Cible de sécurité evolynx^{NG}

Validation du Document

REV	REDACTEUR	VERIFICATEUR	APPROBATEUR	DATE D'APPLICATION
A	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	07/04/2022
B	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	31/08/2022
C	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	21/09/2022
D	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	25/09/2023
E	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	25/01/2024
F	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	05/11/2024
G	O.BERTHET-RAYNE	A.DA SILVA	F.ROBEYN	30/07/2025

Historique des modifications

REV	PAGE	CHAPITRE	OBJET DE LA MODIFICATION
A	Tout	Tout	Première émission – document de travail
B			Mises à jour référence et versions des sous systèmes
C	30,31,33,37		Prise en compte des remarques d'Oppida sur firmware ITL/UED
D			Mises à jour suite au rapport d'évaluation Oppida
E			Mises à jour référence et versions des sous systèmes
F			Mises à jour suite au rapport d'évaluation Oppida
G			Version diffusable

Référence documentaire

REF	DOCUMENT	REVISION	DATE
[Doc1]	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection – v2.0	2.0	04/03/2020
[Doc2]	anssi-cspn-note-07-methodologie-pour-evaluation-cspn-contrôle-d_acces_v2.1.pdf	2.1	13/02/2025
[Doc3]	Evolynx–-NT-FR - Mécanismes cryptographiques	F	05/11/2024
[Doc4]	Architecture cible de sécurité Evolynx iPerflex	D	28/01/2020

TABLE DES MATIERES

1 PRESENTATION

1.1 OBJECTIF

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

La solution dispose d'un CSPN Evolynx-ITL 2020-39 en date du 25/11/2020, dont la cible est définie dans [Doc4] ; l'objet de ce document est de définir une cible plus étendue en intégrant la partie serveur (GAC) ainsi que les nouvelles générations d'automate terrain.

1.2 IDENTIFICATION DU PRODUIT

Nom du produit	evolynx^{NG}
Constructeur	Secure Systems & Services
Site web	https://www.secure-systems.fr
Version supervision	evolynx^{NG} 2024.2
Version firmware ITL/UED	8.3.2a

2 ARGUMENTAIRE DU PRODUIT

2.1 DESCRIPTION GENERALE DU PRODUIT

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

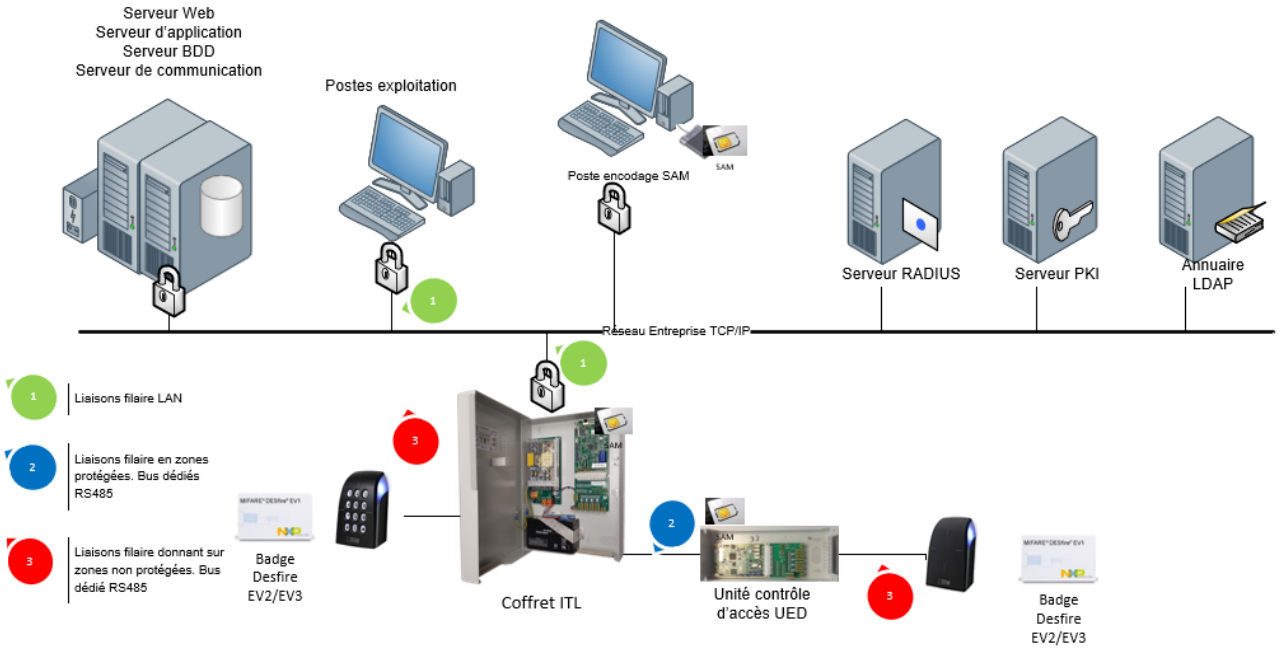
La solution est composée d'un GAC et d'équipements de terrains.

Le GAC se compose des sous-ensembles suivants :
- Serveur de base de données,
- Serveur web
- Serveur d'application
- Frontal de communication

Les équipements de terrains sont constitués de :
- Une ITL32 (UTL dans la référence ...),
- Une UED (unité de contrôle d'accès),
- Lecteurs de badges Stid Desfire (référence ARC-W33*x* /PH5-7AD),
- Badges Desfire EV2/EV3

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^{NG}** 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^{NG} *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^{NG},** *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^{NG} 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 ELEMENTS CONSTITUANT LA SOLUTION

- Le serveur de gestion des accès (GAC), comprenant les briques fonctionnelles base de données centralisée, serveur d'application, serveur web et frontal de communication.
- La station de programmation des SAM.
- Les postes (client léger) d'exploitation.
- 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 EV2/EV3

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 DONNEES

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 SERVEUR WEB

Rôle : Le serveur web assure :

- *Le point d'entrée des clients IHM,*
- *La mise en forme des informations du serveur d'application sur la couche de représentation,*
- *Les fonctions de proxy pour accéder au serveur d'application depuis une requête d'un client web,*

2.1.6 POSTE D'EXPLOITATION

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

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.

	Le poste client est supposé de confiance.

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…).*

Sur certains postes, il est possible d'utiliser des lecteurs de table. Ces lecteurs ont pour but l'encodage et l'enrôlement des badges. Dans ce cas le poste est équipé d'un logiciel qui communique avec le lecteur de table de puce à insertion connecté en PCSC. Ce lecteur contient une SAM « encodage » qui contient les clés de lecture/écriture des badges.

Il n'existe qu'une seule interface pour réaliser l'ensemble des fonctions accessibles dans notre solution, y compris le paramétrage des équipements terrain. Les fonctionnalités peuvent toutefois être cloisonnées par la mise en œuvre des profils utilisateurs.

2.1.7 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'evolynx^{NG} 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.*

2.1.8 EQUIPEMENTS DE TERRAIN

2.1.8.1 CONCENTRATEUR D'ACCES 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.*

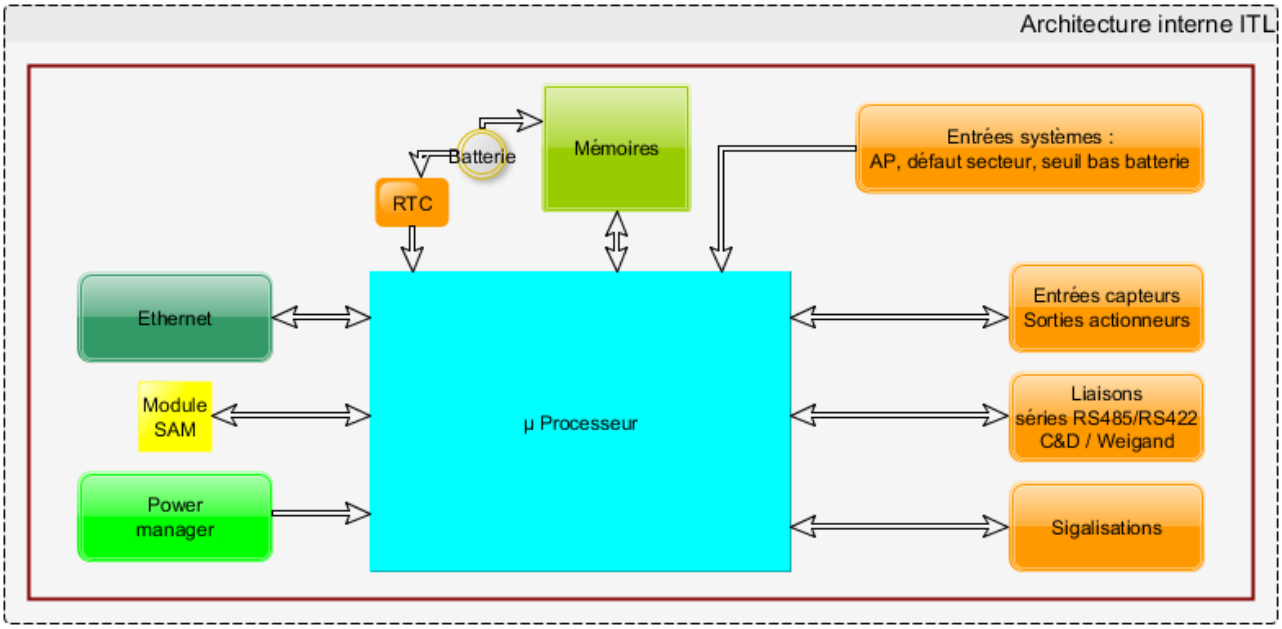
Elle contrôle la validité des badges, stocke les évènements et les mouvements, les horodate et les transmet au superviseur. L'ITL possède une intelligence locale et peut fonctionner de manière autonome en mode dégradé.

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 AV3 externe.



Composant	Description
Désignation	ITL
Référence produit	M20102C
Version logicielle	V8.3.2a
Mémoires	Flash NOR/ Flash NAND

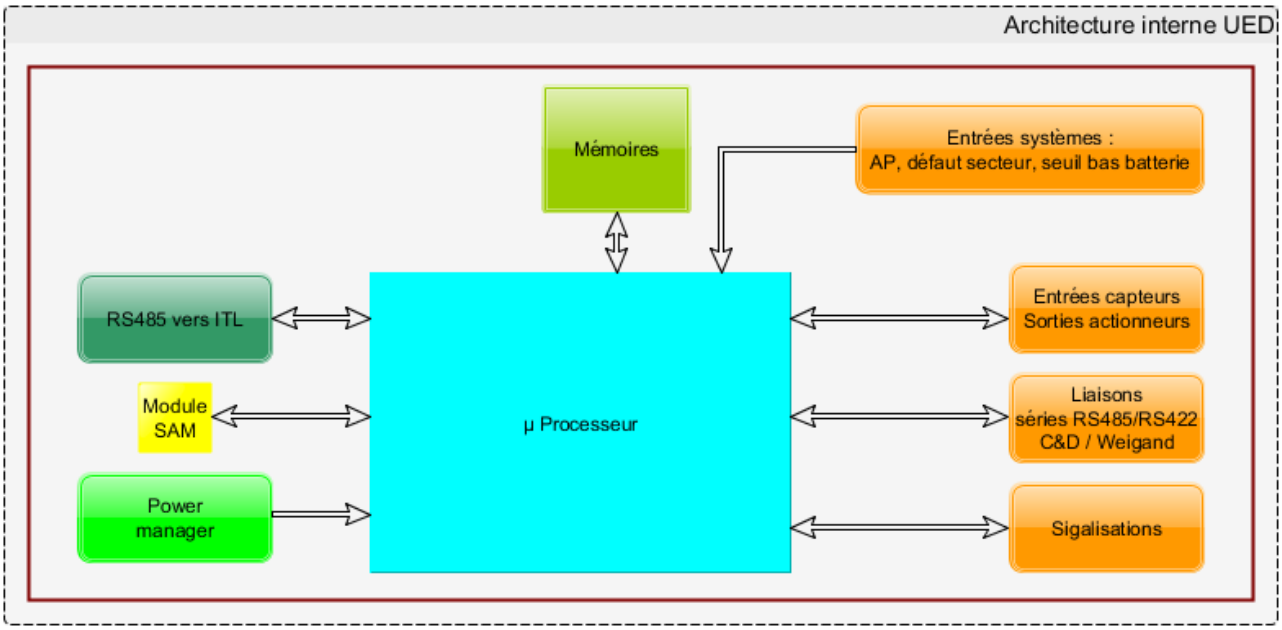
2.1.8.2 UNITE DE CONTROLE D'ACCES UED

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 AV3 externe.



Composant	Description
Désignation	UED
Référence produit	M20122C
Version logicielle	V8.3.2a
Mémoires	Flash NOR/ Flash NAND

2.1.9 RESEAUX 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.

2.1.10 RESEAUX DEDIES

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.

2.1.11 SERVEUR ANNUAIRE DES UTILISATEURS

Le serveur annuaire a pour rôle l'authentification des utilisateurs qui se connectent à l'application. Il est fourni par l'infrastructure informatique du client. Le serveur d'application evolynx^{NG} communique avec le serveur annuaire au travers du protocole LDAPS. Dans le contexte de cette évaluation, il s'agit d'un serveur Active Directory.
Le serveur annuaire contient la liste des utilisateurs du système ainsi que leurs mots de passe. Il gère totalement la politique de mots de passe, leur renouvellement. Les profils utilisateurs sont quant à eux gérés entièrement dans notre application.

	Le serveur annuaire est supposé de confiance.

2.1.12 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.

	Le serveur Radius est supposé de confiance.

2.1.13 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
TLS1.3	Serveur d'application	Serveur Web	JKS
TLS1.3	Serveur web	IHM	X.509
LDAPS	Serveur annuaire	Serveur d'application	X.509
EAP-TLS	Serveur d'application	Serveur Radius (optionnel)	X.509
TLS1.2	Base de données	Serveur d'application	PKCS#12
EAP-TLS	IHM	Serveur Radius (optionnel)	X.509
EAP-TLS	Frontal de communication	Serveur Radius (optionnel)	X.509
EAP-TLS	ITL	Serveur Radius (optionnel)	X.509
TLS1.3	ITL	Frontal de communication	PKCS#12
TLS1.3	Frontal de communication	ITL	PKCS#12
TLS1.3	Poste de programmation des SAM	ITL	PKCS#12
TLS1.3	ITL	Poste de programmation des SAM	PKCS#12

Dans le contexte de cette cible de sécurité, le serveur de PKI est supposé de confiance.

2.1.14 POSTE DE PROGRAMMATION DES SAM

Ce poste permet la programmation des SAM NXP AV3 au travers d'un logiciel client lourd.
Ce logiciel communique avec deux lecteurs de table de puce à insertion connectés 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.*

	Dans le contexte de cette cible de sécurité, le poste de programmation est supposé de confiance.

2.1.15 LECTEUR DE PROXIMITE

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 EV2 ou EV3 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.*
- *L'utilisation d'une SAM physique sur les équipements lecteur de table nécessitant la connaissance des clés de lecture et d'écriture du badge et des données sensibles.*
- *Une diversification des clés de lecture et d'écriture des données sensibles via l'algorithme NXP AN-10922.*

2.3 DESCRIPTIONS DES FONCTIONS D'ACCES

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 HYPOTHESES SUR L'ENVIRONNEMENT DU PRODUIT

La solution de sureté evolynx^{NG} 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 HYPOTHESES 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 postes d'encodage et enrôlement

Les postes d'encodage et d'enrôlement sont installés dans des locaux sécurisés dont l'accès est strictement limité aux personnes habilitées et nécessitent une connexion utilisateur en adéquation avec les missions confiées. Ces postes sont équipés de lecteurs de table intégrant une SAM « Encodage ».

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 HYPOTHESES 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 Secure Systems & Services.
Ils disposent d'un compte opérateur en adéquation avec leur profil. Ce profil est personnalisable par l'administrateur, qui est lui-même un exploitant disposant des privilèges maximums. 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.

Le ou les officiers de sécurité sont des exploitants avec un haut niveau de privilège. En particulier, ils sont les seuls habilités à enregistrer les informations névralgiques comme les clés de chiffrement des badges Desfire.

2.4.3 HYPOTHESES SUR LES USAGERS (PORTEURS DE BADGES)

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

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 transmises aux usagers lors de la remise de leur badge afin de les sensibiliser aux bonnes pratiques et au respect 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 HYPOTHESES SUR LES AGENTS TECHNIQUES (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 « classiques ». 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 HYPOTHESES SUR L'ENVIRONNEMENT TECHNIQUE DU PRODUIT

Les serveurs

Les Serveurs evolynx[NG] fonctionnent sous un environnement Microsoft® Windows Server, ils disposent des dernières mises à jour de sécurité, 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 à minima sur des VLAN différents du réseau entreprise. Idéalement ceux-ci sont sur des réseaux physiquement distincts.
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 modifiés 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 § 2.1.13) déployé sur l'infrastructure du client final. Ils sont mis en œuvre en se conformant aux recommandations evolynx[NG].
Ces certificats concernent les échanges entre :
- la machine serveur d'application / frontal et le serveur radius (optionnel)
- la machine serveur d'application et le serveur d'annuaire
- la machine IHM et le serveur radius (optionnel)
- la carte ITL et le serveur radius (optionnel)
- l'applicatif IHM et le serveur web
- l'applicatif serveur web et le serveur d'application
- l'applicatif base de données et le serveur d'application
- l'applicatif frontal et l'applicatif ITL (deux canaux de communications)
- l'applicatif Evolynx-securityManager et l'applicatif ITL

Les badges sans contact

Les badges de technologie sans contact sont encodés soit par la solution evolynx[NG] 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.

Les lecteurs de table

Les lecteurs de table sont équipés d'une SAM permettant de les utiliser en mode transparent, en protocole PCSC. La communication avec le badge est chiffrée en AES128.

Le lecteur de table mis en œuvre dans la cible de sécurité est le suivant :

- *uTrust 4701 F*

2.5 DESCRIPTION DES USAGERS (UTILISATEURS TYPES)

2.5.1 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.

2.5.2 EXPLOITANTS

L'exploitant est un utilisateur de la solution evolynx^{NG}. 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.

2.5.3 OFFICIER DE SECURITE

L'officier de sécurité est un exploitant à haut niveau de privilège. Son profil lui permet notamment de :

- *Créer la carte SAM Maître et y enregistrer les clés de chiffrement Desfire, lors de la cérémonie de remise des clés. Pour plus de sécurité, cette cérémonie est réalisée par deux officiers de sécurité ne connaissant qu'une partie des clés chacun.*

2.5.4 USAGERS

Ils représentent la population la plus importante du système.
Les usagers sont les utilisateurs des accès physiques de la solution evolynx^{NG}. 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 PERIMETRE D'EVALUATION

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

Composant du système			Inclus dans la cible de l'évaluation	Non évalué	
				Supposé de confiance	Est un attaquant potentiel
GAC	Système d'exploitation	Windows Server 2022		X	
	Applicatifs	Serveur Apache Serveur Wildfly Evolynx^{NG} application serveur Frontal de communication	X X X X		
	Base de données	Oracle	X		
	Fonctions cryptographique	Openssl OpenJDK	X X		
	Base de données annuaires	Active Directory		X	
	Serveur Radius	FreeRadius		X	
	Certificats			X	
ITL	Système d'exploitation	Linux microship basé sur la branche officielle	X		
	Applicatifs	Firmware Appweb	X X		
	Fonctions cryptographiques	Openssl MbedTLS Librairies AES, SHA, HMAC soft Dialogue ITL/UED	X X X X		
	SAM	SAM NXP AV3		X	
	Certificats			X	
UED	Système d'exploitation	Linux microship basé sur la branche officielle	X		
	Applicatifs	Firmware	X		
	Fonctions cryptographique	Openssl Librairies AES, SHA, HMAC soft Dialogue ITL/UED	X X X		

	SAM	SAM NXP AV3		X	
Lecteurs	Lecteurs simples	*ARCW33APH57AD1*	*X*		
	Lecteurs clavier	*ARCW33BPH57AD1* *ARCW33CPH57AD1*	*X*		
Badges		Desfire EV2/EV3		X	

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'ACCES

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 2022 incluant les derniers correctifs,*
- *Une machine virtuelle avec FreeRadius pour la mise en œuvre du 802.1X (optionnel)*
- *Poste d'exploitation en windows 11 incluant les derniers correctifs.*

3.4 BADGES

Les badges sont de technologies Mifare ® Desfire EV2/EV3.
Ils sont encodés à partir de la solution evolynxNG 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 AV3, correctement encodées.
L'encodage est réalisé à partir de la solution evolynxNG 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 EV2/EV3 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 données sensibles sont :

- Les identifiants contenus dans le badge des usagers.
- Les codes PIN associés.
- Les droits d'accès des usagers présents dans le contrôleur ITL.
- Le couple login/mot de passe des exploitants (lors de l'interaction avec le serveur d'annuaire)
- Les profils des exploitants et leurs droits associés
- La clé secrète utilisée pour le chiffrement AES sur le serveur d'application et le frontal.
- Les informations sensibles (mots de passe) enregistrées en base de données ou dans les fichiers de paramétrage des sous-systèmes
- Les firmwares ITL et UED
- Les logs applicatifs des utilisateurs / usagers

4.2 REPARTITION DES BIENS SENSIBLES SUR LES ELEMENTS CONSTITUTIFS DE LA TOE

Biens	GAC	Contrôleur ITL	Contrôleur UED	Lecteur
B1 : 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	X	
B6 : identifiant du badge	X	X		
B7 : code PIN	X	X		
B8 : droits d'accès de l'usager	X	X		
B9 : couple login/mot de passe de l'exploitant	X			

B10 : profil des exploitants	X			
B11 : clé secrète pour le chiffrement AES	X			
B12 : informations sensibles (mots de passe)	X	X		
B13 : firmwares ITL et UED	X	X	X	
B14 : logs applicatifs des utilisateurs / usagers	X	X[2]		

1 : ces clés sont stockées dans un module SAM.
2 : mode dégradé, conservation des x derniers événements/mouvements (x paramétrable)

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	Disponibilité	Authenticité
B1 : clé de lecture de l'identifiant du badge	X	X		X
B2 : clé d'authentification SAM	X	X		X
B3 : clé mère de communication ITL-UED	X	X		X
B4 : clé mère de communication entre le lecteur et le contrôleur (protocole SSCPv2)	X	X		X
B5 : données de mapping du badge	CA	CA		
B6 : identifiant du badge	X	X		X
B7 : Code PIN	X	X		X
B8 : Droits d'accès usager	CA	CA		
B9 : couple login/mot de passe de l'exploitant	X	X		X
B10 : profil des exploitants	CA	CA		
B11 : clé secrète pour le chiffrement AES	X	X		X
B12 : informations sensibles (mots de passe)	X	X		X
B13 : firmwares ITL et UED	X	X		X
B14 : logs applicatifs des utilisateurs / usagers	CA	CA	CA	

Le tableau suivant présente les mécanismes cryptographiques utilisés pour chaque fonction de sécurité définie au paragraphe 6.1 :

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.
P6 : Sécurisation du lecteur / lecteur clavier	Protocole SSCPv2 : génération d'aléa, chiffrement symétrique, fonction de hachage, code d'authentification de message.
P7 : Protection des données échangées entre le	Protocole TLS : Génération d'aléa, cryptographie

poste opérateur et le serveur d'application	sur courbe elliptique, chiffrement intègre, fonction de hachage, code d'authentification de message.
P8 : Protection des données échangées entre la base de données et les applications	Génération d'aléa, chiffrement symétrique, fonction de hachage, code d'authentification de message.
P9 : Protection des connexions opérateurs	Protocole LDAPS : génération d'aléa, cryptographie sur courbe elliptique, chiffrement intègre, fonction de hachage, code d'authentification de message.
P11 : Protection des données sensibles stockées dans la base de données	Génération d'aléa, chiffrement symétrique, fonction de hachage
P12 : Protection du mot de passe d'accès à la base de données Oracle	Génération d'aléa, chiffrement symétrique, fonction de hachage
P13 : Protection de l'intégrité des firmwares ITL/UED	Chiffrement et signature des firmwares
P14 : Protection du démarrage des ITL/UED ainsi que de l'intégrité des flash	Mise en œuvre du mécanisme de secureBoot pour établir une chaine de confiance depuis le bootstrap jausqu'au rootfs par chiffrement et signature des différents éléments.

5 DESCRIPTION DES MENACES

5.1 AGENTS MENAÇANTS

Les agents menaçants peuvent être des usagers ou tout utilisateur du réseau sureté. Les exploitants et les agents techniques sont quant à eux réputés de confiance.

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).
- Attaque sur le serveur applicatif au travers de vulnérabilités exploitables,
- Attaque sur la base de données au travers de vulnérabilités exploitables,
- Attaque sur le mécanisme d'authentification des exploitants,
- Attaque par téléchargement de firmwares ITL/UED corrompus

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.

Ne sont pas pris en compte les attaques sur la technologie du Badge. Les postes informatiques sont censés être à jour de toute vulnérabilité connue à la date de l'évaluation.

Le GAC est considéré dans un local protégé de toute attaque physique.

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
Ecoute d'une transaction entre le poste opérateur et le serveur d'application	M13 : Tentative de saturation de l'historique de l'application
Ecoute d'une transaction entre le serveur d'application et la base de données	M14 : Modifier/supprimer la traçabilité des événements
Ecoute d'une transaction de connexion à l'application	M15 : Tentative d'usurpation d'identité
Ecoute d'une transaction d'utilisation de l'application	M16 : Tentative d'élévation de privilège sur les accès utilisateurs
Ecoute d'une transaction contenant des données de biens sensibles du GAC	M17 : Modifier les données sensibles du GAC
Récupération du mot de passe d'accès à la base de données	M18 : Tentative de modification des données de configuration ou d'historique

5.3 INTRUSION SUR LES RESEAUX DEDIES

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	M19 : Copie de badge
Ecoute d'une transaction contenant les données du mapping (AID, n° de fichier)	M20 : Copie de badge
Ecoute d'une transaction contenant le code pin	M21 : Usurpation d'identité
Ecoute d'une transaction contenant un événement d'accès	M22 : Modifier la traçabilité des événements
Ecoute d'une transaction contenant une alarme	M23 : Modifier la traçabilité des alarmes
Ecoute d'une transaction contenant une commande d'ouverture à distance	M24 : Tenter le rejeu
Ecoute d'une transaction avec le contrôleur ITL	M25 : Emuler un contrôleur ITL
Ecoute d'une transaction contenant la mise à jour de la clé de lecture du badge	M26 : Copie de badge
Ecoute d'une transaction contenant la mise à jour du firmware logiciel	M27 : Tentative d'injection d'un code en lieu et place du firmware UED
Ecoute d'une transaction entre l'ITL et l'UED	M28 : 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	M29 : 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 (M30).

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 (M31).

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 (M32).

5.7 ATTAQUE PAR INJECTION DE CODE MALVEILLANT SUR ITL/UED

L'objectif de cette attaque est de télécharger sur l'ITL ou l'UED un code non original, corrompu (M33).

6 DESCRIPTION DES FONCTIONS DE SECURITE

6.1 PROTECTIONS MISES EN ŒUVRE

P1 : Protection des données échangées entre le serveur et le contrôleur ITL

Cette protection est réalisée au travers de plusieurs moyens :

- 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 1.3 ; 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 saisis 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 Secure Systems & Services.

P7 : Protection des données échangées entre le poste opérateur et le serveur d'application

Cette protection est réalisée par l'établissement d'un canal de communication chiffré entre le serveur de d'application et le poste opérateur.

Les données échangées sont protégées en confidentialité et en intégrité (emploi du protocole https utilisant TLS 1.3 ; 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).

Les échanges sont réalisés dans le contexte d'une session, initiée par la fourniture du couple login/mot de passe de l'exploitant, et pour laquelle le serveur génère un jeton d'accès. Un mécanisme de renouvellement du jeton est mis en place, afin de doter ce jeton d'une durée de validité très courte, sans pour autant pénaliser l'opérateur en lui redemandant de saisir son mot de passe.

P8 : Protection des données échangées entre la base de données et les applications

Cette protection est réalisée par les mécanismes cryptographiques mis à disposition par Oracle permettant de sécuriser les communications. La sécurisation est assurée par un chiffrement des échanges en AES et un contrôle d'intégrité par fonction de hachage, incluant un échange de clés de sessions par algorithme cryptographique ; voir [Doc3] pour le détail du paramétrage de la fonctionnalité.

P9 : Protection des connexions opérateurs

Les phases de connexion des opérateurs donnent lieu à un échange sécurisé (protocole LDAPS) avec le serveur LDAP. Une fois établie la connexion d'un opérateur autorisé, on lui attribue un jeton d'accès JWT, ainsi qu'un jeton de rafraichissement. L'application cliente utilise le jeton d'accès pour authentifier chacune de ses demandes au serveur d'application. A échéance de la durée de validité de ce jeton (durée courte, de l'ordre de quelques minutes), l'application cliente doit utiliser son jeton de rafraichissement pour demander un nouveau jeton. Voir [Doc3] pour le détail des vérifications liées aux jetons JWT.

P10 : Protection des privilèges opérateurs

En ce qui concerne la menace d'élévation de privilège, la solution evolynx^NG utilise une notion de profil opérateur qui permet d'avoir une granularité fine du contrôle d'accès, définie au niveau de chaque requête transmise au serveur Wildfly. Ainsi, toutes les requêtes sont contrôlées vis-à-vis du profil de l'opérateur qui les exécute.

P11 : Protection des données sensibles stockées dans la base de données

Cette protection est réalisée par le chiffrement en AES et un contrôle d'intégrité par fonction de hachage des données sensibles stockées en base de données. Voir [Doc3] pour le détail du mode de chiffrement.

P12 : Protection du mot de passe d'accès à la base de données

Le mot de passe d'accès à la base de données n'est conservé que sur les serveurs GAC : serveur d'application et frontal. Ces serveurs sont protégés en accès physique et l'accès logique est limité aux administrateurs du SI, réputés de confiance.

Une protection supplémentaire est réalisée par le chiffrement du mot de passe. Selon les sous-systèmes nécessitant une connexion à la base de données, le stockage du mot de passe chiffré se fait :

- En base de registres : sous-système frontal
  Le chiffrement se fait à l'aide d'une application exécutée sur le frontal, utilisant la clé secrète Evolynx pour un chiffrement en AES.
- Dans le fichier de paramétrage du serveur Wildfly
  Le chiffrement se fait à l'aide d'un outil de Wildfly utilisant une clé secrète stockée dans un « credential-store ».

Voir [Doc3] pour le détail des modes de chiffrement.

P13 : Protection de l'intégrité des firmwares ITL/UED

Un mécanisme cryptographique est utilisé pour protéger le « package » contenant le firmware de l'ITL ou de l'UED.

Ce package est disponible pour téléchargement depuis l'IHM pour mise à jour à distance. Il peut aussi être déposé dans une clé USB pour effectuer la mise à jour localement sur la carte ITL ou UED.

Ce mécanisme repose sur l'utilisation d'un couple clé publique/clé privé de type RSA avec une taille de clé de 2048 bits pour la signature.

Le package est chiffré en AES 128 CBC et est signé en SHA256 en utilisant la clé privé RSA 2048.

Voir [Doc3] pour le détail de la fonctionnalité.

P14 : Protection du démarrage des ITL/UED ainsi que de l'intégrité des flash

Un mécanisme de secureBoot est utilisé pour établir une chaine de confiance sur l'ITL et l'UED garantissant que chaque composant chargé est authentique et n'est pas altéré.

De plus, les répertoires sensibles du système de fichier des ITL/UED sont sécurisés par l'utilisation du mode XTS utilisant l'algorithme AES avec une taille de clé de 256 bits.

Voir [Doc3] pour le détail de la fonctionnalité.

6.2 TRAÇABILITE ENTRE LES FONCTIONS DE SECURITE ET LES MENACES

	M1 à M12	M13	M14	M15	M16	M17	M18	M18 à M28	M29	M30	M31	M32	M33
P1	X												
P2								X					
P3									X				
P4										X			
P5											X		
P6												X	
P7		X											
P8			X										
P9				X									
P10					X								
P11						X							
P12							X						
P13													X
P14										X	X		

FIN DU DOCUMENT

Evolynx-CS-FR-Cible de sécurité evolynx^{NG} Révision G

Secure Systems & Services