serveurs peuvent être hébergés sur des machines virtuelles ou physiques. Ils peuvent être démultipliés afin d'augmenter les capacités de traitement du système.

Le contrôle des accès est assuré localement par des terminaux 'intelligents', appelés ITL, raccordés au réseau de communication IP. Les ITL possèdent une mémoire sauvegardée contenant une copie de la base de données du serveur. Cela autorise un fonctionnement autonome en cas de coupure de la liaison avec le serveur.



2.1.1 Description fonctionnelle

La solution de sureté ***EVOLYNX*** est un système de contrôle d'accès physique, qui permet de répondre à des besoins de sécurisation et de supervision pour le contrôle de sites.
Il permet d'associer des identifiants à des personnes et de filtrer leurs accès sur un site en gérant des autorisations d'accès.
Cette solution est déployée chez le client final et utilisée par des responsables de sécurité, qui vont définir et administrer les fonctions d'accès pour les zones protégées.

*La solution **EVOLYNX** permet de répondre aux exigences de sécurité accrue dans les autorisations d'accès aux zones sensibles par :*

- L'identification fiable de la personne par plusieurs possibilités combinées :

- *Affectation par personne d'un ou plusieurs badges.*
- *Affection d'un code pin pour accéder à des zones nécessitant une authentification.*
- *Enregistrement de données biométriques, empreinte digitale et/ou réseau veineux.*

- La gestion des droits d'accès poussée :

- *Droits d'accès standards.*
- *Droits d'accès projets : l'attribution d'autorisation de droits d'accès spécifiques à un « projet » afin de restreindre les droits d'accès habituels des usagers selon l'activité de ces projets. Un projet est une situation d'exploitation qui n'autorise que les personnes explicitement habilitées au projet à accéder aux zones contrôlées par des accès intégrés au projet, lorsque le projet est actif.*
- *Droits d'accès multisites gérés par site.*
- *Droits d'accès minimum par catégorie de personnes par site, ou fonction de règles préalablement établies.*
- *Droits d'accès personnalisés avec droit temporaire et inhibition automatique pour des missions ponctuelles à des zones normalement non autorisées.*
- *Droits d'accès « partagés ». Chaque accès peut être géré par plusieurs propriétaires qui utilisent le même accès selon leur profil.*
- *Droit d'accès planifié qui permet de valider les autorisations d'entrée sur des jours de la semaine.*
- *Droit d'accès selon niveau de crise (Mode normal + 9 niveaux de crise).*
- *Gestion de l'anti-passback géographique par zone, avec contrôle avant ou après sortie de zone.*
- *Contrôle du passage effectif de l'accès activable ou pas selon le degré de sécurité. C'est l'obstacle physique (porte, barrière, tripode, ...) qui donne l'information de passage. Fonction utilisée dans le cas d'une zone gérée en anti-passback.*
- *Gestion de l'anti-passback géographique : une personne entrée dans une zone au préalable ne pourra pas y entrer de nouveau avant d'en sortir d'abord.*
- *Gestion de l'anti-passback temporel : une personne qui entre par un accès donné ne pourra pas y entrer de nouveau avant un délai configurable.*

*La gestion de l'anti-passback, au-delà de la solution **EVOLYNX,** exige des contraintes d'exploitation et d'infrastructure :*

- *Il faut obligatoirement disposer de lecteur en entrée et en sortie de la zone traitée en anti-passback pour identifier les personnes qui entrent et sortent.*
- *Les usagers doivent s'identifier individuellement en entrée et en sortie des zones contrôlées. Pour cela, les obstacles physiques (barrière, tripode, ...) qui contrôlent l'unicité de passage sont recommandés pour garantir cette exigence.*

Une fois les autorisations d'accès aux zones sensibles paramétrées, le système est opérationnel et enregistre tous les mouvements. L'exploitant utilisera alors le système EVOLYNX comme un système d'information puissant et sécurisé pour les besoins suivants :

- *Mise en attention : pas d'incidence sur les droits d'accès de la personne mais tout accès sera tracé afin de surveiller les mouvements de la personne.*
- *Consultation des personnes, badges, historique selon des critères multiples.*
- *Inventaire des personnes, badges créés, et des statistiques mensuelles d'opérations sur les badges personnes, telles que :*
  - *Création, modification, suppression de fiches personnelles.*
  - *Création, modification, suppression de badges.*
  - *Attribution, suppression de droits d'accès.*
- *Historiques, statistiques des personnes, visiteurs et prestataires externes et conservation des données. Impression et export des données et historiques.*
- *Traçabilité des actions opérateurs.*
- *Archivage des événements, historiques et statistiques.*
- *Consultation des mouvements d'accès.*
- *Liste des présents en zone, comptage en zone avec seuil possible d'interdiction.*
- *Editeur de requêtes personnalisées.*
- *Restauration/Consultation archivage mensuel des événements.*
- *Edition et export type Excel planifié périodique, sur alarme, sur événement, statistique.*
- *Redondance à chaud des serveurs en cluster, des frontaux.*

2.1.2 Listes des éléments constituants la solution

- Le serveur de gestion des accès iPerflex, comprenant les briques fonctionnelles base de données centralisé, serveur d'application et frontal de communication.
- La station de programmation des SAM.
- Les postes (client léger) d'exploitation iPerflex.
- Les contrôleurs ITL.
- Les interfaces UED.
- Les lecteurs de proximité de marque STid en configuration lecteur transparent
- Les lecteurs claviers de marque STid en configuration lecteur transparent
- Les badges d'accès de marque NXP et de modèle Mifare® Desfire EV1

Les lecteurs de proximité permettent de réaliser l'identification tandis que les lecteurs claviers permettent de réaliser l'authentification du porteur de badge au travers de la saisie d'un code PIN.
Le système demande le code pin après avoir identifié le porteur et vérifié que celui-ci dispose de droits sur l'accès concerné.

2.1.3 Base de données

Rôle : La base de données Oracle est le cœur du système pour :

- *Le stockage des données de configuration et d'exploitation.*
- *L'enregistrement des historiques.*

Elle assure également :

- *L'intégrité des données.*
- *La définition des utilisateurs applicatifs et leurs droits d'accès aux données.*
- *L'optimisation des recherches (vues, index…).*

2.1.4 Serveur d'application

Rôle : Le serveur assure l'interface entre les IHM et la base de données :

- *Le traitement des fonctions métiers (création personnes, badges, attribution des droits, gestion des visiteurs, affichage des synoptiques…).*
- *La persistance des données dans la base.*
- *La mise à disposition des données pour les postes clients.*
- *La surveillance de fonctionnement des équipements.*
- *Les traitements batch (suppression des données périmées pour les droits d'accès, demandes de visite…).*
- *L'exécution des asservissements généralisés.*

Le serveur est complété d'un programme appelé DatabaseManager permettant d'assurer les fonctions de :

- *Export et sauvegarde de la base de données*
- *Clôture et export de l'archivage mensuel des événements.*

2.1.5 Poste d'exploitation

Le poste d'exploitation utilise l'interface Homme Machine (IHM). L'IHM assure l'interface des opérateurs avec le système EVOLYNX

Accessible à partir de tous postes d'exploitation sous forme d'une application interactive dans un navigateur web, elle permet l'accès aux différents menus, écrans, synoptiques… suivant des profils utilisateurs.

Les principales fonctions sont :

- *La gestion des usagers (personnes, badges…).*
- *La définition et attribution des droits d'accès.*
- *La gestion des visiteurs.*
- *Le traitement des alarmes (affichage, acquittement, aide à l'intervention…).*
- *La consultation des événements, historiques, statistiques.*
- *L'affichage de synoptiques animés.*
- *L'affichage des images vidéo et la consultation de films enregistrés, la configuration du système et des équipements installés (UTL, accès, plages horaires…).*
- *Les commandes d'exploitation (ouverture de porte, changement de mode d'accès…).*
- *La sécurisation de fonctionnement (utilisateurs, profils utilisateur).*
- *Le paramétrage et la codification des éléments caractéristiques du système.*
- *La surveillance des différents éléments du système (sous-systèmes, espace disponible…).*

Il n'existe qu'une seule interface pour réaliser l'ensemble des fonctions accessibles dans notre solution, y compris le paramétrage des équipements terrain.

2.1.6 Frontal de communication

Rôle : Sa mission est d'assurer le pilotage des communications entre la base de données et les ITL, en réalisant :

- *La transmission des données vers les ITL.*
- *L'acquisition des événements détectés par les ITL.*
- *Le traitement des événements/alarmes acquis (alarmes, historiques…).*
- *La surveillance des ITL.*

Dans le cas d'architectures mettant en œuvre l'interconnexion d'iPerflex avec des systèmes externes (vidéo-surveillance, centrales d'alarme, …), le frontal assure également :

- *La transmission des données vers les systèmes externes.*
- *L'acquisition des événements détectés par les systèmes externes.*
- *Le traitement des événements/alarmes acquis (alarmes, historiques…).*
- *La surveillance de la communication avec les systèmes externes.*

2.1.7 Equipements de terrain

2.1.7.1 Concentrateur d'accès ITL

L'ITL est une carte électronique qui acquiert des informations venant :

- *D'UED et/ou de lecteurs de badge, via des liaisons série (RS485).*
- *D'entrées/sorties pour la gestion d'alarme ou de contrôle d'accès.*

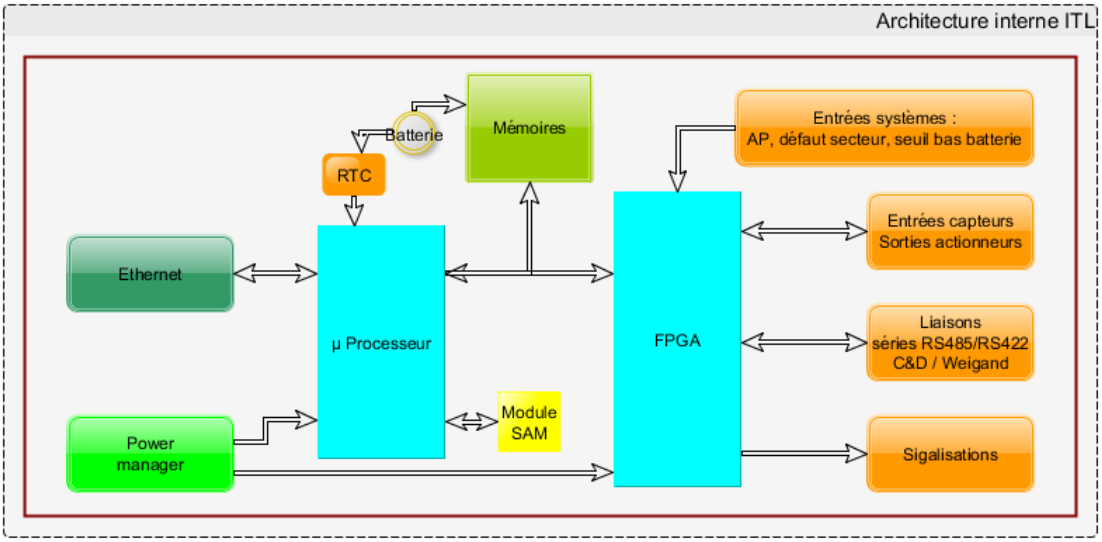
Elle contrôle la validité des badges, stocke les évènements et les mouvements, les horodate et les transmet au superviseur. L'ITL possède une intelligence locale et peut fonctionner de manière autonome en mode dégradé.

Elle gère jusqu'à 16 UED ou UAD (unité d'alarme déporté).

Elle dispose de 4 bus de communications pouvant être utilisés soit pour la communication avec des UED, soit en liaison directe vers un lecteur.

Elle peut gérer seule jusqu'à 4 accès et jusqu'à 32 accès au total au travers de ces UED.

Elle dispose d'un support de lecteur de carte SAM et d'une SAM NXP AV2 externe.



Composant	Description
Désignation	ITL
Référence produit	M20102
Version logicielle	V8.2.0c
Processeur	MCF 54452 32 bits
OS embarqué	Linux 2.6.23
Mémoires	Flash, SRAM, SDRAM

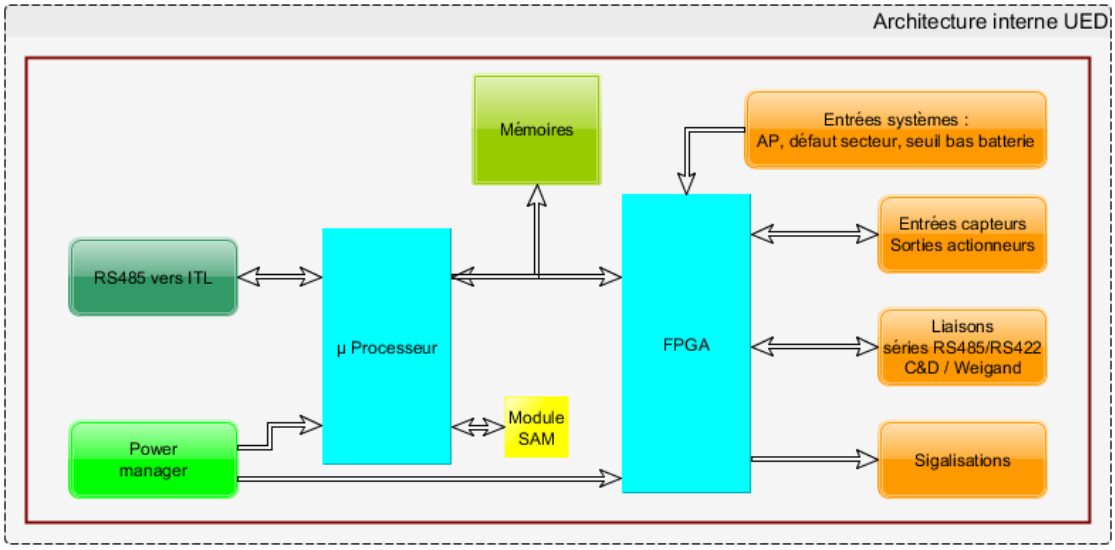
2.1.7.2 Unité de contrôle d'accès UED

La carte UED est une carte d'extension de l'ITL pour la gestion des lecteurs de badges, des capteurs et des actionneurs.

Elle ne dispose pas d'intelligence locale, ni de mémoire de stockage de données et doit être obligatoirement connectée à une ITL.

Elle dispose d'un bus dédié RS485 permettant la communication avec son ITL et de 4 bus de RS485 pour communiquer avec les lecteurs terrains.

Elle dispose d'un support de lecteur de carte SAM et d'une SAM NXP AV2 externe.



Composant	Description
Désignation	UED
Référence produit	M20122
Version logicielle	V8.2.0c
Processeur	MCF 54452 32 bits
OS embarqué	Linux 2.6.23
Mémoires	Flash, SDRAM

2.1.8 Réseaux LAN & raccordements

Les postes opérateurs et les serveurs sont raccordés sur un réseau du client. Ce réseau est administré, par le client.
Le réseau est de type Ethernet TCP/IP généralement IPv4.
Ce réseau permet d'échanger des informations entre les postes opérateurs et les serveurs ainsi qu'avec les équipements terrain de type ITL.

Le réseau client est hors périmètre de l'évaluation CSPN.

2.1.9 Réseaux dédiés

Les réseaux dédiés sont ceux définit par les repères (2) et (3) sur la figure d'architecture.

Le repère (2) concerne les liaisons filaires de communication entre l'ITL et ses UED. Cette liaison n'est pas partagée avec d'autres équipements. Elle correspond à un bus de terrain RS485. Les échanges sont réalisés sous un protocole Modbus intégrant un chiffrement des données et une signature

Le repère (3) concerne les liaisons filaires de communication entre ITL/UED et les lecteurs de proximité seul ou avec clavier. Les échanges sont réalisés sous un protocole SSCP intégrant un mode de communication chiffrée/signée. Ces lecteurs disposent d'une fonction permettant de communiquer en mode « transparent ou direct » avec le badge.

Ces deux réseaux sont inclus dans le périmètre d'évaluation

2.1.10 Serveur Radius

Le serveur Radius a pour rôle l'authentification IEEE 802.1X. Cela permet d'identifier l'ensemble des éléments qui se connectent sur le réseau Ethernet du client.
Les équipements réseaux doivent supporter le 802.1X et être paramétrés pour fonctionner avec ce principe d'authentification.
Remarque : l'authentification 802.1x n'est pas obligatoire dans la mise en œuvre de la sécurité du système de contrôle d'accès. C'est un mécanisme supplémentaire ajoutant une sécurité de plus. Il faut considérer cette fonctionnalité comme optionnelle.

2.1.11 Serveur infrastructure de PKI

Le serveur d'infrastructure de PKI a pour rôle entre autres de créer les certificats, publier des listes de certificats révoqués.
Les certificats mis en œuvre sont :

Protocole	Hôte	Communication avec	Format
HTTPS	Serveur d'application	L'ihm	X.509
EAP-TLS	Serveur d'application	Serveur Radius	X.509
SQLNET Encryption	Serveur d'application	Base de données	AES256
EAP-TLS	IHM	Serveur Radius	X.509
EAP-TLS	Frontal de communication	Serveur Radius	X.509
SQLNET Encryption	Frontal de communication	Base de données	AES256
EAP-TLS	ITL	Serveur Radius	X.509
TLS1.2	ITL	Frontal de communication	PKCS#12
TLS1.2	Frontal de communication	ITL	PKCS#12
TLS1.2	Poste de programmation des SAM	ITL	PKCS#12
TLS1.2	ITL	Poste de programmation des SAM	PKCS#12

2.1.12 Poste de programmation des SAM

Ce poste permet la programmation des SAM NXP AV2 au travers d'un logiciel client lourd.
Ce logiciel communique avec deux lecteurs de table de puce à insertion connecté en PCSC.

Ce poste permet la saisie des clés puis leur enregistrement dans une SAM Master.
Cette SAM Master dispose des clés accessibles, elle doit être séquestrée et utilisée exclusivement lors de la création d'une nouvelle SAM Esclave.

La saisie des clés peut être réalisée suivant différents modes :

- *Saisie manuelle.*
- *Saisie manuelle suivant un processus de cérémonie de remise des clés.*
- *Génération aléatoire.*
- *Génération d'une clé en saisissant une passphrase en suivant le RFC2898.*

Les clés pouvant être saisies concernent :

- *La clé de lecture des données d'identification du badge, présente dans la SAM Esclave Terrain.*
- *La clé PICC Master.*
- *La clé Application Master.*
- *La clé d'écriture des données d'identification du badge.*
- *La clé de changement des conditions d'accès.*
- *Ces clés sont présentes dans la SAM Esclave Encodage.*

2.1.13 Lecteur de proximité

Le rôle du lecteur de proximité est de servir d'antenne active afin d'alimenter la puce RFID présente dans le badge.
Les échanges de communications sont pilotés directement par le contrôleur connecté au lecteur.

Le lecteur/clavier dispose d'une fonctionnalité lecteur de proximité et d'une interface physique permettant à l'utilisateur de saisir un code PIN après avoir présenté son badge sur le lecteur.
Cette interface physique peut être de deux type : touches physique rétroéclairées ou touches sur écran tactile, dans ce dernier cas il est possible d'avoir un mode de fonctionnement avec apparition aléatoire de l'emplacement des touches.

2.2 Description de l'environnement d'utilisation du produit

Depuis plus de 30 ans, nous assistons nos clients dans leur démarche d'amélioration de leur solution de sureté.

Nous prenons en compte l'ensemble de cet environnement en intégrant :

- *La mise en œuvre de moyens technique et organisationnels.*
- *L'adéquation entre les menaces et les mesures mises en œuvre.*
- *Une stratégie de gestion de défense en profondeur.*
- *L'intégration du SI dans la gestion de la sureté.*
- *La gestion des identifiants.*
- *La maitrise des données du mapping.*
- *La gestion en multi site.*
- *La formation des utilisateurs.*
- *L'information des responsables sécurités.*

Nous avons toujours conseillé nos clients vers des solutions intégrant un haut niveau de sureté, en intégrant notamment des badges RFID basé sur la technologie Mifare® DESFire EV1 ou EV2 de NXP, ou l'utilisation de badge de technologie Legic® Advant et en utilisant des standards ouverts.

Dans ce contexte d'amélioration, nous appliquons les préconisations du document ANSSI « Guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques » et nous mettons en œuvre :

- *Le chiffrement entre le badge RFID et le lecteur via un algorithme AES128.*
- *L'utilisation du lecteur s'effectue dans un mode dit « Transparent », il ne contient aucune clé liée à la communication avec le badge.*
- *L'utilisation d'une SAM physique sur les équipements terrain (ITL/UED) nécessitant la connaissance de la clé de lecture du badge et des données sensibles.*
- *Une diversification de la clé de lecture des données sensibles via l'algorithme NXP AN-10922.*

2.3 Descriptions des fonctions d'accès

2.3.1 Identification RFID

Les badges d'accès peuvent avoir plusieurs origines :

- *Fourniture par Secure Systems & Services dans le cadre d'une prestation incluant la personnalisation des données d'un badge.*
- *Fourniture par le client final, dans le cadre de solution « corporate ».*
- *Fourniture par un fournisseur spécialisé (imprimerie nationale, …).*

2.3.2 Identification avec confirmation par PIN Code

Cette fonction est activable dans la solution et paramétrable. Les paramètres possibles sont la saisie du code pin ou la génération d'un code pin via un algorithme calculé.
Cette fonction permet la mise en place d'une solution d'authentification du porteur de badge en réalisant l'étape d'identification via le badge puis d'authentification via la saisie d'un code connu uniquement du porteur de badge.

2.4 Descriptions des hypothèses sur l'environnement du produit

La solution de sureté iPerflex est souvent intégrée au SI du client final. Elle hérite donc des protections mises en place par celui-ci. A savoir et de façon non exhaustive :

- *Un réseau dédié sureté non connecté au réseau « entreprise », ou connecté via un firewall/ passerelle/ sas informatique.*
- *Un contrôleur de domaine.*
- *Un annuaire centralisant les comptes utilisateurs.*
- *Une politique anti virale avec mise à jour automatique.*
- *Une politique de mise à jour des patchs de sécurités (Oracle, windows, java...).*
- *Une redondance des sources d'alimentations sont mise en œuvre. (Double alimentation ou onduleur).*

2.4.1 Hypothèses sur l'environnement physique du produit

Installation des serveurs

Les serveurs sont installés dans un local informatique sécurisé dont l'accès est strictement limité aux personnes habilitées.

Les serveurs disposent d'alimentations redondantes, de lien réseaux redondants, et si possible d'une architecture redondante (Virtualisée, cluster…)

Installation de la machine de programmation des SAM

Ce poste est installé dans un local sécurisé dont l'accès est strictement limité aux personnes habilitées. Il dispose d'un coffre permettant de séquestrer la carte SAM Master.

Installation des postes d'exploitations

Les postes d'exploitations sont installés dans des locaux sécurisés et nécessitent une connexion utilisateur en adéquation avec les missions confiées.

Installation des ITL/UED

Ces équipements sont installés en zone protégée, souvent dans un local technique sécurisé dont l'accès est strictement limité aux personnes habilitées.

La source d'alimentation est secourue (mise en place d'une batterie).

Installation des Lecteurs

Les lecteurs peuvent être positionnés en zone non protégé.

Côté raccordement, les câbles ne doivent pas être apparents.

2.4.2 Hypothèses sur les exploitants du produit

Les exploitants du produit sont des employés du client ou des mandataires autorisés de celui-ci.
Ils ont suivi une formation adaptée aux missions qu'ils doivent réaliser. Formations dispensées en interne ou auprès du constructeur Evolynx.
Ils disposent d'un compte opérateur en adéquation avec leur profil. Ce profil est personnalisable par l'administrateur. Ce profil regroupe la liste des actions autorisées, le profil géographique d'application de ces

actions, les niveaux d'alarmes, les niveaux opérateurs, la visibilité ou non des catégories de personnes, les formulaires de représentations des données adaptés à leurs droits d'en connaitre.

Ce compte est nominatif et dispose d'une politique de mot de passe en adéquation avec la politique de sécurité du client.

2.4.3 Hypothèses sur les usagers (porteurs de badges)

Les usagers correspondent aux employés, aux sous-traitants, aux visiteurs.
La solution Evolynx permet la mise en œuvre de badges de technologie sans contact pour ces différentes catégories de population.

Les technologies sans contact recommandées sont actuellement le Mifare ® Desfire EV1 ou EV2 ainsi que la technologie Legic® Advant.

En complément de l'identification du badge sans contact, il peut être ajouté la saisie d'un code pin attaché à l'usager. Ce code pin peut être choisi par l'usager, sous contrôle d'un exploitant habilité, ou généré par le système.

Nous supposons que des consignes ont été transmis aux usagers lors de la remise de leur badge afin de les sensibiliser aux bonnes pratiques et aux respects des règles de sécurité inhérentes aux sites du client. Parmi ces règles nous pouvons noter le caractère personnel du badge impliquant le non prêt de celui-ci à un tiers, la saisie d'un code d'accès sous contrainte, la notification aux responsables sécurité immédiatement lors du constat de la perte de celui-ci, le port du badge de façon apparente, de ne pas faire entrer une personne qui serait bloquée devant un accès, de respecter le badgeage sur les lecteurs y compris si plusieurs personnes se présentent sur une même porte, …

2.4.4 Hypothèses sur les agents technique (Maintenancier)

Les agents techniques sont des exploitants disposant d'un profil spécifique permettant pour certains la configuration / paramétrage des équipements terrains pour la mise en service, et pour d'autres l'accès aux états et commandes élémentaires dans le cadre d'opérations de maintenance.

Ils peuvent également accéder aux équipements terrains dans les locaux techniques ou au plus près des accès.

L'ensemble de leurs actions est tracé de façon identique aux exploitants « classique ». L'accès aux contrôleurs de terrain génère également une alarme et une trace sur l'interface.

Nous supposons que le produit est correctement configuré par les agents techniques.

2.4.5 Hypothèses sur l'environnement technique du produit

Les serveurs

Les Serveurs Evolynx fonctionnent sous un environnement de Microsoft® Windows Server, ils disposent des dernières mises à jour de sécurités, et d'un anti-virus à jour.

Les serveurs disposent de compte administrateur permettant les actions d'administration du Serveur, il existe également un compte exploitant doté de privilèges restreints à usage courant du système.

Les postes exploitants

Ces postes disposent de compte windows de type utilisateurs sans pouvoir avec une politique de mot de passe. Ces comptes sont des comptes de domaines centralisés. Ces comptes sont nominatifs.

Les réseaux

Les réseaux de contrôle d'accès sont a minima sur des VLAN différents du réseau entreprise. Idéalement ceux-ci sont sur des réseaux physiquement distinct.
Il est préconisé de mettre en œuvre (optionnel) le protocole 802.1X qui nécessite une authentification par certificat pour permettre la communication sur ce support (ajout d'un niveau de sécurité complémentaire sur le réseau).

Les contrôleurs ITL

Ces contrôleurs disposent d'un compte administrateur et d'un compte de maintenance par défaut. Ces comptes sont supposés avoir été modifié lors de la mise en service du système.
Le compte de maintenance peut être distinct par ITL. L'utilisation de cette connexion génère une alarme sur le système de supervision et nécessite une action manuelle sur la carte pour activer cette fonction.

Les certificats électroniques

Les certificats sont émis par le serveur PKI (voir § 2.1.11) déployé sur l'infrastructure du client final. Ils sont mis en œuvre en se conformant aux recommandations Evolynx.
Ces certificats concernent les échanges entre :
- la machine serveur d'application / frontal et le serveur radius
- la machine IHM et le serveur radius
- la carte ITL et le serveur radius
- l'applicatif IHM et l'applicatif serveur d'application
- l'applicatif frontal et l'applicatif ITL (deux canaux de communications)
- l'applicatif Evolynx-security et l'applicatif ITL

Les badges sans contacts

Les badges de technologie sans contact sont encodés soit par nos soins soit par un mandataire tiers.
Ils doivent à minima respecter les contraintes suivantes :

- *Modification de la clé PICC MASTER par défaut, passage de celle-ci en AES128.*
- *Authentification nécessaire à la création d'une application.*
- *Authentification nécessaire au formatage, à la liste des applications.*
- *Utilisation de clés diversifiées (dans le respect de l'algorithme NXP AN-10922).*
- *Taille de l'identifiant compris entre 4 et 16 octets.*
- *Utilisation de la gestion des versions de clés.*
- *Modification des valeurs par défauts.*
- *Utilisation d'une clé de lecture de l'identifiant, cette clé n'est pas utilisée dans une autre configuration.*
- *Les données enregistrées sont en mode chiffré/signé. Aucune donnée n'est en mode « Plain ».*

Les Lecteurs de badge

Les lecteurs doivent disposer de la fonctionnalité permettant une communication en mode transparent. Ils permettent à l'ITL ou l'UED de communiquer directement avec le badge. Les données échangées sont chiffrées en AES128 entre nos contrôleurs et le badge.

Les lecteurs de badges qui sont mis en œuvre dans la cible de sécurité sont les suivants :

- *ARCW33APH57AD1 (lecteur simple)*
- *ARCW33BPH57AD1 (lecteur + clavier physique)*
- *ARCW33CPH57AD1 (lecteur + clavier tactile sur afficheur)*

Ils disposent tous du même protocole SSCPv2.

2.5 Description des usagers (utilisateurs types)

2.5.1 Exploitants

L'exploitant est un utilisateur de la solution Evolynx. En fonction de ses missions, il pourra soit :

- *Configurer le système.*
- *Attribuer des droits, gérer la validité des personnes, prolonger ou suspendre des droits affectés.*
- *Prêter/rendre des badges, déclarer perdu/ retrouvé des badges.*
- *Interdire une personne.*
- *Surveiller une personne.*
- *Créer, modifier, supprimer des fiches personnelles.*
- *Créer des badges, encoder ceux-ci.*
- *Superviser le système au travers du bandeau des alarmes, des mouvements et des synoptiques.*
- *Commander des ouvertures de porte à distance.*
- *Valider via une authentification visuelle les accès à certains locaux.*
- *Accueillir des visiteurs.*
- *Valider des demandes de visites.*
- *…*

Toute action des exploitants est tracée dans le système dans l'historique des événements en associant le login, ainsi que le poste utilisé. Parmi ces événements générés nous avons la capacité de tracer sa connexion, ses échecs de connexion, y compris la consultation des fiches personnelles, ainsi que l'ensemble des créations, modifications, suppression sur le système. Dans les fiches personnelles une information d'identification de l'exploitant est disponible pour les actions de création et de modification permettant ainsi de savoir qui a créé cette fiche et quel est le dernier exploitant qui a modifié celle-ci.
Les exploitants sont supposés être compétents, formés et de confiance.

2.5.2 Agents techniques

Les agents techniques sont des personnes intervenant dans le cadre de la mise en service ou dans le cadre d'opération de maintenance préventive ou corrective.
Les agents techniques sont des exploitants disposant de profils spécifiques. Leurs actions sont tracées de la même façon que les exploitants.
Ils disposent d'une formation complémentaire sur les contrôleurs et leurs mises en œuvre.

2.5.3 Usagers

Ils représentent la population la plus importante du système.
Les usagers sont les utilisateurs des accès physiques de la solution Evolynx. Pour accéder aux zones protégées, ils disposent d'un badge sans contact ainsi que d'un code pin. Ils peuvent également utiliser des solutions d'authentification biométrique.

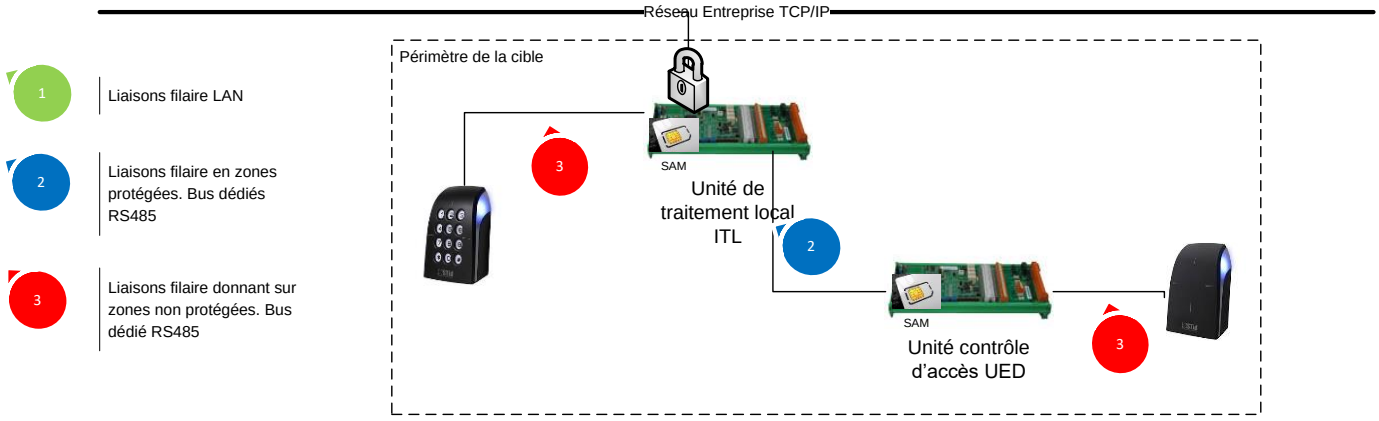
Les usagers sont regroupés au sein de catégorie :

- *Les employés ou résidents.*
- *Les employés « corporates » mais non-résidents.*
- *Les sous-traitants ou externes.*
- *Les stagiaires, intérimaires.*
- *Les visiteurs, les visiteurs VIP.*
- *…*

2.6 Description du périmètre d'évaluation

La cible de sécurité prévoit l'évaluation de la sécurité des fonctions de contrôle d'accès des équipements suivants :

- *Le contrôleur Maître ITL.*
- *Le contrôleur Esclave UED.*
- *Les lecteurs de proximité et les lecteurs/ clavier.*



3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

Les équipements suivants ou leurs simulations via une boite à bouton / affichage de leds sont nécessaires à l'évaluation.

3.1 Dispositif d'accès

Gestion d'environnement d'accès disposant des éléments à minima :

- *Détecteur d'ouverture (contact position porte).*
- *Bouton poussoir d'ouverture (commande en sortie).*
- *Contact sec de passage effectif délivré par l'obstacle physique.*
- *Organe de serrurerie condamnant l'accès (commande par contact sec et alimentation secourue).*

3.2 Dispositifs de raccordements et d'alimentation

- *Un switch disposant du 802.1X (optionnel)*
- *Câble réseaux cat 5 10/100 BASE-T*
- *Liaison bus RS485 entre :*
  - *ITL / UED*
  - *ITL / Lecteur Clavier*
  - *UED / Lecteur proximité*
- *Alimentation de l'ensemble des équipements ITL/ UED/ Lecteurs via l'alimentation de l'ITL. Cette alimentation dispose d'une batterie.*

3.3 Postes informatiques

- Serveurs en windows 2012 incluant les derniers correctifs,
- Une machine virtuelle avec FreeRadius pour la mise en œuvre du 802.1X (optionnel)
- Poste d'exploitation en windows 7 ou windows 10 incluant les derniers correctifs.

3.4 Badges

Les badges sont de technologies Mifare ® Desfire EV1.
Ils sont encodés à partir de la solution Evolynx évaluée.
Ils correspondent aux niveaux III du tableau 2 du document de référence [Doc1] §4.1.1 « Badges : niveaux de sureté, résistance aux attaques logiques ».

3.5 Secure Access Module (SAM)

Des cartes NXP SAM AV2, correctement encodées.
L'encodage est réalisé à partir de la solution Evolynx évaluée.

4 DONNEES NEVRALGIQUES & SENSIBLES

Les mécanismes cryptographiques utilisés dans le cadre de l'évaluation CSPN sont décrits dans le document [Doc3].

4.1 Descriptions

Les données névralgiques sont :

- Les données liées au badge :
  - La ou Les clés de lecture Mifare ® Desfire EV1 de l'identifiant du badge
  - Les données du mapping du badge (AID Desfire, N° de fichier, taille de l'identifiant)

- Les données liées à la sécurisation des communications entre les constituants :
  - La ou les clés d'authentification d'accès à la SAM.
  - Les clés d'authentification d'accès aux lecteurs lors des échanges non transparent (pour la gestion du code pin…).
  - Les certificats intervenants dans les échanges ITL/Frontal, Frontal/ ITL.
  - Les certificats intervenants dans les échanges ITL/ serveur Radius (optionnel).

Les données sensibles sont :

- Les identifiants contenus dans le badge des usagers.
- Les codes PIN associés.
- Les droits d'accès des usagers présent dans le contrôleur ITL.

4.2 Répartition des biens sensibles sur les éléments constitutifs de la TOE

Biens	Contrôleur ITL	Contrôleur UED	Lecteur
B1 : La clé de lecture de l'identifiant du badge	X[1]	X[1]	
B2 : Clé d'authentification SAM	X	X	
B3 : Clé mère de communication ITL-UED	X[1]	X[1]	
B4 : Clé mère de communication entre le lecteur et le contrôleur (protocole SSCPv2)	X[1]	X[1]	X
B5 : données de mapping du badge	X	X	
B6 : Certificats	X		
B7 : identifiant du badge	X		
B8 : Code PIN	X		
B9 : Droits d'accès	X		

1 : ces clés sont stockées dans un module SAM.

4.3 Protection des biens sensibles

Le tableau suivant présente les protections apportées sur les biens sensibles. La mention « CA » signifie que le bien est protégé par un mécanisme de contrôle d'accès. La mention « X » signifie que le bien est protégé par un mécanisme cryptographique.

Biens	Confidentialité	Intégrité	Authenticité
B1 : La clé de lecture de l'identifiant du badge	X	X	
B2 : Clé d'authentification SAM	X	X	
B3 : Clé mère de communication ITL-UED	X	X	
B4 : Clé mère de communication entre le lecteur et le contrôleur (protocole SSCPv2)	X	X	
B5 : données de mapping du badge	CA	CA	
B6 : Certificats	CA	CA	
B7 : identifiant du badge	X	X	
B8 : Code PIN	X	X	
B9 : Droits d'accès	CA	CA	

Le tableau suivant présente les mécanismes cryptographiques utilisés pour chaque fonction de sécurité :

Fonctions de sécurité	Mécanismes cryptographiques
P1 : Protection des données échangées entre le serveur et le contrôleur ITL	Protocole TLS : Génération d'aléa, cryptographie sur courbe elliptique, chiffrement intègre, fonction de hachage, code d'authentification de message.
P2 : Protection des données échangées entre le contrôleur ITL et le contrôleur UED	Génération d'aléa, chiffrement symétrique, fonction de hachage, code d'authentification de message.
P3 : Protection en transmission du code PIN	Protocole SSCPv2 : génération d'aléa, chiffrement symétrique, fonction de hachage, code d'authentification de message.
P4 : Sécurisation du contrôleur ITL	
P5 : Sécurisation du contrôleur UED	
P6 : Sécurisation du lecteur / lecteur clavier	Protocole SSCPv2 : génération d'aléa, chiffrement symétrique, fonction de hachage, code d'authentification de message.

5 DESCRIPTION DES MENACES

5.1 Agents menaçants

Les agents menaçants peuvent commettre les différentes attaques logiques suivantes :

- Attaque sur le réseau TCP/IP établi entre le serveur de communication et le contrôleur ITL.
- Attaque sur le réseau dédié RS485 entre le contrôleur ITL et le contrôleur UED.
- Attaque externe sur le réseau dédié RS485 entre le lecteur ou le lecteur clavier et le contrôleur (ITL ou UED).

Les agents menaçants peuvent commettre les différentes attaques physiques suivantes :

- Attaque sur le contrôleur ITL.
- Attaque sur le contrôleur UED.
- Attaque sur le bus ITL ou UED.
- Attaque sur un lecteur de proximité ou lecteur clavier.

Nous ne prenons pas en compte les attaques sur la base de données, le serveur d'application, les postes d'exploitations, les serveurs. Ces attaques doivent être prises en compte dans le cadre d'une homologation du SI complet de la solution de sureté.

5.2 Intrusion externe

Cette intrusion concerne le réseau LAN TCP/IP du client. Repère (1) sur le schéma d'architecture.
L'objectif de cette intrusion est d'intercepter des données sensibles, d'injecter des données voire envoyer des commandes.
L'attaquant est connecté sur le réseau.

Ecoute transactions	Menaces
Ecoute d'une transaction contenant l'ID	M1 : Copie de badge
Ecoute d'une transaction contenant les données du mapping (AID, n° de fichier)	M2 : Copie de badge
Ecoute d'une transaction contenant le code pin	M3 : Usurpation d'identité
Ecoute d'une transaction contenant les droits d'accès	M4 : Modifier des droits
Ecoute d'une transaction contenant les plage horaires	M5 : Elargir les plages d'accès
Ecoute d'une transaction contenant la validité du droit	M6 : Elargir la validité du droit
Ecoute d'une transaction contenant un événement d'accès	M7 : Modifier la traçabilité des événements du terrain
Ecoute d'une transaction contenant une alarme	M8 : Modifier la traçabilité des alarmes du terrain
Ecoute d'une transaction contenant une commande d'ouverture à distance	M9 : Tenter le rejeu
Ecoute d'une transaction avec le Frontal	M10 : Emuler un contrôleur ITL, se substituer à un contrôleur existant.
Ecoute d'une transaction contenant la mise à jour du firmware logiciel	M11 : Tentative d'injection d'un code en lieu et place du firmware ITL
Ecoute d'une transaction contenant la mise à jour de la clé de lecture du badge	M12 : Copie de badge

5.3 Intrusion sur les réseaux dédiés

Cette intrusion concerne les bus de communication RS485 entre le contrôleur ITL et UED. Repère (2) sur le schéma d'architecture.
L'objectif de cette attaque est d'intercepter les données sensibles ainsi que d'injecter des données, rejouer des commandes.

Ecoute transactions	Menaces
Ecoute d'une transaction contenant l'ID	M13 : Copie de badge
Ecoute d'une transaction contenant les données du mapping (AID, n° de fichier)	M14 : Copie de badge
Ecoute d'une transaction contenant le code pin	M15 : Usurpation d'identité
Ecoute d'une transaction contenant un événement d'accès	M16 : Modifier la traçabilité des événements
Ecoute d'une transaction contenant une alarme	M17 : Modifier la traçabilité des alarmes
Ecoute d'une transaction contenant une commande d'ouverture à distance	M18 : Tenter le rejeu
Ecoute d'une transaction avec le contrôleur ITL	M19 : Emuler un contrôleur ITL
Ecoute d'une transaction contenant la mise à jour de la clé de lecture du badge	M20 : Copie de badge
Ecoute d'une transaction contenant la mise à jour du firmware logiciel	M21 : Tentative d'injection d'un code en lieu et place du firmware UED
Ecoute d'une transaction entre l'ITL et l'UED	M22 : Tentative d'envoi d'ordre d'ouverture d'accès à l'UED
Ecoute d'une transaction entre l'ITL et le lecteur ou l'UED et le lecteur	M23 : Tentative d'usurpation d'un code PIN

5.4 Attaque sur ITL

L'objectif de cette attaque est de réaliser la substitution d'un contrôleur ITL, d'obtenir des informations via des tentatives de cryptanalyse et de lecture du code exécutable (M24).

5.5 Attaque sur UED

L'objectif de cette attaque est de réaliser la substitution d'un contrôleur UED, d'obtenir des informations via des tentatives de cryptanalyse et de lecture du code exécutable (M25).

5.6 Attaque sur lecteur ou lecteur-clavier

L'objectif de cette attaque est de réaliser la substitution/remplacement d'un lecteur, émulation de celui-ci (M26).

6 DESCRIPTION DES FONCTIONS DE SECURITE

6.1 Protections mises en œuvres

P1 : Protection des données échangées entre le serveur et le contrôleur ITL
Cette protection est réalisée au travers de plusieurs moyen :

- Une Authentification du contrôleur ITL sur le réseau TCP/IP au travers de l'utilisation du protocole EAP-TLS
- L'établissement d'un canal de communication chiffré entre le serveur de communication et le contrôleur ITL, avec une session avec authentification mutuelle au préalable.
  Les données échangées sont protégées en confidentialité et en intégrité (emploi du protocole https utilisant TLS 1.2 ; voir [Doc3] pour le détail des cipher suites utilisées, des algorithmes impliqués dans l'échange des clés, le chiffrement et la signature des données ainsi que la taille des clés mises en œuvre).

P2 : Protection des données échangées entre le contrôleur ITL et le contrôleur UED
Cette protection est réalisée par l'établissement d'un canal de communication chiffré/signé entre les deux contrôleurs qui ont au préalable établi une session avec authentification mutuelle.
Les données échangées sont protégées en confidentialité.
Les tentatives de rejeu sont protégées par la mise en œuvre d'un compteur de trame.

P3 : Protection en transmission du code PIN
Les codes pin saisies sur le lecteur clavier le sont dans la démarche construite suivante :

- Passage d'un badge sur le lecteur (le clavier est inopérant).
- Vérification des droits d'accès autorisé pour ce badge par le contrôleur ITL.
- Demande de saisi du code clavier (activation du code clavier).
- Saisie du code pin.
- Transmission en liaison chiffrée/signée AES128 entre le clavier et le contrôleur des informations saisies.

Les données sont téléchargées depuis les serveurs jusqu'aux contrôleurs ITL en mode chiffré.

P4 : Sécurisation du contrôleur ITL
Le contrôleur est placé en zone protégée.
La détection des défauts génère des alarmes techniques vers le serveur.
Ces défauts sont :

- Autoprotection coffret (Ouverture coffret).
- Défaut communication ITL/Frontal et Défaut communication Frontal/ITL (ce défaut est analysé par le frontal).
- Saturation réseau.
- Utilisation serveur web local.
- Défaut communication UED.
- Défaut alimentation.
- Absence/retrait carte SAM.

P5 : Sécurisation du contrôleur UED
Le contrôleur est placé en zone protégée.
La détection des défauts génère des alarmes techniques vers le serveur.
Ces défauts sont :

- Autoprotection coffret (Ouverture coffret).
- Absence/retrait carte SAM.

P6 : Sécurisation du lecteur / Lecteur clavier
La détection des défauts génère des alarmes techniques vers le serveur.
Ces défauts sont :

- Autoprotection (contact gyroscopique).
- Défaut communication lecteur.

La communication entre le lecteur et les contrôleurs s'effectue avec une authentification mutuelle à la mise sous tension.
Les clés sont modifiées en usine chez Evolynx.

6.2 Traçabilité entre les fonctions de sécurité et les menaces

	M1 à M12	M13 à M22	M23	M24	M25	M26
P1	X					
P2		X				
P3			X			
P4				X		
P5					X	
P6						X

