FABRICANT FRANÇAIS DE SÉCURITÉ ÉLECTRONIQUE

Cible de sécurité

Système de contrôle d'accès XSecur'-Evo

V3.5

Référence : SYN-CIBLE-SCA-XSECUR-EVO
Date : lundi 18 mai 2026

Synchronic

Historique des versions

Version	Date	Auteur	Approbateur	Description des modifications
V1.05	18/07/2018	Laurent GALVAN	Nicolas BIGNARD	Cible de sécurité CSPN - XSecur'
V2.10	11/05/2022	Paul VAUTIER Antoine PROVOT Thomas BELTRANDO	Laurent GALVAN	Cible de sécurité UTL pour XSecur'-Evo
V3.0	03/02/2025	Simon BOEDEC Charles PARMENTIER Thomas BELTRANDO	Laurent GALVAN	Cible de sécurité Système de contrôle d'accès XSecur'-Evo
V3.1	09/05/2025	Théo MARTINEZ	Simon BOEDEC	Modification suite aux commentaires du CESTI et du CCN
V3.2	13/07/2025	Simon BOEDEC	Charles PARMENTIER	Mise à jour des versions logicielles
V3.4	04/12/2025	Théo MARTINEZ	Charles PARMENTIER Laurent GALVAN	Modification suite retour CESTI
V3.5	02/02/2026	Charles PARMENTIER	Théo MARTINEZ Laurent GALVAN	Modification suite aux commentaires du CCN

Copyright

Sommaire

1 INTRODUCTION

1.1 Identification de la cible de sécurité

Le présent document constitue la cible de sécurité du Système de contrôle d'accès XSecur'-Evo. Cette cible a été élaborée en vue de l'obtention de la Certification de Sécurité de Premier Niveau (CSPN) délivrée par l'ANSSI dans la catégorie identification, authentification et contrôle d'accès.

1.2 Identification du produit

Catégorie	Description / Lien
Fabricant	SYNCHRONIC
Dénomination commerciale du produit	Système de contrôle d'accès XSecur'-Evo
Version du produit évalué	v2.1
Site du fabricant	www.synchronic.fr
Catégorie du produit	Identification, authentification et contrôle d'accès

1.3 Références et glossaire

1.3.1 Références

N°	Source	Description / lien
[1]	ANSSI	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection (ANSSI-PA-72 v2.1)
[2]	ANSSI	Recommandations relatives à l'authentification multifacteur et aux mots de passe (ANSSI-PG-078 v2.0)
[3]	NXP	NXP AN10922 Symmetric key diversifications (v2.2)
[4]	ANSSI	Recommandations de sécurité relatives à TLS (v1.2)
[5]	ANSSI	Recommandations de déploiement du protocole 802.1x pour le contrôle d'accès à des réseaux locaux (ANSSI-PA-043 - v1.0)
[6]	SYNCHRONIC	SYN-DES-MEC-CRY-XSECUR-EVO.pdf
[7]	ANSSI	GUIDE D'HYGIÈNE INFORMATIQUE - Renforcer la sécurité de son système d'information en 42 mesures (v2.0)
[8]	SYNCHRONIC	DI XSecur-Evo.pdf
[9]	SYNCHRONIC	Guide Mapping MIFARE® DESFire®.pdf
[10]	SYNCHRONIC	SYN-DEP-SCA-XSECUR-EVO.pdf
[11]	SYNCHRONIC	SYN-SA-SCA-XSECUR-EVO.pdf
[12]	ANSSI	Certification de sécurité de premier niveau des produits des technologies de l'information (ANSSI-CSPN-CER-P-01 v5.0)
[13]	ANSSI	Méthodologie pour évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN (ANSSI-CSPN-NOTE-07 v2.1)
[14]	ANSSI	Contenu et structure de la cible de sécurité CSPN (ANSSI-CSPN-NOTE-09 v1.0)

1.3.2 Glossaire

Terme	Nom complet	Description
AES	Advanced Encryption Standard	Algorithme de chiffrement symétrique
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	
AP	Auto-Protection	Mise en protection automatique sur action non autorisée
CA	Contrôle d'Accès	
CRL	Certificate Revocation List	Liste de révocation des certificats
CSR	Certificate Signing Request	Demande de signature de certificat
DES	Data Encryption Standard	Algorithme de chiffrement symétrique
DESFire®		Carte à puce sans contact développée par NXP
GAC	Centre de Gestion des Accès Contrôlés	Aussi appelé Unité de Traitement de Supervision (UTS)
JWT	JSON Web Token	Format de jeton utilisé pour l'authentification sur des applications web
Mapping		Structure des données d'une puce MIFARE® DESFire®
Master Suite Evolution		Suite de logiciels permettant la configuration et l'exploitation des produits de la gamme XSecur'-Evo
NPS	Network Policy Server	Serveur qui gère les stratégies d'accès au réseau
PIN	Personal Identification Number	Code secret utilisé pour l'authentification
RADIUS	Remote Authentication Dial-In User Service	Protocole d'authentification de terminal sur le réseau
RFID	Radio Frequency IDentification	Technologie d'identification sans fil
SAM	Secure Access Module	Conteneur sécurisé transportable
SE	Secure Element	Elément actif permettant de stocker et provisionner des secrets ainsi que d'effectuer des opérations cryptographiques.
SBus	Secure Bus protocol	Bus sécurisé propriétaire Synchronic
SSCPv2	STid Secure Common Protocol version 2	Bus sécurisé propriétaire STid
TLS	Transport Layer Security	Protocole de sécurisation d'échanges TCP/IP
UID	Unique IDentifier	Identifiant unique du badge
URL	Uniform Resource Locator	Adresse permettant d'accéder à une ressource web
UTL	Unité de Traitement Local	
UTP-SEC-EVO		Unité de Traitement de Porte Sécurisée acceptant une extension SAM-SE
UTR	Unité de Traitement de Ressources	

2 DESCRIPTION DU PRODUIT

2.1 Description générale du produit

Le Système de contrôle d'accès XSecur'-Evo s'articule autour de l'interfaçage, via une liaison TCP/IP, de l'UTL pour XSecur'-Evo et du centre de Gestion des Accès Contrôlés (GAC).

L'UTL pour XSecur'-Evo est constituée des équipements terrain du système de contrôle d'accès physique centralisé, conçu et fabriqué en France par Synchronic. Elle utilise des technologies sans contact RFID ainsi que des claviers de saisie de codes PIN. Elle peut également s'interfacer via le protocole SBus avec des unités de traitement de ressources (UTR) pour la gestion des systèmes anti-intrusion.

Le GAC quant à lui est constituée de plusieurs serveurs et équipements de sécurité. Il inclut notamment le serveur hébergeant le logiciel de gestion du système de contrôle d'accès Xt Manager ainsi que sa base de données assurant la gestion des données essentielles au système.

2.1.1 Description des éléments constitutifs de la solution

La solution complète s'articule en deux sous-ensembles communicants :

- Le « **GAC** » composé des éléments de l'infrastructure informatique :
  - Le Serveur CA comprenant les logiciels et les bases de données de gestion/exploitation
  - L'Autorité de certification (non fourni par Synchronic)
  - Le Serveur RADIUS (non fourni par Synchronic)
  - Les postes clients
  - Les stations d'encodage de badges
  - Les stations de programmation SAM-SE

- L'« **UTL pour XSecur'-Evo »**, composée des équipements terrain :
  - Les concentrateurs d'accès de la gamme d'UTL pour XSecur'-Evo (cf. Annexe 4 : Références des concentrateurs de la Gamme d'UTL pour XSecur'-Evo)
  - Les modules de portes sécurisés UTP-SEC-EVO
  - Les lecteurs et lecteurs-claviers (cf. Annexe 5 : Références des lecteurs compatibles)
  - Les badges MIFARE® DESFire® EV2 / EV3 (natif ou applet sur JavaCard – ex : JCOP 3, JCOP 4.5)

2.1.2 Description fonctionnelle de la solution

Le Système de contrôle d'accès XSecur'-Evo répond au besoin de sécurisation d'accès physique, grâce à l'utilisation des technologies sans contact RFID 13,56MHz suivant la norme ISO 14443-A.

La mise en œuvre de la solution offre les fonctionnalités suivantes :

- Administrer et exploiter l'installation à travers le GAC :
  - Administration des droits d'accès selon les profils d'exploitation définis
  - Configuration et administration des équipements terrain
  - Gestion des populations de porteurs de badge depuis l'application métier Xt Manager publiée sur le GAC
  - Recensement des porteurs de badge avec garantie d'unicité
  - Attribution de droits d'accès aux porteurs selon restrictions (zones, horaires…)

- Gérer les flux de personne entre et au sein des zones sécurisées grâce à l'UTL pour XSecur'-Evo :
  - Identification et authentification du badge puis authentification du porteur tel que défini dans le guide ANSSI [1].
  - Décision de déverrouillage d'accès par télé-action prise par le concentrateur selon les droits d'accès accordés au porteur
  - Supervision de l'état physique d'accès avec remontée d'informations au GAC

Pour cela elle s'appuie à minima sur un Serveur CA, une autorité de certification, un Serveur RADIUS (802.1X), un poste client, une station d'encodage de badges, une station de programmation des SAM-SE, un concentrateur XSecur'-Evo, des modules de portes UTP-SEC-EVO, des lecteurs de badges ou lecteurs-claviers et des badges. Le GAC ainsi que le concentrateur XSecur'-Evo sont interconnectés via réseau Ethernet tandis que les éléments de la partie terrain sont interconnectés en bus filaire RS-485.

Afin d'optimiser les temps de réponse et d'ouverture d'accès du système, les droits d'accès sont contenus au plus près des lecteurs, à savoir dans le concentrateur XSecur'-Evo. Combinée à une alimentation secourue, l'UTL pour XSecur'-Evo bénéficie d'une grande résilience.

Pour accéder à une zone sécurisée, l'utilisateur final de la solution, appelé porteur de badge, place son badge RFID dans le champ électromagnétique du lecteur. L'authentification du badge est assurée par la robustesse des mécanismes cryptographiques de la technologie MIFARE® DESFire®.

Selon l'accès et afin d'authentifier le porteur du badge, un moyen d'authentification de type PIN doit être fourni en tant que second facteur. Les lecteurs d'accès, équipés de clavier, sont situés en dehors de la zone qu'ils contrôlent.

Aucune information nécessaire à la lecture d'un badge sécurisé n'est contenue dans les lecteurs. Ils transmettent les données sans les modifier et ne participent pas aux mécanismes cryptographiques. Ce mode de fonctionnement des lecteurs est appelé mode « transparent ». Cette architecture correspond à la configuration n°1 hautement recommandée du guide ANSSI [1] (cf. Annexe 1 : Configuration n°1, hautement recommandée).

2.1.3 Schéma d'architecture de la solution

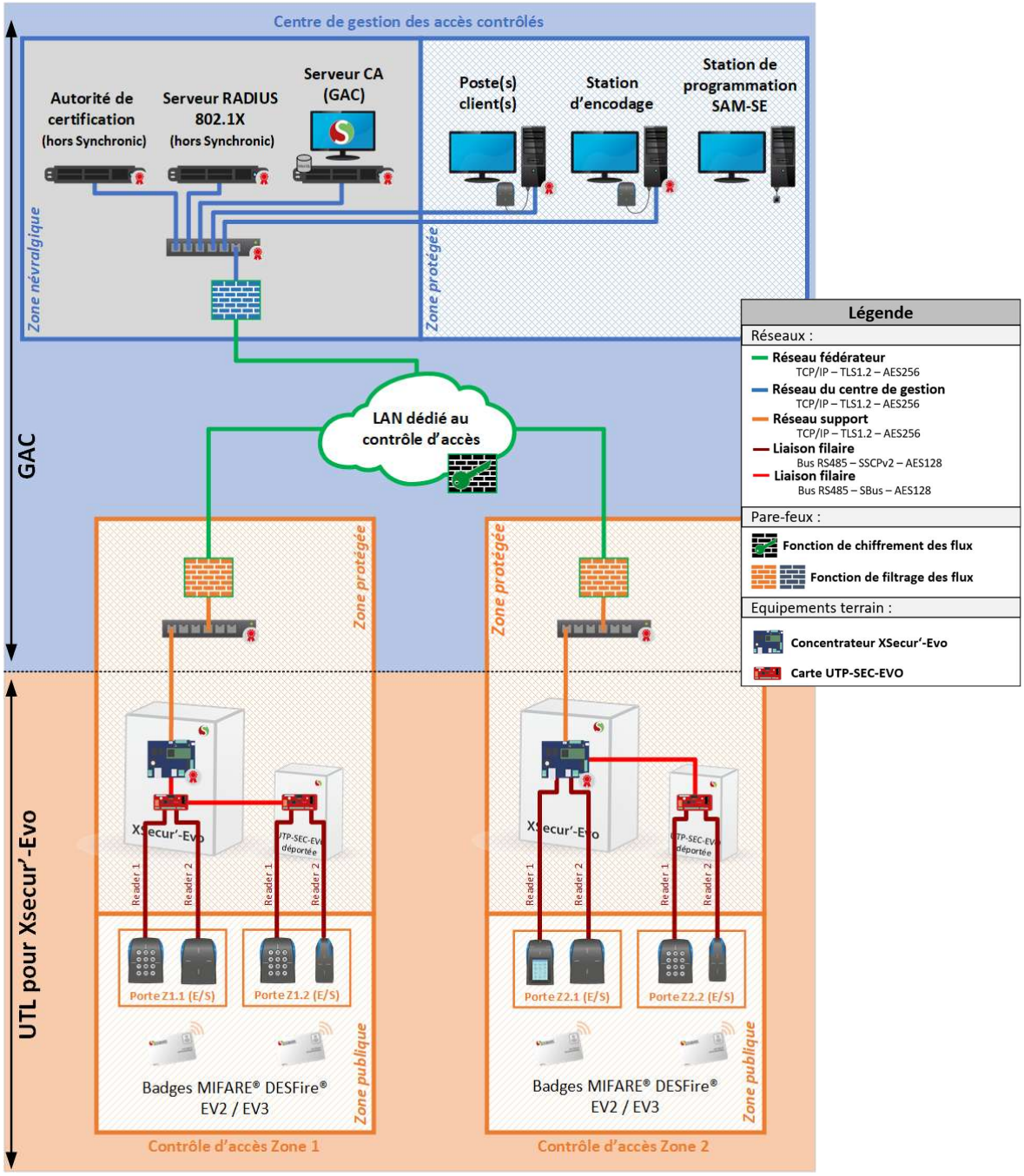

Figure 1 : Schéma d'architecture type d'un Système de contrôle d'accès XSecur'-Evo

2.1.4 Description des zones

Les composantes du système sont réparties dans différentes zones à niveau de protection adaptée à la criticité des valeurs métiers ou des biens supports à protéger (cf. Figure 1)

Trois types de zones sont distingués :

- **Zone publique** : Accessible à tout le monde (ex : accès extérieur à une zone protégée)
- **Zone protégée** : Accessible aux seuls employés autorisés et aux visiteurs accompagnés munis d'un badge (ex : bureaux, local technique, poste central de sécurité…)
- **Zone névralgique** : Accessible aux seuls employés autorisés et aux visiteurs accompagnés, et authentifiés au moyen d'un badge et d'un code PIN (ex : salle serveurs)

2.1.5 Description des réseaux

2.1.5.1 Réseaux Ethernet

Une partie de l'interconnexion des équipements (GAC ⇔ Concentrateurs XSecur'-Evo) repose sur l'infrastructure réseau du client.

Afin de segmenter les différents composants en fonction de leur nature et le rôle qu'ils assurent dans le système, le réseau Ethernet est décomposé en trois types de réseaux :

- Un ou plusieurs **réseaux support** dédié aux concentrateurs XSecur'-Evo qui sont authentifiés via le protocole RADIUS (802.1X). Dans la mesure du possible, aucun autre équipement n'est intégré à ces réseaux. A défaut, ces équipements supplémentaires sont à minima authentifiés ou, en cas d'incompatibilité avec le protocole RADIUS, vérifiés par un contrôle d'adresse MAC.
- Un **réseau du centre de gestion** dédié à l'interconnexion des différents équipements permettant la gestion du contrôle d'accès (Serveur CA, poste client, station d'encodage…) ainsi que les serveurs offrant des services d'infrastructures (autorité de certification, serveur RADIUS…). Ces équipements sont également authentifiés.
- Un **réseau fédérateur** qui a pour rôle d'assurer l'interconnexion des différents réseaux supports avec le réseau du centre de gestion. Un filtrage de flux est opéré sur ce réseau afin que seules les flux nécessaires et légitimes puissent transiter (filtrage de protocole, source/destination…) limitant ainsi les risques de compromission du centre de gestion depuis un réseau support.

Le **réseau fédérateur** n'est **pas inclus** dans le périmètre de l'évaluation à l'exception des flux qui transitent sur ce réseau entre les concentrateurs XSecur'-Evo et le GAC.

2.1.5.2 Bus RS-485

La seconde partie (Concentrateur ⇔ UTP-SEC-EVO, UTP-SEC-EVO ⇔ Lecteurs/Lecteurs-claviers) repose sur des bus RS-485 dédiés à l'installation du contrôle d'accès physique.

La partie terrain de l'UTL pour XSecur'-Evo, à savoir le module UTP-SEC-EVO natif des concentrateurs XSecur'-Evo, les éventuels modules UTP-SEC-EVO optionnels et les lecteurs sont interconnectés sur ces bus.

Ces bus sont situés dans la zone de sécurité protégée par l'UTL pour XSecur'-Evo. Les échanges de données y sont sécurisés via les protocoles SBus et SSCPv2, tel que décrit dans la description des mécanismes cryptographiques du Système de contrôle d'accès XSecur'-Evo [6].

Les **bus RS-485** sont **inclus** dans le périmètre de l'évaluation.

2.1.6 Description du GAC

2.1.6.1 Description du Serveur CA

Le Serveur CA a pour rôle la configuration et l'administration du Système de contrôle d'accès XSecur'-Evo dans son intégralité via les applicatifs métiers développés par Synchronic et constituant la Master Suite Evolution. Le poste Serveur CA est composé d'un serveur physique ou virtuel sous système d'exploitation Windows Server 2019 ou 2022. Il héberge la base de données reposant sur un système de gestion de base de données de type MySQL Server ou SQL Server.

La base de données contient l'ensemble des informations nécessaires à la gestion du contrôle d'accès physique, à savoir la liste des concentrateurs, des accès, des porteurs de badge ainsi que les droits d'accès. De plus toute opération effectuée sur l'interface métier de gestion des accès physiques est historisée avec horodatage dans la base de données.

Le Serveur CA est soumis aux différentes mesures du guide ANSSI [7] avec notamment la protection par une solution antivirus éprouvée ou encore le respect d'une politique rigoureuse de mise à jour, tout particulièrement en ce qui concerne les correctifs liés à la sécurité.

La stratégie de mot de passe appliquée par le client respecte à minima les préconisations du guide ANSSI [2] en ce qui concerne à la fois l'ensemble des mots de passe du système d'information et des mots de passe du Système de contrôle d'accès XSecur'-Evo.

Un compte administrateur bénéficiant de tous les droits de configuration et d'exploitation ainsi qu'un compte exploitant bénéficiant de droits restreints d'exploitation de la solution ont été paramétrés. Les différents services nécessaires aux applications sont également exécutés avec un compte de service dédié et au périmètre restreint aux seules autorisations nécessaires.

Le **Serveur CA** est **inclus** dans le périmètre de l'évaluation.

2.1.6.2 Description de l'Autorité de certification

L'Autorité de certification a pour rôle l'émission de certificats pour la mise en œuvre de la sécurisation de l'ensemble des éléments du Système de contrôle d'accès XSecur'-Evo. Elle est notamment capable d'assurer la gestion des demandes de signature de certificat (*CSR*) conforme à la spécification PKCS#10. Elle est également chargée de maintenir à jour et de publier la liste de révocation de certificats *(CRL)*. Etant un service d'infrastructure, sa configuration, son exploitation et son administration sont de la responsabilité du client ou de l'infogérant désigné.

L'**Autorité de certification** n'est **pas incluse** dans le périmètre de l'évaluation.

2.1.6.3 Description du Serveur RADIUS (802.1X)

Le Serveur RADIUS a pour rôle d'authentifier tous les équipements se connectant sur le réseau. Ceci permet de s'assurer que seuls les équipements légitimes accèdent à ce réseau. Les équipements réseaux actifs réalisent une isolation physique de leur port sur lequel un équipement non autorisé est connecté. Etant un service d'infrastructure, sa configuration, son exploitation et son administration sont de la responsabilité du client ou de l'infogérant désigné.

Le **Serveur RADIUS (802.1X)** n'est **pas inclus** dans le périmètre de l'évaluation.

2.1.6.4 Description du poste client

Le poste client a pour rôle l'exploitation de la gestion du contrôle d'accès physique à l'aide de l'applicatif métier Xt Manager. Il permet l'affectation et la propagation des droits d'accès au concentrateur XSecur'-Evo par le biais du Serveur CA. Sa communication avec le Serveur CA s'appuie sur le protocole HTTPS.

Il peut également avoir pour rôle l'enrôlement des badges préalablement mis à la clé via la station d'encodage. L'enrôlement consiste à lire l'ID Privé du badge afin de l'affecter à un utilisateur et nécessite que le poste soit équipé d'un dispositif USB d'enrôlement supporté par la solution.

Le poste client est soumis aux différentes mesures du guide ANSSI [7] avec notamment la protection par une solution antivirus éprouvée ou encore le respect d'une politique rigoureuse de mise à jour, tout particulièrement en ce qui concerne les correctifs liés à la sécurité.

La stratégie de mot de passe appliquée par le client respecte à minima les préconisations du guide ANSSI [2] en ce qui concerne à la fois l'ensemble des mots de passe du système d'information et des mots de passe du Système de contrôle d'accès XSecur'-Evo.

Un compte administrateur bénéficiant de tous les droits de configuration et d'exploitation ainsi qu'un compte exploitant bénéficiant de droits restreints d'exploitation de la solution ont été paramétrés.

Les **postes clients** sont **inclus** dans le périmètre de l'évaluation.

2.1.6.5 Description de la station d'encodage

La station d'encodage désigne le poste de travail à partir duquel un opérateur effectue les opérations de mise à la clé des badges. Les modèles d'équipement USB d'encodage listés dans l'Annexe 7 : Dispositifs USB d'encodage compatibles sont supportés par la solution. Comme pour les postes clients, la station d'encodage est connectée au réseau du centre de gestion pour réaliser l'encodage via Xt Manager.

La **station d'encodage n'**est **pas incluse** dans le périmètre de l'évaluation.

2.1.6.6 Description de la station de programmation SAM-SE

La station de programmation SAM-SE désigne le poste de travail à partir duquel un opérateur effectue les opérations de mise à la clé des cartes d'extension SAM-SE. Les opérations de mise à la clé de ces cartes consistent en l'injection des secrets nécessaires au bon fonctionnement de l'UTL pour XSecur'-Evo via le logiciel Leosac Key Manager. Les cartes d'extension SAM-SE peuvent ensuite être déployées sur le terrain afin de mettre l'UTL pour XSecur'-Evo dans ses conditions d'exploitation. Il est recommandé que cette station soit hors réseau.

La **station de programmation SAM-SE n'**est **pas incluse** dans le périmètre de l'évaluation.

2.1.7 Description des équipements terrain

2.1.7.1 Description du concentrateur XSecur'-Evo

Le concentrateur XSecur'-Evo a pour rôle de vérifier les droits d'accès des porteurs de badge suite à leur authentification et de piloter les organes d'ouverture de l'environnement de porte. Il possède les droits d'accès des utilisateurs et peut stocker jusqu'à 200 000 identifiants distincts.

Pour assurer un contrôle d'accès résilient, le concentrateur XSecur'-Evo, possédant ces dits-droits, ne dépend pas de la disponibilité du Serveur CA auquel il est associé pour autoriser le franchissement d'accès.

Les données sensibles du concentrateur sont stockées sur une partition chiffrée dont les caractéristiques sont décrites dans la description des mécanismes cryptographiques du Système de contrôle d'accès XSecur'-Evo [6]. L'ensemble des interfaces dédiées au développeur du concentrateur sont désactivées en production, celles-ci sont détaillées dans [11].

Le concentrateur XSecur'-Evo est notamment composé :

- D'un module de porte UTP-SEC-EVO natif chargé de l'interface avec les lecteurs de badges ou lecteurs-claviers (entrée et sortie) et l'environnement de porte. Le concentrateur XSecur'-Evo peut prendre également en charge jusqu'à 45 modules de porte UTP-SEC-EVO par ajout de cartes d'extensions réparties sur 3 bus terrain RS-485 (15 par bus).
- D'un SAM-SE Synchronic amovible de référence SE050 NXP, certifié EAL6+, chargé du stockage des secrets et des traitements cryptographiques sensibles. Son paramétrage réalisé par la station de programmation SAM-SE lui permet une gestion des lecteurs en mode « transparent ». Le SAM-SE exécute les mécanismes cryptographiques nécessaires à la communication avec les badges.

Cet ensemble est usuellement appelé UTL.

Une communication permanente avec le Serveur CA assure la remontée en temps réel des événements du contrôle d'accès physique, des défauts techniques (via supervisions des éléments) et des alarmes qui sont historisés et horodatés en base de données.

La sécurisation des échanges entre le concentrateur (UTP-SEC-EVO natif) et les lecteurs est assurée par le protocole SSCPv2 dont les caractéristiques sont décrites dans la description des mécanismes cryptographiques du Système de contrôle d'accès XSecur'-Evo [6]. Une clé d'initialisation de la communication appelée clé K, est paramétrée d'usine et doit être personnalisée avant exploitation de l'UTL pour XSecur'-Evo.

La sécurisation des échanges entre le concentrateur XSecur'-Evo et son Serveur CA repose sur le protocole TLS1.2 dans le respect du guide ANSSI [4]. La négociation TLS reposant sur une authentification mutuelle, un certificat d'initialisation de la communication est assigné d'usine du côté de l'UTL et du côté du Serveur CA. Ils devront être personnalisés par le client. Cette personnalisation s'appuie sur la génération de deux CSR transmises à l'autorité de certification qui pourra générer à partir de ces demandes deux certificats signés. L'un sera à injecter dans le SAM-SE de l'UTL, l'autre à installer sur le Serveur CA.

Le concentrateur XSecur'-Evo est compatible avec le protocole RADIUS (802.1X) tel que décrit dans le guide ANSSI [5] qui nécessitera un serveur RADIUS.

La sécurisation des échanges entre l'UTP-SEC-EVO native au concentrateur et son SAM-SE repose sur le protocole SCP03 dont les caractéristiques sont décrites dans la description des mécanismes cryptographiques du Système de contrôle d'accès XSecur'-Evo [6].

Le concentrateur XSecur'-Evo, usuellement situé en zone protégée, possède des mécanismes de protection d'ouverture de coffret (AP) à l'ouverture (lamelle et accéléromètre sur la face interne du capot) et à l'arrachement.

Information	Description
Dénomination	Gamme XSecur'-Evo (cf. Annexe 4 : Références des concentrateurs de la Gamme d'UTL pour XSecur'-Evo)
Dénomination technique	XL02-v7 / XP02-v5a (A5_SOCKET-V6)
Version noyau	V7-01-00 (Linux 6.6)
Version logicielle (Concentrateur XSecur'-Evo / Module UTP-SEC-EVO / Module TLS)	V13-71-98 / V4-18-50 / V2-37-50
Microprocesseur	ARM cortex A5
Emplacement	Coffret alarme en zone protégée ou zone névralgique
Données	Fichiers utilisateurs, fichier de configuration de lecture. Base de données sur une partition chiffrée
AP	Détection mécanique d'ouverture/arrachement et accéléromètre

Le **concentrateur XSecur'-Evo** est **inclus** dans le périmètre de l'évaluation.

2.1.7.2 Description de la carte d'extension SAM-SE

Le SAM-SE a pour rôle de stocker les clés et déporter certaines opérations cryptographiques sensibles. Il est amovible afin de faciliter son extraction ou son remplacement mais aussi permettre une diffusion des secrets par déploiement physique de carte d'extension SAM-SE.

Le SAM-SE dialogue avec le module UTP-SEC-EVO et le concentrateur via le protocole SCP03. Les clés d'authentification SCP03 du SAM-SE sont personnalisables et inextractibles du SAM-SE.

Plus généralement, toutes les clés cryptographiques stockées dans le SAM-SE respectent des politiques de clés non extractibles.

Information	Description
Dénomination	SAM-SE
Dénomination technique	SE050C
Version hardware	SAM V4
Cryptocoprocesseur	NXP SE050C1
Emplacement	Coffret alarme en zone protégée ou zone névralgique
Données	Paramètres MIFARE® DESFire®, clé SCP03, clé K, Certificats
AP	Anti tamper SE050 NXP EAL6+

La mise à la clé initiale du SAM-SE est réalisée d'usine et doit être personnalisée avant la mise en exploitation de l'UTL pour XSecur'-Evo par le client final. Cette mise à la clé s'effectue depuis la station de programmation SAM-SE.

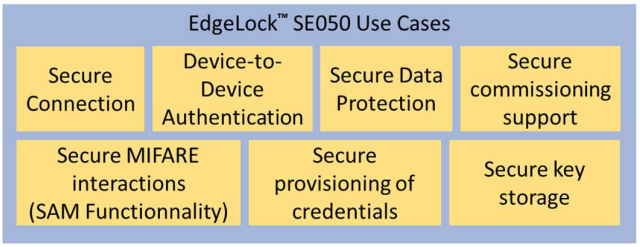

Figure 2 : Diagramme des cas d'usage SE050

La carte d'extension **SAM-SE** est **incluse** dans le périmètre de l'évaluation.

2.1.7.3 Description du module de porte UTP-SEC-EVO

Le module de porte sécurisé UTP-SEC-EVO a pour fonction d'étendre les capacités de gestion d'accès physiques du concentrateur XSecur'-Evo. Il peut être intégré dans le coffret de l'UTL ou déporté et reprend les fonctions assurées par le ou les modules UTP-SEC-EVO natifs du concentrateur à savoir : superviser l'environnement de porte, s'interfacer avec le lecteur-clavier et piloter l'organe de verrouillage de l'accès par télé-action.

Chaque module de porte sécurisé UTP-SEC-EVO est doté de sa propre carte d'extension SAM-SE. La sécurisation des échanges entre l'UTP-SEC-EVO déportée et son SAM-SE repose sur le protocole SCP03 dont les caractéristiques sont décrites dans la description des mécanismes cryptographiques du Système de contrôle d'accès XSecur'-Evo [6]. L'ensemble des interfaces dédiées au développeur du module UTP-SEC-EVO sont désactivées en production, celles-ci sont détaillées dans [11].

Information	Description
Dénomination	UTP-SEC-EVO
Version hardware	V10
Microcontrôleur	NXP Kinetis MK11
Emplacement	Coffret alarme ou coffret déporté en zone protégée

Le module de porte **UTP-SEC-EVO** est **inclus** dans le périmètre de l'évaluation.

2.1.7.4 Description des lecteurs et lecteurs-claviers

L'UTL pour XSecur'-Evo est compatible avec l'ensemble des lecteurs et duos lecteur-clavier de la gamme STid fonctionnant en mode sécurisé grâce à une liaison RS-485 s'appuyant sur le protocole SSCPv2 (cf. Annexe 5 : Références des lecteurs compatibles).

Le lecteur ou lecteur-clavier a pour rôle de transmettre les échanges RFID entre le badge et le module UTP-SEC-EVO. Ils fonctionnent en mode « transparent », et permettent d'authentifier le badge, et le porteur du badge par la saisie d'un code PIN en complément de la présentation de son badge d'accès. L'ensemble des interfaces dédiées au développeur des lecteurs sont désactivées en production, celles-ci sont détaillées dans [11].

Information	Description
Dénomination	Gamme STid 7AD
Dénomination technique	Cf. Annexe 5 : Références des lecteurs compatibles
Version logicielle	Z18-Z22
Microcontrôleur	NXP cortex M4
Emplacement	Zone publique ou zone protégée
Données	Clé K en EEPROM
AP	Accéléromètre (ouverture et arrachement)

Les **lecteurs** et **lecteurs-claviers** sont **inclus** dans le périmètre de l'évaluation.

2.1.7.5 Description du badge MIFARE® DESFire® EV2 / EV3

Le badge MIFARE® DESFire® EV2 / EV3 (natif ou applet sur JavaCard) certifié EAL5+, détenu par les utilisateurs de la solution contient l'identifiant privé unique de l'utilisateur. L'intégralité des informations présentes dans le badge est sécurisée par la méthode de diversification NXP-AN10922 [3] permettant à partir d'une clé maître, de paramètres de diversification et de l'UID du badge de générer une clé diversifiée unique. Cette clé intervient dans l'opération de chiffrement AES-128 de l'ID Privé réalisée par le badge.

Aucune information visuelle à l'exception d'un code de traçabilité n'est présente sur le support pour les badges de type carte. Ce code de traçabilité est différent de l'UID de la puce.

Les **badges** ne sont **pas inclus** dans le périmètre de l'évaluation.

2.2 Description de l'utilisation courante du produit

Le Système de contrôle d'accès XSecur'-Evo est basée sur l'utilisation de badges répondant aux caractéristiques spécifiées dans le §2.1.7.5. Ces badges sont prêts à l'emploi, ils ont été paramétrés soit par une station d'encodage de la solution soit par un prestataire. Ils contiennent une application propre au contrôle d'accès du client et disposent d'au moins un fichier de données contenant l'ID Privé. Cet ID Privé est sécurisé par l'utilisation de la méthode de diversification NXP-AN10922 [3].

2.2.1 Badge

Le porteur de badge positionne son badge dans le champ électromagnétique du lecteur contrôlant l'accès qu'il souhaite franchir. L'UTP-SEC-EVO, par l'intermédiaire du lecteur en mode « transparent », identifie la technologie du badge, lit l'UID de la puce puis sélectionne l'application paramétrée afin de consulter les données d'un fichier représentant l'ID Privé.

Le module SAM-SE possédant les paramètres de diversification NXP-AN10922 [3] ayant servie à l'encodage du badge à l'exception de l'UID, récupère l'UID du badge via le module UTP-SEC-EVO. Le module SAM-SE procède ensuite à l'authentification et à la génération de clés de session, au déchiffrement et à la vérification de l'intégrité de l'ID Privé.

Le concentrateur XSecur'-Evo vérifie dans sa base de données les paramètres de droits d'accès associés à l'ID Privé déchiffré afin d'établir la légitimité de la demande d'accès du porteur de badge. Un ordre de déverrouillage peut alors être transmis par le concentrateur au dispositif de verrouillage de l'accès via le canal de communication sécurisé SBus.

Cet événement de lecture contenant l'ID Privé est simultanément inscrit dans les journaux locaux au concentrateur ainsi que remonté via sécurisation TLS1.2 pour historisation sur le Serveur CA.

Afin d'assurer une transition temporelle de révocation de clé de lecture MIFARE® DESFire® ou de pouvoir lire les ID Privés de plusieurs populations de badges distinctes, l'UTL pour XSecur'-Evo permet de lire jusqu'à quatre configurations de paramètres MIFARE® DESFire®.

2.2.2 Badge + Code PIN

Afin de renforcer la sécurisation de l'accès, en plus de l'identification et l'authentification du badge assurées par les mécanismes de la technologie MIFARE® DESFire®, certains lecteurs sont équipés d'un clavier physique ou d'un clavier LCD permettant un affichage de position aléatoire des touches. Cela permet au porteur de badge de s'authentifier via un code PIN.

Suite à la présentation de son badge valide (ID Privé accepté) au lecteur-clavier, son porteur saisit un code PIN qui est transmis au concentrateur XSecur'-Evo de manière sécurisée via la liaison filaire RS-485 utilisant le protocole SSCPv2. Il est chiffré en AES-128 jusqu'à l'UTL.

Le module UTP-SEC-EVO déchiffre le code PIN transmis par le lecteur-clavier et le concentrateur s'assure de sa validité en correspondance avec le badge préalablement authentifié par son porteur. Un ordre de déverrouillage temporaire peut alors être transmis par le concentrateur au dispositif de verrouillage de l'accès.

Cet événement de saisie de code PIN est simultanément inscrit dans les journaux locaux au concentrateur ainsi que remonté via sécurisation TLS1.2 pour historisation sur le Serveur CA par le biais du réseau fédérateur.

La fonctionnalité badge+code est active selon configuration soit sur grille horaire soit selon le profil du porteur de badge. Le porteur dispose d'un délai paramétrable de saisie du code PIN suite à authentification de son badge.

2.3 Description de l'environnement d'utilisation du produit

Le Système de contrôle d'accès XSecur'-Evo intègre les recommandations présentes dans le guide ANSSI [1]. Les lecteurs proposés dans le périmètre sont munis, en plus de la fonctionnalité RFID, d'un moyen d'authentification du porteur du badge (code PIN).

L'architecture mise en œuvre correspond à « Configuration type n°1 » du guide susmentionné (cf. Annexe 1 : Configuration n°1, hautement recommandée), les lecteurs ne possèdent donc aucune clé cryptographique nécessaire à la lecture de badges (le « mode transparent ») afin d'éloigner celles-ci des abords immédiats de la zone publique. Cela a été rendu possible par l'intégration du protocole SSCPv2 sur bus RS-485.

Le Système de contrôle d'accès XSecur'-Evo a pour vocation de sécuriser les accès physiques de locaux industriels, tertiaires, bancaires et des administrations.

2.4 Description des compatibilités / dépendances

La Système de contrôle d'accès XSecur'-Evo est compatible avec les badges RFID de technologies MIFARE® Classic, MIFARE® DESFire®, EV2 et EV3. Cependant, il est fortement recommandé d'utiliser cette solution avec des badges répondant aux caractéristiques spécifiées dans le §2.1.7.5.

Le module UTP-SEC-EVO est compatible avec l'ensemble des équipements 7AD communiquant via le protocole SSCPv2 du fabricant de têtes de lecture RFID STid (cf. Annexe 5 : Références des lecteurs compatibles).

La Système de contrôle d'accès XSecur'-Evo est déployée sur des infrastructures informatiques opérant sous système d'exploitation Windows.

Les bases de données reposent sur un système de gestion de bases de données de type MySQL Server ou SQL Server. MySQL Server 8.0 est inclus dans le programme d'installation de la Master Suite Evolution.

Les bibliothèques tierces exploitées par la solution sont détaillées dans le document [10].

2.5 Description des utilisateurs typiques

2.5.1 Exploitants et Administrateurs

Les exploitants et les administrateurs sont les personnes internes ou externes à l'organisation du client ayant été mandatées et formées pour assurer la gestion de la sûreté et interviennent sur les éléments du GAC. La liste de leurs tâches diffère selon leur niveau d'habilitations (cf. Annexe 6 : Liste des tâches associées aux utilisateurs). Par ailleurs, ils ont également pour rôle de se connecter logiquement au concentrateur XSecur'-Evo pour réaliser sa configuration.

Les connexions aux applications du GAC et au concentrateur XSecur'-Evo sont toutes tracées avec un détail des actions effectuées.

Parmi les exploitants, seront distingués les agents sûreté et le Responsable sûreté.

2.5.2 Agents Techniques

Les agents techniques sont les personnes internes ou externes à l'organisation du client ayant été mandatées pour assurer le déploiement, la mise en service et la maintenance de l'UTL pour XSecur'-Evo. Ils sont les seuls à disposer des procédures d'accès physique au concentrateur XSecur'-Evo et à intervenir sur les éléments de l'UTL pour XSecur'-Evo (cf. Annexe 6 : Liste des tâches associées aux utilisateurs).

Les ouvertures du coffret contenant le concentrateur sont toutes tracées avec un détail des actions effectuées. En cas d'ouverture du coffret hors procédure les données sensibles sont automatiquement supprimées (cf. *DI XSecur'-Evo*).

2.5.3 Porteurs de Badge

Les porteurs de badge du Système de contrôle d'accès XSecur'-Evo sont toutes les personnes utilisatrices du dispositif de contrôle d'accès physique du client (cf. Annexe 6 : Liste des tâches associées aux utilisateurs). Ils peuvent appartenir, d'un point de vue du client final, à une population de :

- Collaborateurs
- Prestataires
- Visiteurs

Ils accèdent aux zones protégées voire névralgiques grâce :

- Au badge RFID remis par le service sûreté du client répondant aux caractéristiques du §2.1.7.5
- (Optionnellement) Au code PIN personnalisé par le porteur de badge.

Ce second facteur d'authentification est réservé aux accès contrôlés par le système devant se conformer au niveau de sûreté IV défini dans le guide ANSSI [1]. (Cf. Annexe 2 : Badges : niveaux de sûreté, résistance aux attaques logiques).

2.6 Description du périmètre de l'évaluation

La présente cible de sécurité prévoit l'évaluation des équipements terrain assurant les fonctions de contrôle d'accès physique par authentification d'un badge et de son porteur, à savoir :

- Le concentrateur XSecur'-Evo avec SAM-SE
- Le module UTP-SEC-EVO avec SAM-SE
- Les lecteurs compatibles

Mais également les éléments du GAC participant à la gestion du contrôle d'accès, à savoir :

- Le Serveur CA
- Le poste client

Composant du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance	Attaquant potentiel
GAC	**Système d'exploitation**		Windows Server 2022 Windows 11	
	Applicatifs	Xt Manager : **1.14.50** ServeurUG_TLS : **5.33.0**		
	Fonctions cryptographiques	Xt Manager : OpenSSL **3.1** ServeurUG_TLS : mbedTLS **3.6.5**		
	Bases de données et annuaires		MySQL Server **8.4**	
UTL	**Matériel**	UTL: **PCB XL02-v7 / XP02-v5a** (Atmel ATSAMA5D44B-CU) UTP-SEC-EVO: **PCB V10** (NXP Kinetis MK11DxxxxAVLK5, xxxx selon taille mémoire)		
	Système d'exploitation	UTL: **v7-01-00** • Linux **6.6** (Microchip LTS) • Debian 1**2** UTP-SEC-EVO : **sans OS**		
	Applicatifs	UTL : Firmware XPert **13-71-98** Module-TLS : **2-37-50** Module-WEB : **15-41-50** UTP-SEC-EVO : **4-18-50**		
	Fonctions cryptographiques	UTL : mbedTLS **3.6.5** UTP-SEC-EVO : mbedTLS **3.6.5** mmCAU library **1.4**		
	SAM	SAM-SE : **PCB SAM V4** (NXP SE050C)		
Lecteurs	**Lecteurs simples**	SSCPv2 : **Z18-Z22**		
	Lecteurs-claviers	SSCPv2 : **Z18-Z22**		
Badges			EV3: MF3D(H)x3, EV2: MF3D(H)x2 (H selon format, x selon capacité) JCOP : JCOP 4.5 sur P71D600	

2.7 Schéma du périmètre de l'évaluation

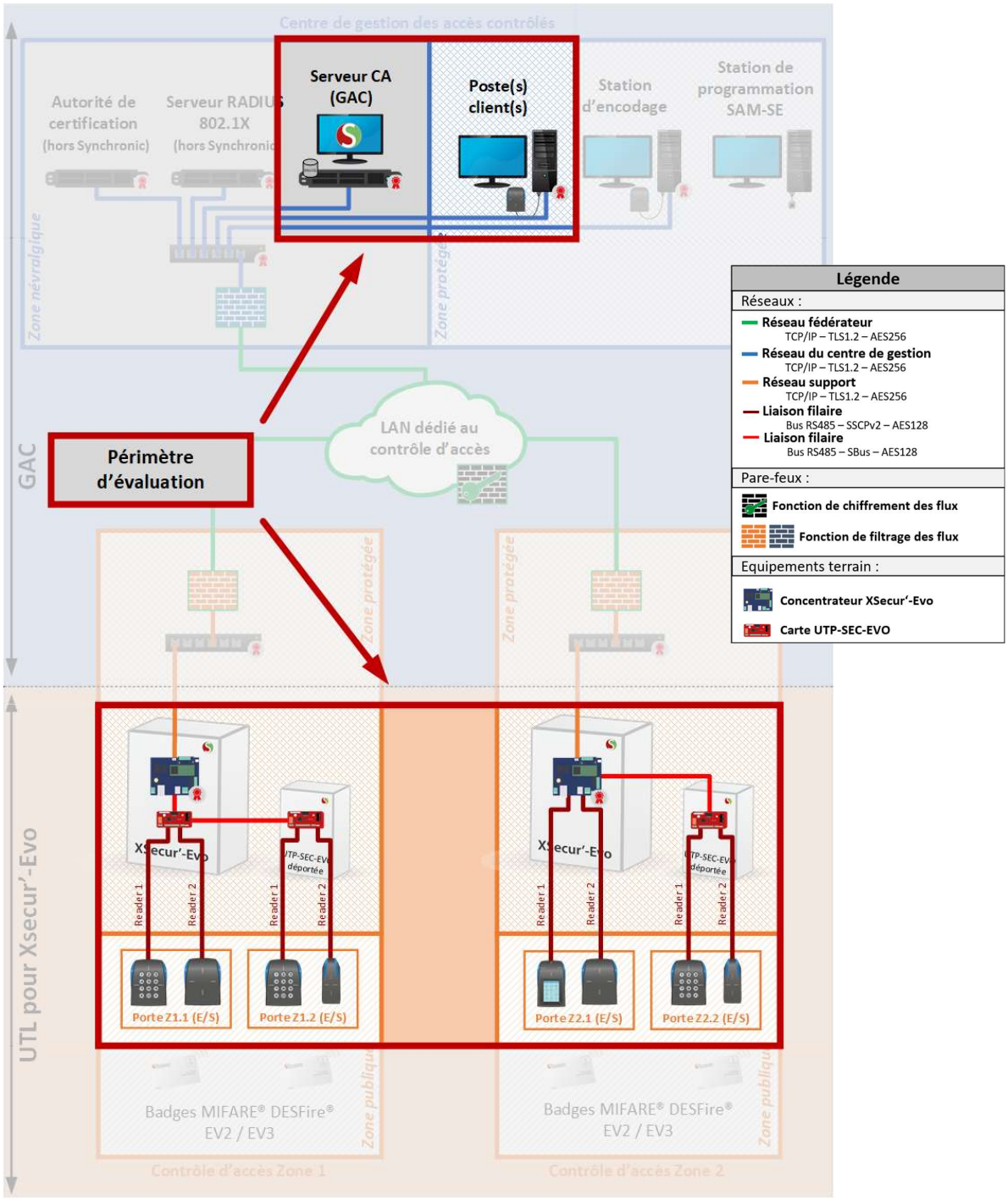

Figure 3 : Schéma du périmètre de l'évaluation

3 DESCRIPTION DES MESURES ENVIRONNEMENTALES (HYPOTHESES)

3.1 Hypothèses d'environnement d'installation du produit

Le produit est déployé chez le client par une société d'installation qualifiée ou le service technique du client, préalablement formés par le constructeur.

3.1.1 Hypothèses d'environnement d'installation logique du produit

Les éléments du GAC répondent aux caractéristiques suivantes :

- Serveur CA : Windows Server 2022, MySQL Server 8.0 avec derniers correctifs
- Autorité de certification : Windows Server 2022 avec rôle d'autorité de certification avec dernier correctifs
- Serveur RADIUS : Windows Server 2022 avec rôle NPS comme serveur RADIUS avec derniers correctifs
- Poste exploitation client : Windows 11 avec derniers correctifs et navigateur Google Chrome 125 ou supérieur ou Mozilla Firefox ESR 115 ou supérieur.

La stratégie de mot de passe appliquée par le client respecte à minima les préconisations du guide ANSSI [2] en ce qui concerne à la fois l'ensemble des mots de passe du système d'information et des mots de passe du Système de contrôle d'accès XSecur'-Evo.

Sur le Serveur CA, les postes d'exploitation et les stations de programmation, un compte administrateur bénéficiant de tous les droits de configuration et d'exploitation ainsi qu'un compte exploitant bénéficiant de droits restreints d'exploitation de la solution ont été paramétrés. Les différents services nécessaires aux applications sont également exécutés avec un compte de service dédié et au périmètre restreint aux seules autorisations nécessaires.

Des certificats X509v3 ont été déployés sur le Serveur CA et dans le concentrateur XSecur'-Evo afin de personnaliser la sécurisation des échanges de données TLS1.2 entre ces deux équipements. Leur génération a été réalisée en conformité avec les recommandations présentes dans le document [8].

Le SAM-SE des concentrateurs XSecur'-Evo et modules UTP-SEC-EVO a été mis à la clé par le biais d'une station de programmation SAM-SE isolée du réseau GAC et a ensuite été déployé physiquement sur son concentrateur.

3.1.2 Hypothèses d'environnement d'installation physique du produit

Serveur CA

Situé dans un local informatique en zone névralgique son accès est limité aux strictes personnes habilitées à administrer le système d'information et le Système de contrôle d'accès XSecur'-Evo. Le Serveur CA sera considéré de confiance et sans attaquant.

Poste client

Situé dans les locaux du client en zone protégée, son accès est limité aux strictes personnes habilitées à exploiter et administrer la solution de contrôle d'accès physique. Les postes d'exploitation seront considérés de confiance cependant les exploitants de type agents sûreté seront considérés comme potentiels attaquants.

Station d'encodage, station de programmation du SAM-SE

Situé dans les locaux du client en zone protégée, son accès est limité aux strictes personnes habilitées à encoder des badges et programmer des SAM-SE. Ces stations sont considérées de confiance et sans attaquant.

Concentrateur XSecur'-Evo

Muni d'un SAM-SE, situé en zone protégée ou en zone névralgique, le câblage de l'environnement de porte est réalisé sur le concentrateur en point à point.

Module UTP-SEC-EVO

Muni d'un SAM-SE, situé en zone protégée ou en zone névralgique, le câblage de l'environnement de porte est réalisé en point et à point (contacts secs). Les liaisons filaires RS-485 vers l'UTL et les lecteurs pénètrent immédiatement et ne sont pas apparentes.

Lecteurs-claviers RFID

Seul dispositif de l'UTL pour XSecur'-Evo installé en zone non protégée, le câble de raccordement au concentrateur XSecur'-Evo ou au module UTP-SEC-EV0 doit pénétrer immédiatement en zone protégée afin de s'assurer d'aucun cheminement en zone non protégée. Cette liaison de type filaire réseau RS-485 est directe.

Dispositif d'accès :

L'UTL pour XSecur'-Evo supervise un dispositif d'accès composé d'un environnement de porte comprenant à minima :

- Un détecteur d'ouverture de porte
- Un contact sec d'état de verrouillage de la porte
- Un bouton poussoir de sortie (ou un lecteur-clavier)
- Un organe de commande d'ouverture soit par contact sec soit par alimentation (rupture : ventouse, émission : gâche électrique)

3.2 Hypothèses sur les réseaux et bus du produit

Réseau fédérateur

Ce réseau, de type liaison filaire Ethernet, sert à interconnecter les réseaux supports et le réseau du centre de gestion. Il est administré intégralement par le client final, ou un prestataire, qui en a l'entière responsabilité. Conformément aux recommandations du guide ANSSI [1], un filtrage des flux transitant sur ce réseau est mis en œuvre afin de n'autoriser que les flux strictement nécessaires.

Réseau support

Ce réseau, de type liaison filaire Ethernet, sert à connecter les concentrateurs. Il est administré intégralement par le client final, ou un prestataire, qui en a l'entière responsabilité. Conformément aux recommandations du guide ANSSI [1], les concentrateurs sont cloisonnés sur le réseau les uns des autres au travers de réseaux locaux virtuels privés ou dédiés, ces derniers n'ayant besoin de communiquer qu'avec le GAC. Seuls les équipements authentifiés par le protocole RADIUS peuvent s'y connecter.

Réseau du centre de gestion

Ce réseau, de type liaison filaire Ethernet, sert à connecter les éléments du centre de gestion des accès contrôlés. Il est administré intégralement par le client final, ou un prestataire, qui en a l'entière responsabilité. Conformément aux recommandations du guide ANSSI [1], un filtrage est mis en place afin de limiter les risques de compromission du Serveur CA depuis le réseau support, fédérateur ou GAC. Seuls les équipements authentifiés par le protocole RADIUS peuvent s'y connecter.

Bus RS-485

Ces bus, de type liaison filaire bus RS-485, sont indépendants physiquement dans le sens où un lecteur sera toujours raccordé à une UTP-SEC-EVO qu'elle soit native au concentrateur ou non. L'interface SBus du concentrateur permet de raccorder d'autres modules UTP-SEC-EVO au besoin. Ces bus se situent en zone protégée.

Les deux liaisons filaires (Ethernet et RS-485), physiquement distincts, sont totalement étanches et ne peuvent échanger aucune donnée entre eux. Le concentrateur XSecur'-Evo assure la séparation entre les deux.

3.3 Hypothèses sur les exploitants et administrateurs du produit

L'exploitation du Système de contrôle d'accès XSecur'-Evo, qui consiste en la gestion des droits d'accès et la supervision des alarmes en temps réel, peut être réalisée par plusieurs profils d'individus selon la structuration organisationnelle du client final, à savoir :

- Membre de l'équipe sûreté
- Membre de la direction
- Prestataire d'une société de service

Ce personnel théoriquement de confiance et non hostile est formé pour s'approprier dans sa pleine mesure le système et réaliser strictement les opérations qui lui incombent.

Cependant afin de réduire la confiance implicite accordée à l'ensemble des exploitants, la gestion des accès de certaines zones et certains porteurs de badges à privilèges seront considérés sensibles. Cette gestion particulière est alors à la charge du Responsable sûreté. Le Responsable sûreté et les administrateurs seront considérés de confiance alors que les agents sûreté seront considérés comme attaquants potentiels.

L'ensemble de ce personnel est formé au périmètre d'actions affectées pour s'approprier dans sa pleine mesure le système. A l'exception des exploitants de type agents sûreté malveillants, ce personnel réalise strictement les opérations qui lui incombent.

Selon son profil, l'exploitant ou l'administrateur se voit affecté un compte d'exploitation nominatif lui permettant l'accès aux applications du GAC avec des droits restreints aux seules opérations qui relèvent de son périmètre de responsabilité.

3.4 Hypothèses sur les agents techniques du produit

Les agents techniques sont les personnels mandatés par le client final et formés à l'installation et la maintenance des composants de l'UTL pour XSecur'-Evo.

Ils disposent des procédures d'accès aux équipements situés en zone protégée et en zone névralgique. Cette procédure est personnalisable. Les étapes suivantes sont préconisées :

- Activation préalable de la maintenance de l'équipement par l'administrateur (à défaut de quoi l'ouverture du coffret provoquera une alarme et l'effacement des secrets du concentrateur et de toutes les cartes UTP-SEC-EVO qui lui sont reliées).
- Accès au local où se situe le coffret par l'agent technique.
- Ouverture du coffret XSecur'-Evo ou UTP-SEC-EVO par l'agent technique et réalisation des opérations de maintenance.

3.5 Hypothèses sur les utilisateurs finaux du produit

Les utilisateurs finaux du système, appelés utilisateurs ou porteurs de badge, sont composés de l'ensemble des catégories d'individus étant amenés à pénétrer physiquement par le biais d'un badge dans une zone contrôlée par un lecteur.

Les utilisateurs finaux ne doivent en aucun cas divulguer leur code PIN ou prêter leur badge à un autre individu.

A chaque passage, un porteur de badge doit réaliser l'authentification qu'impose l'accès même si l'accès est franchissable sans cette procédure (exemple : porte déjà ouverte).

3.6 Hypothèses sur les badges

Les badges sont de technologie MIFARE® DESFire® de la société NXP et sont certifiés EAL5+. L'utilisation de l'UID est proscrite au profit d'un identifiant, appelé ID Privé, qui aura été préalablement encodé dans les puces soit par un prestataire extérieur, soit par le client final via la solution d'encodage Synchronic ou une solution tierce. Le mapping de ces badges devra respecter les recommandations Synchronic (cf. [9]).

La confidentialité de l'identifiant privé, composé de 5 à 7 octets, est assurée par une clé AES-128 diversifiée pouvant être introduite par cérémonie des clés dans le système. La diversification, utilisant la méthode NXP-AN10922 [3], est employée en tant que moyen de résistance aux attaques logiques comme le spécifient les méthodes des niveaux de sécurité III et IV du guide de l'ANSSI [1].

La traçabilité des badges type carte est assurée par un numéro visible sur le support qui n'est qu'un numéro de traçabilité. Il ne doit en aucun cas correspondre à l'UID, l'ID Privé ou encore au numéro de matricule du porteur.

Comme défini dans le tableau présent Annexe 2 : Badges : niveaux de sûreté, résistance aux attaques logiques, les badges sont encodés avec des paramètres spécifiques correspondant soit :

- **Au niveau de sûreté II** : utilisation d'une clé de lecture AES-128
- **Au niveau de sûreté III** : utilisation d'une clé de lecture AES-128 diversifiée NXP-AN10922 [3]
- **Au niveau de sûreté IV** : utilisation d'une clé de lecture AES-128 diversifiée NXP-AN10922 [3] et authentification du porteur via un second facteur (code PIN)

Les badges de technologies MIFARE® DESFire® EV2 / EV3 permettent de répondre aux niveaux de sûreté ci-dessus.

3.7 Synthèse des mesures environnementales

Type	Description	Acteurs
Organisationnelle	Le produit est déployé chez le client par une société d'installation qualifiée ou le service technique du client, préalablement formés par le constructeur.	Administrateur, Synchronic
Organisationnelle	L'accès au Serveur CA est limité aux strictes personnes habilitées à administrer le système d'information et le Système de contrôle d'accès XSecur'-Evo	Administrateur
Organisationnelle	L'accès au poste client est limité aux strictes personnes habilitées à exploiter et administrer la solution de contrôle d'accès physique	Administrateur
Organisationnelle	L'accès à la station d'encodage de badges ou à la station de programmation SAM-SE est limité aux strictes personnes habilitées à encoder des badges ou programmer des SAM-SE	Administrateur
Organisationnelle	L'ensemble des réseaux est intégralement administré par le client final, ou un prestataire, qui en a l'entière responsabilité.	Administrateur
Organisationnelle	L'ensemble des acteurs exploitant le Système de contrôle d'accès XSecur'-Evo est formé pour s'approprier dans sa pleine mesure le système et réaliser strictement les opérations qui lui incombent.	Administrateur
Organisationnelle	La gestion des accès et porteurs de badges considérés sensibles est réalisée uniquement par le Responsable Sûreté.	Responsable sûreté
Organisationnelle	Un compte d'exploitation nominatif d'accès aux applications du GAC est affecté à tout exploitant ou administrateur avec des droits restreints aux seules opérations qui relèvent de son périmètre de responsabilité.	Administrateur
Organisationnelle	Les porteurs de badges réalisent l'authentification qu'impose l'accès même si l'accès est franchissable sans cette procédure	Responsable Sûreté
Organisationnelle	Les porteurs de badges ne prêtent pas leur badge et ne divulguent pas leur code PIN.	Responsable Sûreté
Organisationnelle	Les badges sont de technologie MIFARE® DESFire® EV2/EV3 de la société NXP et sont certifiés EAL5+	Administrateur
Organisationnelle	L'utilisation de l'UID est proscrite au profit de l'ID Privé, qui aura été préalablement encodé dans les puces soit par un prestataire extérieur, soit par le client final via la solution d'encodage Synchronic ou une solution tierce.	Administrateur
Installation	Le SAM-SE des concentrateurs XSecur'-Evo et modules UTP-SEC-EVO a été mis à la clé par le biais d'une station de programmation SAM-SE et a ensuite été déployé physiquement sur son concentrateur	Administrateur
Installation	Le Serveur CA est situé dans un local informatique en zone névralgique.	Administrateur
Installation	Le poste client est situé dans les locaux du client en zone protégée.	Administrateur
Installation	La station d'encodage de badges et la station de programmation SAM-SE sont situés dans les locaux du client en zone protégée.	Administrateur
Installation	Les concentrateurs XSecur'-Evo et les modules UTP-SEC-EVO sont situés en zone protégée ou en zone névralgique.	Administrateur, Agent technique
Installation	Chaque environnement de porte de compose d'un détecteur d'ouverture de porte, un contact sec d'état de verrouillage de la porte, un bouton poussoir de sortie, un organe de commande d'ouverture par contact sec ou par alimentation.	Administrateur, Agent technique
Installation	Le câblage de l'environnement de porte est réalisé en point à point (contacts secs)	Administrateur, Agent

		technique
Installation	Les liaisons filaires RS-485 pénètrent immédiatement et ne sont pas apparentes.	Administrateur, Agent technique
Installation	Tous les bus sont situés en zone protégée.	Administrateur, Agent technique
IT	Les serveurs, postes clients, et stations répondent aux spécifications du chapitre §3.1.1	Administrateur
IT	Une stratégie de mot de passe est appliquée par le client respectant à minima les préconisations du guide ANSSI [2] que ce soit pour les mots de passe du système d'information ou pour le Système de contrôle d'accès XSecur'-Evo	Administrateur
IT	Sur le serveur CA et les différents postes de gestion du système, un compte administrateur et des comptes exploitants restreints sont paramétrés.	Administrateur
IT	Les certificats nécessaires à la communication entre le Serveur CA et le concentrateur XSecur'-Evo ont été personnalisés et générer selon les recommandations de la documentation [8].	Administrateur
IT	Un filtrage de flux est mis en place entre chaque type de réseau et entre le Serveur CA et les postes de gestion du système pour ne laisser transiter que les flux nécessaires.	Administrateur
IT	Seuls les équipements authentifiés par le protocole RADIUS peuvent se connecter au réseau du centre de gestion, fédérateur ou support.	Administrateur

4 DESCRIPTION DES BIENS SENSIBLES

4.1 Liste des biens sensibles du Système de contrôle d'accès XSecur'-Evo

Les biens sensibles protégées par l'UTL pour XSecur'-Evo sont :

- Les données confidentielles du contrôle d'accès :
  - Les paramètres MIFARE® DESFire® d'accès à l'identifiant privé :
    - Clé maître de lecture
    - Clé de lecture UID du badge
    - Vecteur de diversification (System Identifier)
    - Paramètres de diversification
  - La BDD des concentrateurs :
    - Les identifiant privés
    - Les codes PIN
    - Les droits d'accès des porteurs de badge
    - Les historiques d'accès
- Les éléments de sécurisation des communications de l'UTL pour XSecur'-Evo :
  - Bus :
    - Clé K SSCPv2 pour dialogue lecteur/concentrateur ou lecteur/UTP-SEC-EVO
    - Clé K' SBus pour dialogue concentrateur/UTP-SEC-EVO
  - Réseau IP (support, fédérateur, centre de gestion) : les clés privées TLS
  - Communication SAM-SE :
    - Clé SCP03 du SAM-SE et du concentrateur
    - Clé SCP03 du SAM-SE et du module UTP-SEC-EVO
- Les éléments logiciels sensibles :
  - Firmwares des concentrateurs XSecur'-Evo
  - Firmwares des UTP-SEC-EVO
- Le système d'exploitation du Serveur CA

Les paramètres MIFARE® DESFire® sont déterminés, conservés et sous contrôle du service sûreté du client.

Les biens sensibles protégées par le GAC sont :

- La base de données du Serveur CA qui contient :
  - Clé maître carte
  - Clé maître application
  - Clé maître de lecture
  - Clé maître d'écriture
  - Clé de lecture UID du badge
  - Vecteur(s) de diversification
  - Paramètres de diversification
  - Les identifiant privés
  - Les codes PIN
  - Les droits d'accès des porteurs de badge
  - Les historiques d'accès
  - Les historiques de modifications
  - Les secrets de connexion des exploitants
  - La politique de gestion de droits applicatifs
- Les éléments de sécurisation des communications
  - Les clés privées TLS
- Les éléments liés à de l'authentification
  - La clé privée pour la signature des JWT
  - Les secrets de connexion au système de gestion de base de données
- Les éléments logiciels sensibles :
  - Firmwares des concentrateurs XSecur'-Evo
  - Firmwares des UTP-SEC-EVO
  - Logiciels Xt Manager, AUTH, API REST
- Les droits applicatifs des exploitants
- Le système d'exploitation du Serveur CA

L'ensemble des biens sensibles liées au GAC sont sur le Serveur CA. Ce dernier étant dans une zone névralgique, il est soumis à l'ensemble des mesures organisationnelles et techniques assurant la sécurité du système sur lequel repose l'ensemble de ces données. **Les biens sensibles retenues dans le cadre de cette cible sont donc celles pouvant être menacées par une attaque via les fonctions de gestion ou via les différents réseaux**. A savoir :

- Toute donnée sensible de la base de données pouvant transiter sur le réseau (données de contrôle d'accès, secrets de connexion des exploitants)
- Les logiciels interagissant avec des équipements tiers (concentrateurs, postes clients, etc.)
- Les droits applicatifs des exploitants

4.2 Besoin de sécurité et emplacement des biens sensibles

Données Sensibles		Besoin de sécurité de la donnée :			Emplacement de la donnée :
		Confidentialité	Authenticité	Intégrité	
BS1	Clé maître de lecture	X	X	X	SAM-SE
BS2	Clé de lecture UID du badge	X	X	X	SAM-SE
BS3	Vecteur(s) de diversification	X	X	X	SAM-SE
BS4	Paramètres de diversification	X	X	X	SAM-SE sauf l'UID
BS5	ID Privé MIFARE® DESFire®	X	X	X	Concentrateur Serveur CA
BS6	Codes PIN	X		X	Concentrateur Serveur CA
BS7	Droits d'accès des porteurs	X		X	Concentrateur Serveur CA
BS8	Journaux d'événements	X		X	Concentrateur Serveur CA
BS9	Clé K SSCPv2	X	X*	X*	SAM-SE* Lecteur (EEPROM)
BS10	Clé K' SBus	X	X	X	UTP-SEC-EVO (Stockage diversifié) Concentrateur
BS11	Clé privée TLS	X	X	X	SAM-SE
BS12	Clé SCP03 UTP	X	X*	X*	SAM-SE* UTP-SEC-EVO
BS13	Clé SCP03 Concentrateur	X	X	X	SAM-SE Concentrateur
BS14	Firmware Concentrateur		X	X	Concentrateur
BS15	Firmware UTP-SEC-EVO	X	X	X	UTP-SEC-EVO
BS16	Certificats (dont autorité)	X	X	X	SAM-SE
BS17	Secrets de connexion	X	X*	X	Serveur CA Concentrateur*
BS18	Logiciels de gestion		X	X	Serveur CA
BS19	Droits des exploitants		X		Serveur CA
BS20	Système d'exploitation du Serveur CA			X	Serveur CA

5 DESCRIPTION DES MENACES

Les menaces auxquelles est exposée le Système de contrôle d'accès XSecur'-Evo peuvent être catégorisées en deux types :

- Les attaques physiques
- Les attaques logiques

Toute attaque en provenance de l'extérieur du périmètre de l'évaluation n'est pas prise en compte.

5.1 Profils des attaquants

Les attaquants potentiels du Système de contrôle d'accès XSecur'-Evo à considérer pour l'évaluation sont :

- Les porteurs de badge
- Les agents techniques et toute personne malveillante pouvant accéder physiquement aux éléments de l'UTL pour XSecur'-Evo alors qu'elle est en exploitation.
- Toute personne malveillante connectée sur le bus RS-485 reliant le concentrateur à l'UTP-SEC-EVO ou le lecteur à son interface (concentrateur ou UTP-SEC-EVO) et pouvant agir avec les éléments de la cible via leur port RS-485.
- Toute personne malveillante connectée au réseau support/fédérateur et pouvant agir avec le concentrateur via son interface réseau.
- Toute personne malveillante connectée au réseau du GAC.
- Les agents sûreté et toute personne malveillante pouvant interagir avec le GAC.

Le **Responsable sûreté** et les **administrateurs ne sont pas** considérés comme attaquants.

5.2 Synthèse des acteurs

ID	Type	Degré de confiance
U1	Administrateur	De confiance
U2	Responsable sûreté	De confiance
U3	Agent sûreté	Attaquant potentiel
U4	Agent technique	Attaquant potentiel
U5	Porteur de badge	Attaquant potentiel
U6	Attaquant sur bus et matériel terrain	Attaquant potentiel
U7	Attaquant sur le réseau fédérateur	Attaquant potentiel
U8	Attaquant sur le réseau GAC	Attaquant potentiel

5.3 Menaces physiques

Les attaques physiques considérées concernent :

- Le coffret de l'UTL contenant le concentrateur XSecur'-Evo
- Le coffret contenant le module déporté UTP-SEC-EVO
- La carte d'extension SAM-SE
- Les lecteurs-claviers compatibles

Les attaquants peuvent être soit hors site (avant déploiement et installation ou après fin de service et mise au rebut), soit externes (en zone publique), soit internes (en zone protégée) et ont un accès direct aux éléments.

5.3.1 Attaques sur un coffret contenant l'UTL pour XSecur'-Evo

Les attaques physiques sur le concentrateur pouvant porter préjudice au service offert par la solution de contrôle d'accès physique sont :

- L'ouverture mécanique ou l'arrachement du coffret abritant le concentrateur
- L'accès à l'applicatif de maintenance du concentrateur
- La cryptanalyse visant au déchiffrement des données sensibles
- L'extraction de code source
- L'exécution de code frauduleux
- La substitution d'une carte XSecur'-Evo
- L'émulation d'une carte XSecur'-Evo
- La substitution d'un SAM-SE
- L'émulation d'un SAM-SE

5.3.2 Attaques sur un coffret contenant le module UTP-SEC-EVO

Les attaques physiques sur le module UTP-SEC-EVO pouvant porter préjudice au service offert par la solution de contrôle d'accès physique sont :

- L'ouverture mécanique ou l'arrachement du coffret abritant la carte UTP-SEC-EVO
- La cryptanalyse visant au déchiffrement des données sensibles
- L'extraction de code source
- L'exécution de code frauduleux
- La substitution d'un module UTP-SEC-EVO
- L'émulation d'un module UTP-SEC-EVO
- La substitution d'une carte d'extension SAM-SE
- L'émulation d'une carte d'extension SAM-SE

5.3.3 Attaques sur un lecteur ou lecteur-clavier

Les attaques physiques sur le lecteur, lecteur-clavier pouvant porter préjudice au service offert par la solution de contrôle d'accès physique sont :

- L'ouverture mécanique ou l'arrachement du lecteur
- La cryptanalyse visant au déchiffrement des données sensibles
- L'extraction de code source
- L'extraction de données sensibles
- L'exécution de code frauduleux
- La substitution d'un lecteur-clavier
- L'émulation d'un lecteur-clavier
- L'authentification d'un badge via un système relai (attaque par relais)

5.4 Menaces logiques

Les attaques logiques considérées concernent :

- Le réseau du centre de gestion : communication Postes clients ←→ Serveur CA
- Les fonctions de gestion
- Les droits de gestion
- L'usurpation d'identité d'un serveur CA
- Le réseau support/fédérateur : communication Serveur CA/concentrateur XSecur'-Evo
- Les données contenues dans le concentrateur (base de données, journaux d'événements)
- La liaison filaire RS-485 :
    - Concentrateur XSecur'-Evo ←→ Lecteur RFID
    - Concentrateur XSecur'-Evo ←→ UTP-SEC-EVO
    - UTP-SEC-EVO ←→ Lecteur RFID
    - UTP-SEC-EVO ←→ UTP-SEC-EVO

Les attaques logiques pouvant porter préjudice au service offert par la solution de contrôle d'accès physique sont de type interception de données sensibles, injection de données ou abus de privilèges.

Les attaquants peuvent être soit externes (en zone publique), soit internes (en zone protégée) et disposent de moyens d'attaque évolués voire sophistiqués comme définis dans le tableau présent Annexe 3 : Niveau de sûreté et types de menaces :

- **Niveau III** : franchissement par attaque logique évoluée, préméditée de personnes initiées et équipées. L'attaquant possède du matériel spécifique facilement réalisable conçu à partir de connaissances recueillies à partir de l'examen d'un dispositif.

- **Niveau IV** : franchissement par attaque logique sophistiquée, préméditée de personnes initiées et fortement équipées et renseignées. L'attaquant possède du matériel spécifique de cryptanalyse conçu spécialement pour neutraliser la sûreté en place à partir de connaissances confidentielles sur la conception et l'exploitation du système.

5.4.1 Attaques logiques sur le réseau support/fédérateur

Les attaquants se trouvent en zone protégée, et sont connectés sur le réseau support ou fédérateur du client. Des moyens d'écoute ont été déployés.

Ecoute de transactions sur le réseau support/fédérateur	Menaces
Interception d'une transaction contenant l'ID Privé	Duplication du badge*
Interception d'une transaction contenant le PIN	Usurpation d'identité**
Interception d'une commande d'affectation de droits	Modification des droits d'accès d'un utilisateur ET création de droits
Interception d'une commande d'affectation de grille horaire	Modification des horaires d'accès d'un utilisateur
Interception d'instructions de configuration et de commande UTP	Ouverture de l'accès via rejeu d'une transaction
Corruption de Firmware	Injection et exécution de code frauduleux, non prévu ou non autorisé. Substitution d'un Firmware légitime par un Firmware frauduleux ensuite déployé par des moyens légitimes.
Interception des journaux d'événements à destination du serveur CA	Mise en défaut de la confidentialité des journaux d'événements
Interception des identifiants de connexion à l'applicatif de maintenance	Accès à l'interface de configuration et de mise à la clé du concentrateur

** : la duplication du badge n'est possible que si les paramètres MIFARE® DESFire® sont également connus.*
*** : l'usurpation d'identité n'est possible que si le code saisi l'est suite à la présentation du badge associé*

5.4.2 Attaques logiques sur la liaison bus terrain RS-485

Les attaquants se trouvent en zone protégée ou non protégée, et sont connectés sur la liaison filaire bus RS-485. Des moyens d'écoute ont été déployés.

Ecoute de transactions sur le réseau bus terrain RS-485	Menaces
Interception d'une transaction contenant l'ID Privé	Duplication du badge ET franchissement de l'accès via rejeu d'une transaction contenant un ID Privé
Interception d'une transaction contenant le PIN	Usurpation d'identité ET franchissement de l'accès via rejeu d'une transaction contenant un PIN
Interception d'une transaction contenant des paramètres MIFARE® DESFire®	Duplication du badge
Interception d'une transaction contenant une commande SSCPv2	Modification du comportement du lecteur via rejeu d'une transaction contenant une commande SSCPv2
Interception d'instructions de configuration et de commande	Ouverture de l'accès via rejeu d'une transaction
Corruption de Firmware	Injection et exécution de code frauduleux, non prévu ou non autorisé. Substitution d'un Firmware légitime par un Firmware frauduleux ensuite déployé par des moyens légitimes.

5.4.3 Usurpation d'identité du serveur CA

Les attaquants se trouvent en zone protégée et ont substitué le serveur CA légitime par un serveur frauduleux.

- Les attaquants détournent un certificat authentique de son usage prévu pour en faire un usage frauduleux.
- Les attaquants émettent un certificat frauduleux dans le but d'initier le dialogue avec le concentrateur en tentant d'usurper l'identité du serveur CA légitime.

Usurpation d'identité du serveur CA	Menaces
Interception d'une transaction contenant l'ID Privé	Duplication du badge ET franchissement de l'accès via rejeu d'une transaction contenant un ID Privé
Interception d'une transaction contenant le PIN	Usurpation d'identité ET franchissement de l'accès via rejeu d'une transaction contenant un PIN
Corruption de Firmware	Injection et exécution de code frauduleux, non prévu ou non autorisé. Substitution d'un Firmware légitime par un Firmware frauduleux ensuite déployé par des moyens légitimes.
Mise à jour frauduleuse	Attribution de droits d'accès non approuvés, suppression de droits d'accès légitimes.

5.4.4 Attaques logiques sur le réseau du centre de gestion

Les attaquants se trouvent en zone protégée, et sont connectés sur le réseau du centre de gestion. Des moyens d'écoute ont été déployés.

Ecoute de transactions sur le réseau fédérateur	Menaces
Interception d'une transaction contenant l'ID Privé	Duplication du badge
Interception d'une transaction contenant le PIN	Usurpation d'identité
Interception d'une commande d'affectation de droits	Modification des droits d'accès d'un utilisateur ET création de droits
Interception d'une commande d'affectation de grille horaire	Modification des horaires d'accès d'un utilisateur
Interception d'une transaction contenant une commande d'ouverture ponctuelle	Ouverture de l'accès via rejeu d'une transaction contenant une commande d'ouverture ponctuelle
Interception d'une transaction contenant une commande d'ouverture permanente	Ouverture de l'accès via rejeu d'une transaction contenant une commande d'ouverture permanente
Interception d'une transaction contenant les secrets de connexion d'un exploitant	Usurpation d'identité d'un exploitant. Elévation de privilèges
Interception d'une transaction contenant un jeton de session	Usurpation d'identité d'un exploitant. Elévation de privilèges
Interception des secrets d'encodage	Création de badges. Mise en défaut de la confidentialité des secrets d'encodage
Interception des journaux d'événements à destination du serveur CA	Mise en défaut de la confidentialité des journaux d'événements

5.4.5 Attaques logiques sur les fonctions de gestion

Les attaquants se trouvent en zone protégée et sont connectés sur le réseau du centre de gestion. Les attaquants tentent de réaliser des opérations malveillantes à l'encontre du logiciel de gestion des accès.

Attaques via les fonctions de gestion	Menaces
Corruption de la base de données (SQL Injection)	Modification des droits d'accès d'un utilisateur ET création de droits. Mise en défaut de la confidentialité des journaux d'événements. Elévation de privilèges
Corruption Logiciel (JS/XSS Injection, URL Parsing, Downgrade…)	Injection et exécution de code frauduleux, non prévu ou non autorisé

5.4.6 Abus de privilèges

Les attaquants font partie de l'organisation qui gère le contrôle d'accès du site (Agents sûreté). Ils possèdent en conséquence des droits d'exploitation sur les logiciels de gestion.

L'agent malveillant peut être tenté, de par ses droits, d'abuser de ses privilèges et de créer des badges illégitimes ou encore attribuer des droits illégitimes pour lui-même ou un autre acteur malveillant pour accéder à des zones sensibles.

5.5 Synthèse des menaces

ID	Menace	Interface d'attaque	Acteur de la menace
AP1	Attaques sur un coffret contenant l'UTL pour XSecur'-Evo	Coffret	U4, U6
AP2	Attaques sur un coffret contenant le module UTP-SEC-EVO	Coffret	U4, U6
AP3	Attaques sur un lecteur ou lecteur-clavier	Lecteur, Lecteur-Clavier	U4, U5, U6
AL1	Attaques logiques sur le réseau support/fédérateur	Interface de raccordement du GAC à l'UTL	U7
AL2	Attaques logiques sur la liaison bus terrain RS-485	Interface de raccordement de l'UTP-SEC-EVO au lecteur Interface de raccordement de l'UTL aux l'UTP-SEC-EVO	U4, U6
AL3	Usurpation d'identité du serveur CA	Communication avec l'UTL	U7
AL4	Attaques logiques sur le réseau du centre de gestion	Interface de raccordement entre les postes de gestion (postes clients) et le Serveur CA	U8
AL5	Attaques logiques sur les fonctions de gestion	Applications du GAC exposés sur le réseau	U3
AL6	Abus de privilèges	Droits applicatifs	U3

La synthèse des biens sensibles impactés par les menaces ci-dessus est détaillé au §7.2 Menaces et données sensibles.

6 DESCRIPTION DES FONCTIONS DE SECURITE

Les fonctions de sécurité offerte par le Système de contrôle d'accès XSecur'-Evo doivent permettre la sécurisation des accès physiques tout en conservant la confidentialité :

- Des identifiants nécessaires au déverrouillage d'accès : badges, PIN
- Des identifiants nécessaires à la gestion du contrôle d'accès
- Des échanges de données sur le réseau support / fédérateur
- Des échanges de données sur le réseau bus terrain
- Des échanges de données sur le réseau du centre de gestion

6.1 Fonctions de sécurité en réponse aux menaces physiques

6.1.1 Autoprotection des coffrets

Le coffret abritant le concentrateur XSecur'-Evo ainsi que celui abritant le module UTP-SEC-EVO déporté sont autoprotégés à l'ouverture par un mécanisme à lamelle ainsi qu'un accéléromètre. Ils sont également protégés à l'arrachement. Ces mécanismes sont supervisés par le concentrateur.

Le déclenchement de l'un de ces mécanismes ou la détection d'une tension basse du concentrateur (perte d'alimentation secteur et batterie en fin de charge), en dehors d'un contexte de maintenance prédéfini et connu de l'équipement déclenche la suppression des données sensibles contenues dans les éléments ci-après :

- Concentrateur XSecur'-Evo,
- Les cartes UTP-SEC-EVO qui lui sont raccordées.

Le déclenchement de ce mécanisme remonte une alarme au Serveur CA et rend inopérant les lecteurs.

6.1.2 Sécurisation de la carte d'extension SAM-SE

Le SAM-SE est situé en zone protégée ou névralgique. Il intègre un mécanisme d'anti-tamper NXP EAL6+.

Il intègre trois clés d'initialisation de dialogue afin de permettre l'authentification et l'échange de clés de sessions assurant l'établissement d'un canal sécurisé via le protocole SCP03 (cf. [6]).

En cas d'échec d'authentification ou d'erreur de communication, un défaut est remonté au Serveur CA.

6.1.3 Sécurisation du lecteur

Le lecteur est situé en zone publique. Il est supervisé par le Serveur CA et possède des mécanismes de protection à l'arrachement et à l'ouverture via accéléromètre. Cela permet la remontée d'événement de tentative de fraude au concentrateur XSecur'-Evo puis au Serveur CA.

Lorsqu'une tentative de fraude, est détectée sur le lecteur, il est mis en sécurité. Cela a pour conséquence de le rendre inactif lorsqu'un badge RFID lui est présenté et ce jusqu'à intervention de personnel habilité.

Il intègre une clé d'initialisation de dialogue afin de permettre l'authentification et l'échange d'une clé de session assurant l'établissement d'un canal sécurisé via les protocoles SSCPv2 (cf. [6]).

En cas de tentative d'attaque par relais sur le lecteur, la protection anti attaque par relais (Proximity Check) se déclenche, refuse l'authentification du badge exploité et notifie le Serveur CA.

En cas d'échec d'authentification ou d'erreur de communication, un défaut est remonté au Serveur CA.

6.2 Fonctions de sécurité en réponse aux menaces logiques

6.2.1 Protection des échanges de données par le protocole SCP03

Le protocole SCP03 établit un canal sécurisé par du chiffrement AES-128. Ces clés assurent la confidentialité et l'intégrité de tous les échanges entre le module UTP-SEC-EVO (Système ou déporté) et le SAM-SE, ainsi qu'entre le concentrateur et le SAM-SE.

L'authentification, la génération de clé de session, l'intégrité et la protection contre le rejeu sont assurés par les mécanismes reposants sur les algorithmes AES-CBC et CMAC (cf. [6]).

6.2.2 Protection des échanges de données par les protocoles SBus et SSCPv2

Les protocoles SBus et SSCPv2 établissent un canal sécurisé suite à une authentification mutuelle via secret partagé dont résultent les clés de session AES-128. Ces clés assurent la confidentialité de tous les échanges du concentrateur XSecur'-Evo jusqu'au lecteur.

L'authentification, l'échange de clé de session, l'intégrité et la protection contre le rejeu sont assurés par des mécanismes reposants sur les algorithmes AES-128, CBC-MAC et SHA256 (cf. [6]).

Ces protocoles interviennent dans la protection des échanges de données entre :

- Le concentrateur XSecur'-Evo et ses lecteurs (SSCPv2)
- Le module UTP-SEC-EVO et ses lecteurs (SSCPv2)
- Le concentrateur XSecur'-Evo et ses modules UTP-SEC-EVO (SBus)

6.2.3 Protection des échanges de données par le protocole TLS (Serveur CA – Concentrateur)

Le protocole TLS1.2 établit un canal sécurisé suite à une authentification mutuelle via certificats X509v3 dont résulte une clé de session AES-256. Cette clé permet d'assurer la confidentialité de tous les échanges entre le concentrateur XSecur'-Evo et le Serveur CA.

L'authentification, l'échange de clés de session, l'intégrité et la protection contre le rejeu sont assurées par le protocole TLS (cf. [6]).

Ce protocole intervient dans la protection des échanges de données entre le concentrateur XSecur'-Evo et le Serveur CA ainsi que dans la protection des échanges avec l'applicatif de maintenance du concentrateur.

6.2.4 Protection des Firmwares

Concernant les modules UTP-SEC-EVO, la protection des Firmwares est assurée en intégrité et en authenticité en amont de leur exécution par le matériel. Un mécanisme de protection en confidentialité vient également compléter la sécurité lors de la mise à jour des Firmwares dans le matériel. L'ensemble de ces mécanismes sont garantis par des algorithmes cryptographiques symétriques.

Les firmwares concentrateur XSecur'-Evo sont protégés en intégrité, en confidentialité et en authenticité lors de leur mise à jour dans le matériel grâce à l'utilisation d'un algorithme à clé publique et d'un algorithme de chiffrement symétrique.

Ces mécanismes sont décrits dans le document [6].

La mise à jour du concentrateur ou de l'UTP-SEC-EVO par un Firmware de version inférieure est impossible.

6.2.5 Protection des données du concentrateur

Les données du concentrateur sont stockées sur la mémoire flash au sein d'une partition protégée en confidentialité, intégrité et authenticité par un mécanisme de chaine de confiance reposant sur des primitives de chiffrement symétriques. La chaine de confiance repose sur un secret unique par unité de matériel, confidentiel et ne pouvant être lu.

Ces mécanismes sont décrits dans le document [6].

6.2.6 Vérification des certificats

Plusieurs tests, effectués à chaque utilisation des certificats, assurent l'intégrité, l'authenticité et l'usage non frauduleux de ces-derniers. Ces tests consistent en une vérification de la signature, une vérification de la CRL et une vérification des données du certificat (validité, durée de vie, SAN, utilisation et utilisation avancée de la clé) [6].

6.2.7 Authentification des équipements par le protocole RADIUS

L'authentification des équipements sur le réseau est assurée par la mise en œuvre du protocole RADIUS et le standard EAP-TLS via certificat. Le concentrateur XSecur'-Evo agit en tant que *supplicant* RADIUS, garantissant son authentification et son interopérabilité sur un réseau RADIUS.

6.2.8 Protection des échanges de données par le protocole TLS (Serveur CA – Poste client / Station d'encodage)

Le protocole TLS établit un canal sécurisé suite à une authentification via certificats X509v3 dont résulte une clé de session AES-256. Cette clé permet d'assurer la confidentialité de tous les échanges entre le Serveur CA et les postes clients ou le poste d'encodage.

L'authentification, l'échange de clés de session, l'intégrité et la protection contre le rejeu sont assurées par le protocole TLS (cf. [6]).

Ce protocole intervient dans la protection des échanges de données entre le Serveur CA et les postes clients ou le poste d'encodage.

6.2.9 Protection du logiciel

Les applicatifs Web, reposant sur une API REST, assurent un certain niveau de résistance aux attaques par l'exploitation d'un mapping objet-relationnel ainsi que par l'exploitation d'un Framework permettant, entre autres, l'échappement automatique du texte affiché.

Le serveur web est quant à lui configuré pour empêcher toute tentative de listage de répertoires et de traitement d'URLs non connus. Il est également configuré pour forcer l'utilisation du protocole HTTPS reposant exclusivement sur les versions TLS1.2 et 1.3 et dont les suites cryptographiques respectent les recommandations du guide ANSSI [4].

Les applicatifs Web sont également soumis à un contrôle d'intégrité reposant sur une comparaison d'un hash interne et d'un hash calculé à intervalle régulier. Cette comparaison est réalisée à chaque appel de l'API. En cas de hash différent, le logiciel retourne une erreur et devient inexploitable.

6.2.10 Authentification des exploitants

Tous les exploitants de l'application Xt Manager doivent se connecter à l'aide d'un identifiant et mot de passe. Ces identifiants peuvent être stockés localement en base de données ou issu d'un annuaire LDAP. Xt Manager est également compatible avec la solution OpenID Connect.

A l'issue d'une identification valide, l'exploitant se voit attribuer un token de session (JWT) signé (RS512) et limité dans le temps (durée configurable). Cf. [6]. A chaque requête à destination de l'API la validité du token de session est vérifiée.

Tous les exploitants de l'outil de maintenance du concentrateur doivent se connecter à l'aide d'un identifiant et mot de passe. Ces identifiants sont stockés de manières sécurisées sur le concentrateur par un mécanisme de chaine de confiance.

6.2.11 Gestion des droits applicatifs

Les droits applicatifs des exploitants sur Xt Manager peuvent être restreints aux strictes tâches qui leurs sont attribuées au travers de la fonctionnalité de gestion de droits matricielle. Ces droits sont détaillés dans l'Annexe 6 : Liste des tâches associées aux utilisateurs.

Ces droits applicatifs assurent l'authenticité des actions effectuées sur Xt Manager.

6.2.12 Cloisonnement des ressources du contrôle d'accès

La fonctionnalité de cloisonnement permet de restreindre le périmètre de ressources du contrôle d'accès (utilisateurs, droits d'accès…) sur lesquels les exploitants peuvent effectuer une action. Une gestion affinée permet d'éviter toute consultation/action concernant des accès à des zones sensibles ou des utilisateurs sensibles par des exploitants à droits restreints.

Ce cloisonnement assure l'authenticité des actions effectuées sur les ressources du contrôle d'accès du logiciel Xt Manager.

6.3 Synthèse des fonctions de sécurité

ID	Description	Argumentaire
FSP1	Autoprotection des coffrets	En cas de tentative de mise en œuvre d'AP1 et AP2 par les acteurs U4 et U6, le mode effraction supprimera les biens sensibles contenus dans les équipements du coffret et une alerte remontera au Serveur CA.
FSP2	Sécurisation de la carte d'extension SAM-SE	En cas de tentative de mise en œuvre d'AP1 et AP2 par les acteurs U4 et U6, le mécanisme anti-tamper du SAM-SE protègera de l'extraction des biens sensibles contenus dans le SE. De plus, le SAM-SE impose une authentification afin d'interagir avec, empêchant toute émulation ou substitution d'équipement. En cas d'événement anormal, une alerte remontera au Serveur CA.
FSP3	Sécurisation du lecteur	En cas de tentative de mise en œuvre d'AP3 par les acteurs U4, U5 et U6, le mécanisme de détection d'ouverture/arrachement rendra inopérant le lecteur jusqu'à intervention d'U1 et génèrera une alerte au Serveur CA. De plus, le lecteur impose une authentification afin d'interagir avec, empêchant toute émulation ou substitution d'équipement. Les acteurs malveillants tentant une attaque par relais seront bloqués par le mécanisme Proximity Check du lecteur.

ID	Description	Argumentaire
FSL1	Protection des échanges de données par le protocole SCP03	En cas de tentative de mise en œuvre d'AP1 et AP2 par les acteurs U4 et U6, la sécurisation des communications via le protocole SCP03 rendra inexploitable l'écoute des échanges avec le SAM-SE.
FSL2	Protection des échanges de données par les protocoles SBus et SSCPv2	En cas de tentative de mise en œuvre d'AL2 par les acteurs U4 et U6, la sécurisation des communications via le protocole SBus rendra inexploitable l'écoute des échanges entre l'UTL et l'UTP-SEC-EVO, et la sécurisation des communications via le protocole SSCPv2 rendra inexploitable l'écoute des échanges entre l'UTP-SEC-EVO et les lecteurs.
FSL3	Protection des échanges de données par le protocole TLS (Serveur CA – Concentrateur)	En cas de tentative de mise en œuvre d'AL1 et AL4 respectivement par les acteurs U7 et U8, la sécurisation des communications via le protocole TLS rendra inexploitable l'écoute des échanges entre le Serveur CA et l'UTL.
FSL4	Protection des Firmwares	En cas de tentative de mise en œuvre d'AL1 et AL3 par l'acteur U7, les équipements refuseront l'installation de firmwares de sources non reconnues ou de versions antérieures.
FSL5	Protection des données du concentrateur	En cas de tentative de mise en œuvre d'AP1 par les acteurs U4 et U6, la sécurisation des données du concentrateur empêchera l'exécution de code frauduleux ou l'extraction de biens sensibles.
FSL6	Vérification des certificats	En cas de tentative de mise en œuvre d'AL1 et AL3 par l'acteur U7, les équipements refuseront d'établir la communication avec des équipements possédant des certificats non conformes à l'ensemble des points de vérification.
FSL7	Authentification des équipements par le protocole RADIUS	En cas de tentative de mise en œuvre d'AL1 par l'acteur U7, le serveur RADIUS refusera d'authentifier des équipements malveillants empêchant ainsi U7 de tenter d'attaquer l'UTL (elle-même authentifiée) via le réseau.
FSL8	Protection des échanges de données par le protocole TLS (Serveur CA – Poste client / Station d'encodage)	En cas de tentative de mise en œuvre d'AL4 par l'acteur U8, la sécurisation des communications via le protocole TLS rendra inexploitable l'écoute des échanges entre le Serveur CA et le poste client ou la station d'encodage.
FSL9	Protection du logiciel	En cas de tentative de mise en œuvre d'AL5 par l'acteur U3, les applications du GAC bloqueront toute entrée frauduleuse, tout tentative de communication depuis des sources non déclarées ou utilisant des protocoles non sécurisés. De plus les applicatifs du GAC seront indisponibles en cas d'altération de l'empreinte de référence.
FSL10	Authentification des exploitants	En cas de tentative de mise en œuvre d'AL5 et AL6 par l'acteur U3, les applicatifs du Serveur CA refuseront toute action sans une authentification préalable. De plus la session est limitée dans le temps et sa validité est vérifiée à chaque interaction. En cas de tentative de mise en œuvre d'AP1 par les acteurs U4 et U6, l'applicatif de maintenance du concentrateur refusera toute action sans une authentification préalable
FSL11	Gestion des droits applicatifs	La politique de droits applicatifs réduit le champ d'action d'U3 aux strictes tâches qui lui sont attribuées empêchant l'accès aux biens sensibles qui sortent de son périmètre et ainsi empêchant la mise en œuvre d'AL5 et AL6
FSL12	Cloisonnement des ressources du contrôle d'accès	La politique de cloisonnement des ressources du contrôle d'accès réduit le champ d'action d'U3 aux strictes ressources qui lui sont autorisés empêchant la mise en œuvre d'AL5 et AL6.

7 MATRICES DE COUVERTURE

7.1 Menaces et fonctions de sécurité

Le tableau ci-dessous met en exergue les fonctions de sécurité mises en œuvre par le Système de contrôle d'accès XSecur'-Evo afin de déjouer les menaces répertoriées :

Menaces et Fonctions de Sécurité		Attaques sur un coffret UTL contenant l' XSecur' -Evo	Attaques sur un coffret contenant le module UTP-SEC-EVO	Attaques sur un lecteur ou lecteur-clavier	Attaques logiques sur le réseau support/fédérateur	Attaques logiques sur la liaison bus terrain RS-485	Usurpation d' identité du serveur CA	Attaques logiques sur le réseau du centre de gestion	Attaques logiques sur les fonctions de gestion	Abus de privilèges
		AP1	AP2	AP3	AL1	AL2	AL3	AL4	AL5	AL6
Autoprotection des coffrets	FSP1	X	X							
Sécurisation de la carte d'extension SAM-SE	FSP2	X	X							
Sécurisation du lecteur	FSP3			X						
Protection des échanges de données par le protocole SCP03	FSL1	X	X							
Protection des échanges de données par les protocoles SBus et SSCPv2	FSL2					X				
Protection des échanges de données par le protocole TLS (Serveur CA – Concentrateur)	FSL3				X			X		
Protection des Firmwares	FSL4				X		X			
Protection des données du concentrateur	FSL5	X								
Vérification des certificats	FSL6				X		X			
Authentification des équipements par le protocole RADIUS	FSL7				X					
Protection des échanges de données par le protocole TLS (Serveur CA – Poste client)	FSL8							X		
Protection du logiciel	FSL9								X	
Authentification des exploitants	FSL10	X							X	X
Gestion des droits applicatifs	FSL11								X	X
Cloisonnement des ressources du contrôle d'accès	FSL12								X	X

7.2 Menaces et données sensibles

Le tableau ci-dessous met en exergue les données sensibles contenues dans le Système de contrôle d'accès XSecur'-Evo vulnérables face aux menaces répertoriées :

Menaces et Données Sensibles		Attaques sur un coffret UTL contenant l' XSecur' -Evo	Attaques sur un coffret contenant le module UTP-SEC-EVO	Attaques sur un lecteur ou lecteur-clavier	Attaques logiques sur le réseau support/fédérateur	Attaques logiques sur la liaison bus terrain RS-485	Usurpation d' identité du serveur CA	Attaques logiques sur le réseau du centre de gestion	Attaques logiques sur les fonctions de gestion	Abus de privilèges
		AP1	AP2	AP3	AL1	AL2	AL3	AL4	AL5	AL6
Clé maître de lecture	BS1	X	X					X	X	
Clé de lecture UID du badge	BS2	X	X					X	X	
Vecteur(s) de diversification	BS3	X	X					X	X	
Paramètres de diversification	BS4	X	X					X	X	
ID Privé MIFARE® DESFire®	BS5	X			X	X	X	X	X	
Codes PIN	BS6	X			X	X	X	X	X	
Droits d'accès des porteurs	BS7	X			X		X	X	X	
Journaux d'événements	BS8	X			X		X	X	X	
Clé K SSCPv2	BS9	X	X	X						
Clé K' SBus	BS10	X	X							
Clé privée TLS	BS11	X								
Clé SCP03 UTP	BS12	X	X							
Clé SCP03 Concentrateur	BS13	X								
Firmware Concentrateur	BS14	X			X		X			
Firmware UTP-SEC-EVO	BS15	X	X		X	X	X			
Certificats (dont autorité)	BS16	X								
Secrets de connexion	BS17	X						X	X	
Logiciels de gestion	BS18								X	
Droits des exploitants	BS19								X	X
Système d'exploitation Serveur CA	BS20								X	

8 SURFACE D'ATTAQUE

La synthèse des interfaces vers les fonctions du produit sont détaillés dans [11].

ANNEXES

Annexe 1 : Configuration n°1, hautement recommandée

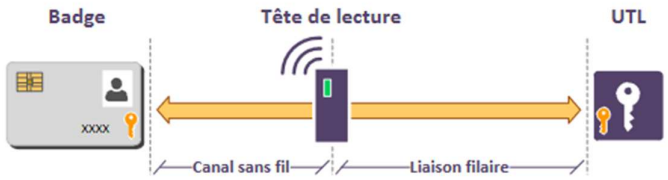

FIGURE 13 – Configuration type n°1 : tête de lecture transparente, authentification de bout en bout

Annexe 2 : Badges : niveaux de sûreté, résistance aux attaques logiques

Niveaux de sûreté	Niveaux de résistance aux attaques logiques	Méthode d'authentification	Technologies
I	-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés, cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.
II	L1	Authentification reposant sur une clé commune ; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES [43]).	Cartes ISO14443, authentification à cryptographie symétrique.
III	L2	Authentification du badge reposant sur une clé dérivée d'une clé maîtresse ou sur une bi-clé asymétrique ; Mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [18]).	Cartes ISO14443, authentification à cryptographie symétrique ou asymétrique.
IV	L3	Authentification du badge reposant sur une clé dérivée d'une clé maîtresse ou sur une bi-clé asymétrique ; Mécanismes conformes aux référentiels cryptographiques recommandés par l'ANSSI (Annexe B1 du RGS [18]) ; Authentification du porteur par un second facteur (information mémorisée ou élément biométrique).	Cartes ISO14443, authentification à cryptographie symétrique ou asymétrique ; Saisie d'un code mémorisé ou d'un élément biométrique.

TABLE 3 – Correspondance entre niveau de sûreté et niveau de résistance aux attaques logiques

Annexe 3 : Niveau de sûreté et types de menaces

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

TABLE 2 – Les quatre niveaux de sûreté

Annexe 4 : Références des concentrateurs de la Gamme d'UTL pour XSecur'-Evo

Réf. Synchronic	Type Concentrateur	Description
3A-XSECURxx-3B-EVO	XP02	UTL en Coffret Alimenté
3A-XSECURxx-BQ-EVO	XP02	UTL en Coffret Alimenté
3A-XSECURxx-EVO	XL02	UTL en Coffret Alimenté
3P-XSECURxx-EVO	XL02	UTL en Coffret non alimenté UTL-POE
CN-XSECUR-3B-EVO	XP02	Carte Nue : UTL seule
CN-XSECUR-EVO	XL02	Carte Nue : UTL seule
CN-XSECURxx-BQ-EVO	XP02	Carte Nue : UTL seule

xx : coffret dans lequel le matériel est intégré

Annexe 5 : Références des lecteurs compatibles

Référence Synchronic	Référence STid	Lecteur	Etroit	Clavier
31-TCLDS-485	ARC-W33-B-PH5-7AD-y	**X**		**X**
31-TPRDS-485	ARC-W33-A-PH5-7AD-y	**X**		
31-TPRDSA1-485	ARC1-W33-B-PH5-7AD-y	**X**	**X**	

y : personnalisation de la coque du lecteur (couleur/motif/texture)

Annexe 6 : Liste des tâches associées aux utilisateurs

Exploitant - Agent sûreté

L'Agent sûreté du système réalise les tâches suivantes :

- Ajout, suppression, modifications des droits d'accès à un porteur de badge pour des accès dits non sensibles
- Envoi des droits mis à jour vers les concentrateurs
- Enrôlement d'un badge et délivrance à un porteur ayant des droits d'accès restreints
- Consultation des historiques d'accès des porteurs de badges ayant des droits d'accès restreints

Exploitant - Responsable sureté

Le Responsable sureté correspond à un agent sûreté à responsabilité. Il réalise les mêmes tâches qu'un agent sûreté mais pour des accès sensibles ou des porteurs de badges ayant des droits d'accès sensibles :

- Ajout, suppression, modifications des droits d'accès à un porteur de badge pour des accès dits sensibles
- Envoi des droits mis à jour vers les concentrateurs
- Enrôlement d'un badge et délivrance à un porteur ayant des droits d'accès sensibles
- Consultation des historiques d'accès des porteurs de badges

Administrateur

L'administrateur du système réalise les tâches suivantes :

- Déclaration des équipements terrain sur le serveur CA
- Maintien en conditions opérationnelles des applications du GAC
- Mise à jour du firmware des concentrateurs et des UTP-SEC-EVO
- Octroi des habilitations d'accès des exploitants aux applications du GAC.
- Déclenchement du mode de maintenance du concentrateur XSecur'-Evo pour accès physique par l'agent technique et connexion logique à ce dernier pour maintenance.
- Encodage d'un badge pour mise à la clé en vue de sa délivrance à un porteur par l'agent sûreté ou le Responsable sûreté
- Programmation des SAM-SE en vue de leur déploiement physique par l'agent technique
- Mise à la clé des équipements terrain
- Consultation de l'ensemble des journaux d'événements techniques générés par la solution

Agent technique

L'agent technique réalise les tâches suivantes :

- Déploiement et maintenance physique des équipements terrain
- Déploiement physique des SAM-SE dans les concentrateurs et les UTP-SEC-EVO

Porteur de badge

Le porteur de badge réalise les tâches suivantes :

- Utilisation courante du badge et PIN mis à sa disposition dans le respect de la politique de sureté définie par le client final
- Déclaration dans les plus brefs délais de toute perte ou suspicion de compromission de son ou ses moyens d'accès.

Annexe 7 : Dispositifs USB d'encodage compatibles

Référence Synchronic	Référence Fabricant
31-USB-XT	HID® OMNIKEY® 5022 CL
31-USB-XT2	SpringCard Prox'N'Roll
31-USB-XT3	SpringCard Puck Base
31-USB-XT4	SpringCard Puck One
31-UTP-USB125K	HID® OMNIKEY® 5427 CK

Synchronic fabricant Français - présent en France et à l'Export – Toutes les coordonnées indiquées sur www.synchronic.fr