FABRICANT FRANÇAIS DE SÉCURITÉ ÉLECTRONIQUE

Cible de sécurité

UTL pour XSecur'-Evo

V2.10

Référence : SYN-CIBLE-XSECUR-EVO-2.10

Date : mercredi 11 mai 2022

Synchronic

Historique des versions

Version	Date	Auteur	Description des modifications
V1.05	18/07/2018	Laurent GALVAN	Cible de sécurité CSPN - XSecur'
V2.00	02/04/2020	Paul VAUTIER	Cible de sécurité XSecur'-Evo
V2.01	19/05/2020	Paul VAUTIER	Modifications suite commentaires ANSSI
V2.02	22/07/2020	Paul VAUTIER	Modifications suite commentaires ANSSI
V2.03	20/10/2020	Antoine PROVOT	Modifications SBUS
V2.04	12/03/2021	Paul VAUTIER	Correction suite retour CCN + relecture CESTI
V2.05	16/04/2021	Paul VAUTIER	Mise à jour des versions
V2.06	23/11/2021	Antoine PROVOT	Modifications suite commentaires CESTI
V2.07	05/01/2022	Antoine PROVOT	Modifications suite commentaires CESTI
V2.08-V2.09	09/05/2022	Thomas BELTRANDO	Modifications suite commentaires CESTI
V2.10	11/05/2022	Thomas BELTRANDO	Modifications suite commentaires CESTI

Diffusion

Prénom	Nom	Société	Fonction
Alexandre	GEAY	ANSSI	Bureau de Qualification
Chrysanthi	MAVROMATI	ANSSI	Centre de Certification
Laurent	GALVAN	SYNCHRONIC	Directeur Technique Adjoint
Charles	PARMENTIER	SYNCHRONIC	Ingénieur Développement Cryptographie
Thomas	BELTRANDO	SYNCHRONIC	Ingénieur Recherche & Développement Embarqué

Copyright

Le présent document est la propriété exclusive de :

SYNCHRONIC SAS
au capital de 1 000 000 €
RCS Rouen B344 539 564
APE 6202A

Adresse du siège social :
393 rue des Manets
ZAC des champs fleuris
76520 Franqueville-Saint-Pierre

Tél : 02 35 08 58 50 / Fax : 02 32 83 00 50
www.synchronic.fr

Les marques mentionnées dans ce document appartiennent à leurs propriétaires respectifs. Copyright © SYNCHRONIC 2022

Sommaire

1 INTRODUCTION

1.1 Identification de la cible de sécurité

Le présent document constitue la cible de sécurité de la gamme de produits UTL pour XSecur'-Evo . Cette cible a été élaborée en vue de l'obtention de la Qualification de niveau élémentaire délivrée par l'ANSSI dans la catégorie identification, authentification et contrôle des accès physiques.

1.2 Identification du produit

Catégorie	Description / Lien
Fabricant	SYNCHRONIC
Dénomination commerciale du produit	UTL pour XSecur'-Evo
Version du produit évalué	1.1
Site du fabricant	http://www.synchronic.fr
Catégorie du produit	Identification, authentification et contrôle des accès physiques

1.3 Glossaire et références

1.3.1 Glossaire

Terme	Désignation
AD	Active Directory
AES	Advanced Encryption Standard, algorithme de chiffrement symétrique
aiR'Evolution	Suite de logiciels permettant la configuration et l'exploitation des produits de la gamme XPert
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP	Auto-Protection
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®	DES, Fast, Innovative, Reliable, and Enhanced supportant AES-128
FID	Numéro de fichier d'application MIFARE® DESFire®
GAC	Système de Gestion des Accès Contrôlés. Aussi appelé Unité de Traitement de Supervision (UTS)
HMAC	Hash Message Authentication Code
MAC-UT	Media Access Control UT : adresse unique d'une carte unité de traitement
Mapping	Structure des données d'une puce MIFARE® DESFire®
NPS	Network Policy Server
PIN	Personal Identification Number
RADIUS	Remote Authentication Dial-In User Service
RFID	Radio Frequency IDentification
SAM	Secure Access Module
SE	Secure Element : Plateforme matérielle sécurisée pouvant stocker et traiter des données en respectant un niveau d'exigence fixé.
Secur'Evolution	Logiciel de génération de fichiers de configuration de lecture RFID
SBus	Secure Bus Protocol
SSCPv2	STid Secure Common Protocol version 2
TCLDS-485	Lecteur RFID 13,56MHz avec clavier RS-485
TLS	Transport Layer Security, protocole de sécurisation d'échanges TCP/IP
UID	Unique IDentifier
UTL	Unité de Traitement Locale
UTP-SEC-EVO	Unité de Traitement de Porte Sécurisée acceptant une extension SAM-SE
SI	System Identifier

1.3.2 Références

N°	source	Description / lien
[1]	ANSSI	https://www.ssi.gouv.fr/uploads/2020/03/anssi-guide-recommandations_securisation_systemes_controle_acces_physique_et_videoprotection-v2.0.pdf
[2]	ANSSI	https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf
[3]	NXP	http://www.nxp.com/documents/application_note/AN10922.pdf
[4]	ANSSI	https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf
[5]	ANSSI	https://www.ssi.gouv.fr/uploads/2018/08/guide_802.1x_anssi_pa_043_v1.pdf
[6]	SYNCHRONIC	SYN-DES-MEC-CRY-XSECUR-EVO.pdf

2 ARGUMENTAIRE DU PRODUIT

2.1 Description générale du produit

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 et s'interface avec le système d'information de gestion des accès contrôlés (GAC) via une liaison TCP/IP. Son usage se destine aux sites industriels, tertiaires, militaires, aux administrations et aux banques. L'ensemble **GAC** et **UTL pour XSecur'-Evo** constitue la solution complète de Contrôle d'accès Synchronic dite « **Solution XSecur'-Evo** ».

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 de base de données
  - Le Serveur CA comprenant les logiciels de gestion/exploitation
  - Le Serveur de Certificats (non fourni par Synchronic)
  - Le Serveur RADIUS (non fourni par Synchronic)
  - Les postes clients
  - Les stations d'encodage
  - Les stations de programmation SAM-SE

- L' « **UTL pour XSecur'-Evo »**, composé des équipements terrain :
  - Les concentrateurs d'accès de la gamme d'UTL pour XSecur'-Evo (cf. §8.4 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. §8.5 Annexe 5 : Références des lecteurs compatibles)
  - Les badges MIFARE® DESFire® EV2

Seule l'UTL pour XSecur'-Evo fait l'objet de la démarche de qualification concernée par la présente cible de sécurité (cf. §3.1 Description du périmètre d'évaluation).

2.1.2 Schéma d'architecture de la solution

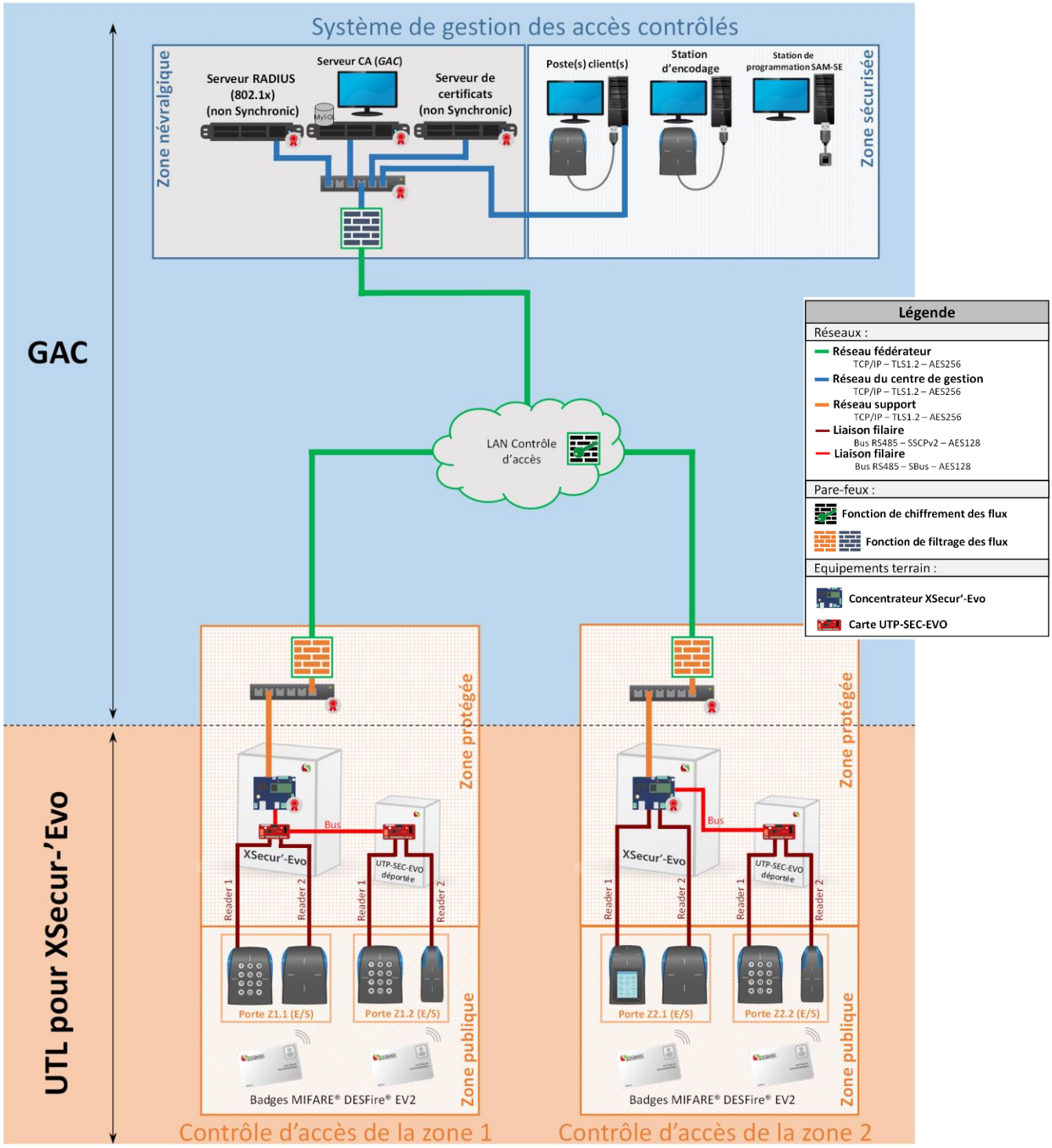

Figure 1 : exemple de schéma d'architecture de l'UTL pour XSecur'-Evo avec son GAC

2.1.3 Description fonctionnelle de la solution

L'UTL pour 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 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 « *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection* » [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 sur un Serveur CA, un Serveur de Certificats, un Serveur RADIUS (802.1X), de(s) poste(s) client(s), une station d'encodage, une station de programmation des SAM-SE, un concentrateur XSecur'-Evo, des modules de portes UTP-SEC-EVO, des têtes de lecture ou lecture/clavier et des badges. La partie GAC ainsi que le concentrateur XSecur'-Evo sont interconnectés sur le réseau Ethernet client tandis que la partie terrain est interconnectée 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. Combiné à une alimentation secourue, elle est aussi au plus proche du concentrateur, l'UTL pour XSecur'-Evo bénéficie d'une grande résilience.

Pour accéder à une zone protégée, l'utilisateur final de la solution, appelé porteur de badge, place son badge de type RFID MIFARE® DESFire® EV2 dans le champ électromagnétique du lecteur. L'authentification du badge est assurée par la robustesse des mécanismes cryptographiques de la technologie MIFARE® DESFire® EV2. 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 l'architecture n°1 hautement recommandée du guide contrôle d'accès de l'ANSSI [1] (cf. §8.1 Annexe 1 : Architecture n°1, hautement recommandée).

2.1.4 Description des réseaux

2.1.4.1 Description du réseau fédérateur

Le réseau fédérateur constitue le réseau local Ethernet TCP/IP du client final sur lequel sont interconnectés les éléments du GAC de la solution XSecur'-Evo, à savoir le Serveur CA, le Serveur de Certificats, le Serveur RADIUS (802.1X), les postes clients ainsi que les concentrateurs XSecur'-Evo. Son déploiement, sa mise en œuvre et sa maintenance sont assurés par le client final.

Ce réseau permet la configuration, l'exploitation et la maintenance de l'UTL pour XSecur'-Evo via la suite logicielle aiR'Evolution présente sur le Serveur CA et les postes clients. Les échanges de données entre le serveur CA et les concentrateurs sont sécurisés via le protocole TLSv1.2 selon les « *Recommandations de sécurité relatives à TLS* » [4].

Le **réseau fédérateur** n'est **pas inclus** dans le périmètre de l'évaluation à l'exception de l'interconnexion du concentrateur XSecur'-Evo sur ce réseau.

2.1.4.2 Description du réseau bus terrain RS-485

Le réseau bus terrain constitue un réseau composé de liaisons filaires bus terrain RS-485 dédié 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 ce réseau. Aucun autre équipement à l'exception de ceux cités précédemment n'est raccordé au réseau bus terrain.

Ce réseau est situé dans la zone de sécurité protégée par l'UTL pour XSecur'-Evo. Les échanges de données sur ce réseau sont sécurisés via les protocoles SBus et SSCPv2, tel que décrit dans la « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo*» [6].

Le **réseau bus terrain RS-485** est **inclus** dans le périmètre de l'évaluation.

2.1.5 Description du GAC

2.1.5.1 Description du Serveur CA

Le Serveur CA a pour rôle la configuration et l'administration de la solution contrôle d'accès physique XSecur'-Evo dans son intégralité via les applicatifs métiers développés par Synchronic et constituant la suite aiR'Evolution. Le poste Serveur CA est composé d'un serveur informatique sous système d'exploitation Windows Serveur 2012 R2, 2016 ou 2019. Il héberge la base de données (MySQL ou SQLServer ou SQL Express ou MariaDB). Le Serveur CA peut être virtualisé dans le SI client, il sera dans cette configuration déployé en machine virtuelle sur serveur.

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 peut assurer la diffusion des secrets nécessaires aux concentrateurs XSecur'-Evo afin d'établir le dialogue avec les lecteurs ainsi que les paramétrages MIFARE® DESFire® (dont les clés cryptographiques) pour un fonctionnement en mode « transparent ».

Le Serveur CA est protégé par une solution antivirus éprouvée. Les mises à jour y sont régulièrement déployées, 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 présentes dans la note technique « *Recommandations de sécurité relatives aux mots de passe* » de l'ANSSI [2] en ce qui concerne à la fois l'ensemble de ses mots de passe SI et les mots de passe des éléments de la solution XSecur'-Evo.

Un compte administrateur bénéficiant de tous les droits de configuration et d'exploitation ainsi qu'un compte exploitant bénéficiant des droits restreints d'exploitation courante 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** n'est **pas inclus** dans le périmètre de l'évaluation.

2.1.5.2 Description du Serveur de Certificats

Le Serveur de Certificats a pour rôle l'émission de certificats pour la mise en œuvre de la sécurisation de l'ensemble des éléments de la solution XSecur'-Evo, avec gestion des demandes de signature de certificat (*CSR*) conforme à la spécification PKCS#10. Celui-ci est également chargé de maintenir à jour et de publier la liste de révocation de certificats *(CRL)*. Ce serveur n'est pas fourni avec la solution XSecur'-Evo mais par le client. Sa configuration, son exploitation et son administration sont donc de la responsabilité du client final.

Le **Serveur de Certificats** n'est **pas inclus** dans le périmètre de l'évaluation.

2.1.5.3 Description du Serveur RADIUS (802.1X)

Le Serveur de RADIUS a pour rôle d'identifier tous les équipements se connectant sur le réseau fédérateur. Ceci permet de s'assurer que seuls les équipements autorisés accèdent à ce réseau. Les équipements réseaux actifs réalisent une isolation physique de leur port sur lequel un équipement non autorisé est connecté.

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

2.1.5.4 Description du poste client

Le poste client a pour rôle l'exploitation de la gestion du contrôle d'accès physique à l'aide de la suite logicielle aiR'Evolution. 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 un protocole HTTPS (TLSv1.2).

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 permet également la définition des paramètres de lecture utilisés par les lecteurs raccordés aux concentrateurs. Il autorise la définition de deux configurations de lecture distinctes par lecteur afin de faciliter entre autre la gestion transitoire d'une migration technologique des badges du client ou la révocation de clés.

Le poste client est protégé par une solution antivirus éprouvée. Les mises à jour y sont régulièrement déployées, 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 présentes dans la note technique « *Recommandations de sécurité relatives aux mots de passe* » de l'ANSSI [2] en ce qui concerne à la fois l'ensemble de ses mots de passe SI et les mots de passe des éléments de la solution XSecur'-Evo.

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

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

2.1.5.5 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 MIFARE® DESFire® EV2. Lors de la rédaction de ce document les modèles d'équipement USB d'encodage ARC-W35-G/PH5-5AA et ARC-W35-G/BT1-5AA sont supportés par la solution. Il est recommandé que cette station soit hors réseau.

Les **stations d'encodage** ne sont **pas incluses** dans le périmètre de l'évaluation.

2.1.5.6 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. 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.

Les **stations de programmation SAM-SE** ne sont **pas incluses** dans le périmètre de l'évaluation.

2.1.6 Description des équipements terrain

2.1.6.1 Description du concentrateur XSecur'-Evo

Le concentrateur XSecur'-Evo a pour rôle de vérifier les droits d'accès des porteurs de badge MIFARE® DESFire® EV2 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 100 000 identifiants distincts. Afin de remplir son rôle, un concentrateur XSecur'-Evo n'est pas dépendant de la disponibilité du réseau fédérateur et n'a donc pas la nécessité d'être en communication avec le Serveur CA pour autoriser le franchissement d'accès.

Les données sensibles du concentrateur sont stockées sur une partition chiffrée dont les caractéristiques sont décrites dans la documentation « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo*» [6].

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/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 NXP de référence SE050 amovible 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 MIFARE® DESFire® EV2.

Cet ensemble est usuellement appelé dans le domaine du contrôle d'accès 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.

La sécurisation des échanges entre l'UTL et les lecteurs est assurée par le protocole SSCPv2 dont les caractéristiques sont décrites dans la documentation « *Description des mécanismes cryptographiques de l'UTL pour 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 TLSv1.2 respectant les recommandations de sécurité relatives à TLS [4]. Un certificat d'initialisation de la communication est assigné d'usine et doit être personnalisé par le client. Cette personnalisation s'appuie sur la génération d'une CSR transmise à l'autorité de certification qui va générer sur cette base un certificat signé qui devra être ensuite injecté dans le concentrateur.

L'interfaçage du concentrateur XSecur'-Evo sur le réseau fédérateur est compatible avec la mise en œuvre du standard 802.1X tel que décrit dans le guide de « *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux* » [5] et requiert un serveur d'authentification RADIUS.

Les secrets MIFARE® DESFire® de la solution peuvent soit être injectés par le déploiement de carte d'extension SAM-SE soit diffusés depuis le Serveur CA. Lors d'une diffusion centralisée, la sécurisation du fichier de configuration des secrets MIFARE® DESFire®, généré par l'applicatif Secur'Evolution, est assurée par une clé privée AES-128. Une clé de déchiffrement du fichier de configuration est assignée d'usine et est stockée dans le SAM-SE. Le chiffrement de ce fichier de configuration permet une plus grande souplesse de la gestion des clés par les responsables sécurité. Cela permet des opérations de diffusion de configuration des secrets sans compromettre la confidentialité de son contenu. Cette clé de déchiffrement doit être personnalisée avant la mise en exploitation de l'UTL pour XSecur'-Evo par le client final.

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 documentation « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo*» [6].

Le concentrateur XSecur'-Evo, usuellement situé en zone protégée (voire en zone névralgique), 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. La confidentialité des clés et des paramètres MIFARE® DESFire® est assurée dans le concentrateur XSecur'-Evo par leur stockage dans le SAM-SE.

Information	Description
Dénomination	Gamme XSecur'-Evo (cf. 8.4 Annexe 4 : Références des concentrateurs de la Gamme d'UTL pour XSecur'-Evo
Dénomination technique	XL02-v7 / XP02-v5a (A5_SOCKET-V6)
Version noyau	V6-01-00 (Linux 4.14)
Version logicielle (Concentrateur XSecur'-Evo / Module UTP-SEC-EVO / Module TLS)	V13-44-51 / V4-08-00 / V2-29-00
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 d'ouverture double (lamelle et accéléromètre sur la face interne du capot) et d'arrachement du coffret

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

2.1.6.2 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 via le protocole SCP03. La clé d'authentification SCP03 du SAM-SE est unique, généré aléatoirement et inextractible 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 Secur'Evolution, clé SCP03, clé K
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.

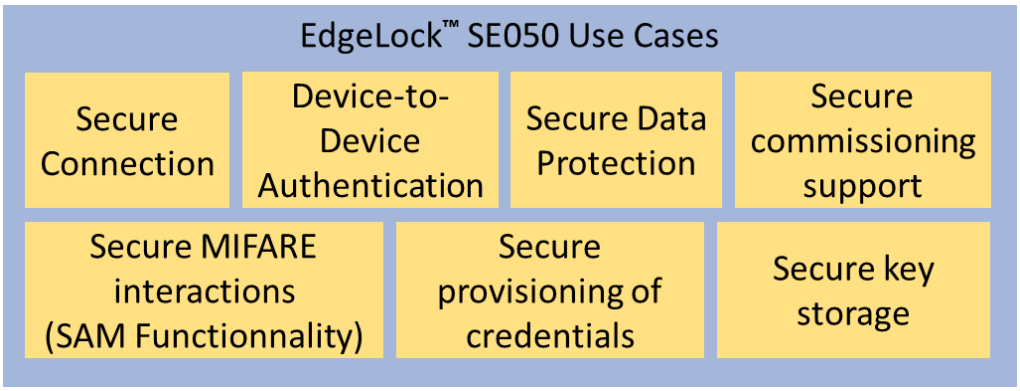

Figure 2 : Diagramme des cas d'usage SE050

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

2.1.6.3 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 documentation « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo*» [6].

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

2.1.6.4 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. §8.5 Annexe 5 : Références des lecteurs compatibles).

Le lecteur ou lecteur/clavier a pour rôle de transmettre les échanges RFID entre le badge MIFARE® DESFire® EV2 et le module UTP-SEC-EVO. Ils fonctionnent en mode « transparent », et permettent d'authentifier le badge et le porteur du badge par saisie d'un code PIN en complément de la présentation de son badge d'accès.

Information	Description
Dénomination	Gamme STid 7AD
Dénomination technique	Cf. 8.5 Annexe 5 : Références des lecteurs compatibles
Version logicielle	Z16
Microcontrôleur	NXP cortex M4
Emplacement	Zone publique ou zone protégée
Données	Clé K en EEPROM
AP	Accéléromètre et arrachement

Les **lecteurs** et **lecteur/clavier** sont **inclus** dans le périmètre de l'évaluation.

2.1.6.5 Description du badge MIFARE® DESFire® EV2

Le badge MIFARE® DESFire® EV2 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. 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'environnement d'utilisation du produit

Afin de répondre aux problématiques de lecture frauduleuse et de duplication de badge, le marché du contrôle d'accès a fait évoluer les technologies RFID.

- Dans un premier temps les badges disposaient uniquement d'un numéro de série public
- Dans un second temps les badges ont été dotés d'une mémoire inscriptible afin de personnaliser l'identifiant de son porteur. Ces mécanismes d'inscription et de lecture d'identifiant personnalisé (ID Privé) ont été intégrés en sécurisant l'accès à cette mémoire libre avec des mécanismes cryptographiques propriétaires puis publics.

La solution de contrôle d'accès physique XSecur'-Evo intègre les recommandations ANSSI présentes dans le guide « *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection* » [1]. Les lecteurs proposés dans le périmètre sont munis, en plus de la fonctionnalité RFID, d'un moyen d'authentification du porteur du badge.

L'architecture mise en œuvre correspond à l'architecture « Configuration type n°1 » du guide susmentionné, 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.

L'UTL pour XSecur'-Evo a pour vocation de sécuriser les accès physiques de locaux industriels, tertiaires, bancaires et des administrations.

2.3 Description de l'utilisation courante du produit

L'UTL pour XSecur'-Evo est basée sur l'utilisation de badges MIFARE® DESFire® EV2. 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].

2.3.1 Badge

Le porteur de badge positionne son badge dans le champ électromagnétique du lecteur contrôlant l'accès qu'il souhaite franchir. Le lecteur 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 badge transmet cet UID et l'ID Privé chiffré en AES-128 au lecteur via la liaison filaire RS-485 utilisant le protocole SSCPv2.

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.

Cet événement de lecture contenant l'ID Privé est simultanément inscrit dans les journaux locaux au concentrateur ainsi que remonté via sécurisation TLSv1.2 pour historisation sur le Serveur CA par le biais du réseau fédérateur.

Afin d'assurer une transition temporelle de révocation de clé de lecture MIFARE® DESFire® ou de pouvoir déchiffrer les ID Privés de deux populations de badges distinctes, l'UTL pour XSecur'-Evo permet la lecture d'une double configuration de paramètres MIFARE® DESFire®. Cette double configuration est paramétrable par lecteur.

2.3.2 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® EV2, 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 TLSv1.2 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.

2.4 Description des utilisateurs typiques

2.4.1 Les Exploitants et Administrateurs

Les exploitants et 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. §8.6 Annexe 6 : Liste des tâches associées aux utilisateurs). Par ailleurs, les exploitants et administrateurs 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.

2.4.2 Les 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. §8.6 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. *DU XSecur'-Evo*).

2.4.3 Les Porteurs de Badge

Les porteurs de badge de la solution XSecur'-Evo sont toutes les personnes utilisatrices du dispositif de contrôle d'accès physique du client (cf. §8.6 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 sécurisées voire névralgiques grâce :

- Au badge RFID de technologie MIFARE® DESFire® EV2 remis par le service sûreté du client
- Optionnellement au code PIN personnalisé par le porteur de badge. Ce second facteur d'authentification est réservé aux accès contrôlés par la solution devant se conformer au niveau de sûreté IV défini dans le guide de l'ANSSI [1]. (cf. §8.2 Annexe 2 : Badges : niveaux de sûreté, résistance aux attaques logiques).

2.5 Description des dépendances/compatibilités

2.5.1 Matérielles

La solution XSecur'-Evo est compatible avec les badges RFID de technologies MIFARE® Classic, MIFARE® DESFire® EV1 et EV2. Il est fortement recommandé d'utiliser cette solution avec des badges MIFARE® DESFire® de génération EV2.

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. §8.5 Annexe 5 : Références des lecteurs compatibles)

2.5.2 Logicielles

La solution XSecur'-Evo est déployée sur des infrastructures informatiques opérant sous système d'exploitation Windows.

3 DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT DU PRODUIT

3.1 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

Les équipements du GAC sont hors périmètre d'évaluation et supposés de confiance (cf. §3.2Hypothèses d'environnement d'installation du produit).

Composant du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
GAC	**Système d'exploitation**		Windows Server 2019	
	Applicatifs		PCPass Evolution	
	Fonctions cryptographiques		TLS **1.2** avec mbedTLS **2.16.10**	
	Bases de données et annuaires		MySQL **5.7**	
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 : **v6-01-00** **Linux 4.14 Debian 10** UTP-SEC-EVO : **sans OS**		
	Applicatifs	UTL : Firmware XPert **V13-44-51** Module TLS **V2-29-00** UTP-SEC-EVO : **V4-08-00**		
	Fonctions cryptographiques	UTL : mbedTLS **2.16.10** UTP-SEC-EVO : mbedTLS **2.16.10** mmCAU library **1.4**		
	SAM	SAM-SE : **PCB SAM V4** (NXP SE050C)		
Lecteurs	**Lecteurs simples**	SSCPv2 : **Z16**		
	Lecteurs-claviers	SSCPv2 : **Z16**		
Badges			**MIFARE DESFire EV2** : NXP MF3Dx2, MFDHx2, x selon taille mémoire	

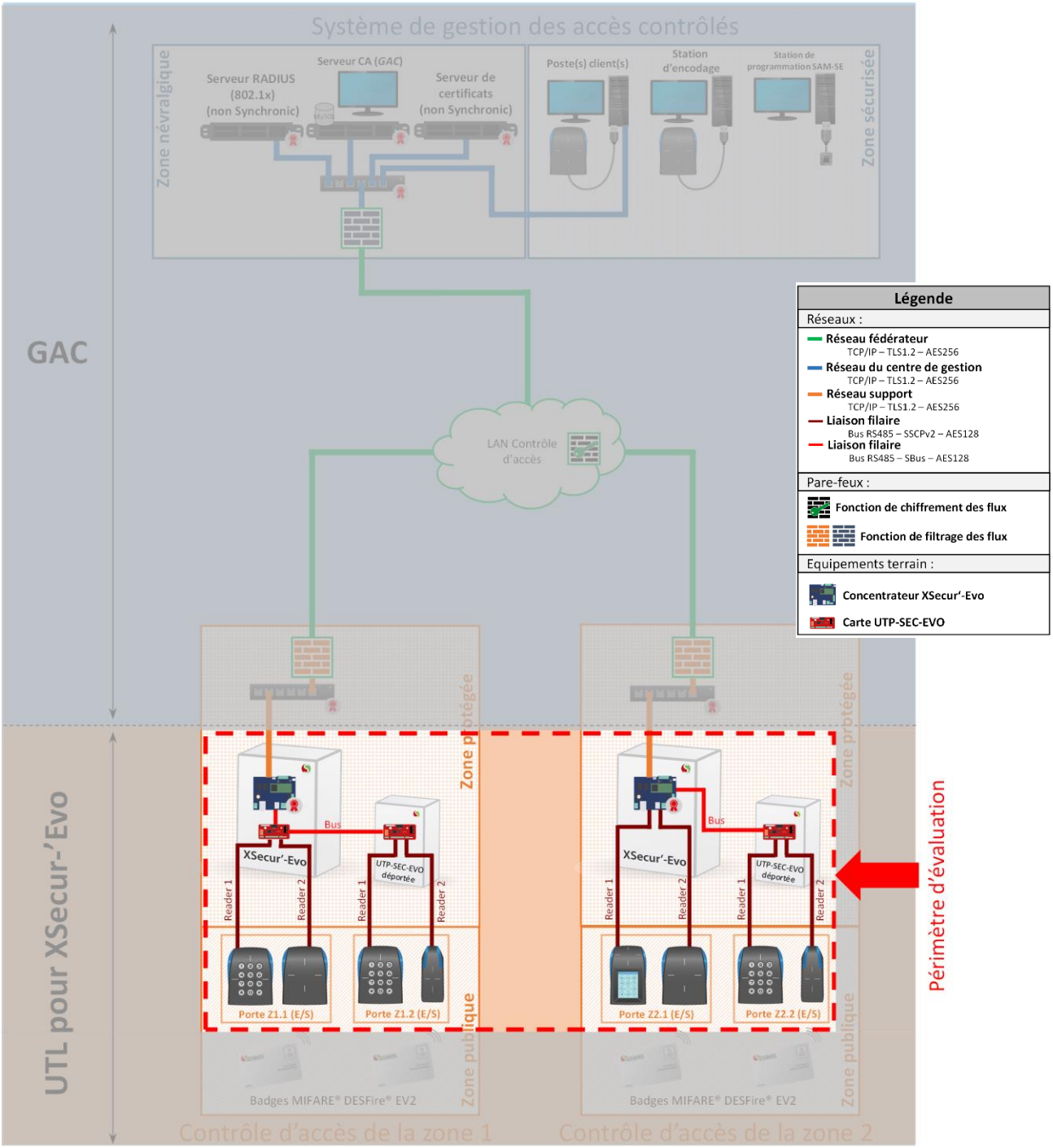

Figure 3 : Schéma du périmètre d'évaluation

3.2 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.

3.2.1 Hypothèses d'environnement d'installation logique du produit

Les éléments du GAC répondent aux caractéristiques suivantes :

- Serveur CA : Microsoft Serveur 2019, MySQLv5.7 avec derniers correctifs
- Serveur de Certificats : Microsoft Serveur 2019 avec rôle d'autorité de certification avec dernier correctifs

- Serveur RADIUS : Microsoft Serveur 2019 avec stratégie NPS et rôle serveur RADIUS avec derniers correctifs
- Poste exploitation client : Windows 7, 8 ou 10 (64 bits) avec derniers correctifs et navigateur Chrome 80 ou supérieur ou Firefox ESR 68 ou supérieur.

La stratégie de mot de passe appliquée par le client respecte à minima les préconisations présentes dans la note technique « *Recommandations de sécurité relatives aux mots de passe* » de l'ANSSI [2] en ce qui concerne à la fois l'ensemble de ses mots de passe SI et les mots de passe des éléments de la solution XSecur'-Evo.

Sur le Serveur CA et les postes d'exploitation, un compte administrateur bénéficiant de tous les droits de configuration et d'exploitation ainsi qu'un compte exploitant bénéficiant des droits restreints d'exploitation courante 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 TLSv1.2 entre ces deux équipements. Leur génération a été réalisée en conformité avec les recommandations présentes dans le guide Synchronic de « *Mise en œuvre XSecur'-Evo* ».

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 de confiance isolée du réseau fédérateur et a ensuite été déployé physiquement sur son concentrateur sans utilisation des mécanismes de diffusion centralisée des secrets, qui ne sont donc pas à évaluer.

3.2.2 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 SI et la solution de contrôle d'accès physique. Le serveur CA sera considéré de confiance et sans attaquant.
- **Poste d'exploitation, 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 exploiter et administrer la solution de contrôle d'accès physique. Les postes d'exploitation seront considérés 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, 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-EVO 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)

Une zone névralgique telle que définie dans le guide « *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection* » [1], correspond à une zone entourée de barrières physiques comprenant un nombre restreint de point d'accès. Elle se situe dans une zone protégée et correspond à la zone la plus protégée.

3.3 Hypothèses sur les réseaux du produit

- **Réseau fédérateur :** Ce réseau, de type liaison filaire Ethernet catégorie 5/5e/6 TCP/IP, sert à interconnecter les réseaux supports et le réseau du centre de gestion. Il est administré intégralement par le SI du client final, ou un prestataire, qui en a l'entière responsabilité. Conformément aux recommandations du guide de l'ANSSI [1], un filtrage des flux transitant sur ce réseau est mis en œuvre afin de n'autoriser que les flux strictement nécessaires au fonctionnement du système.

- **Réseau support :** Ce réseau, de type liaison filaire Ethernet catégorie 5/5e/6 TCP/IP, sert à connecter les concentrateurs sur le réseau fédérateur. Il est administré intégralement par le SI du client final, ou un prestataire, qui en a l'entière responsabilité. Conformément aux recommandations du guide de l'ANSSI [1], un filtrage est mis en place afin de limiter les communications entre les réseaux support raccordés à un même réseau fédérateur aux seuls flux nécessaires au fonctionnement du système.

- **Réseau du centre de gestion :** Ce réseau, de type liaison filaire Ethernet catégorie 5/5e/6 TCP/IP, sert à connecter les éléments du système de gestion du contrôle d'accès (cf. §2.3.2 Schéma d'architecture de la solution) au réseau fédérateur. Conformément aux recommandations du guide de l'ANSSI [1], un filtrage est mis en place afin de limiter les risques de compromission du centre de gestion depuis un réseau support compromis.

- **Bus RS-485** : ce réseau, de type liaison filaire bus RS-485, est indépendant physiquement dans le sens où seul le lecteur d'un concentrateur XSecur'-Evo y est raccordé ainsi que les éventuelles extensions UTP-SEC-EVO. Il se situe tant que possible en zone protégée.

Les deux réseaux filaires (Ethernet et RS-485) physiquement distincts sont totalement étanches et ne peuvent communiquer les moindres données entre eux. Le concentrateur XSecur'-Evo assure la séparation de ces deux réseaux.

3.4 Hypothèses sur les exploitants et administrateurs du produit

L'exploitation de la solution 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

Ces profils sont considérés comme des personnes non hostiles. Ce personnel de confiance est formé pour s'approprier dans sa pleine mesure le système et réaliser strictement les opérations qui lui incombent.

Selon son profil, l'exploitant ou l'administrateur se voit affecté un compte utilisateur lui permettant l'accès aux applications du GAC et à l'interface logique du concentrateur XSecur'-Evo avec des droits d'accès restreints aux seuls opérations qui relèvent de son périmètre de responsabilité.

3.5 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, Synchronic préconise :

- 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 via badge + PIN.
- Ouverture du coffret XSecur'-Evo ou UTP-SEC-EVO par l'agent technique et réalisation des opérations de maintenance.

3.6 Hypothèses sur les utilisateurs finaux du produit

Les utilisateurs finaux de la solution, 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 RFID MIFARE® DESFire® EV2 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).

3.7 Hypothèses sur les badges

Les badges sont de technologie MIFARE® DESFire® EV2 de la société NXP. 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 (Guide Mapping MIFARE® DESFire® EV1/EV2).

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 de ces badges 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 §8.2 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 permettent de répondre aux niveaux de sûreté ci-dessus.

4 DESCRIPTION DES DONNEES SENSIBLES

4.1 Liste des données sensibles de l'UTL pour XSecur'-Evo

Les données 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 diversification
    - 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 :
  - Réseau bus terrain : clé K protocole SSCPv2 pour dialogue lecteur/concentrateur ou lecteur/UTP-SEC-EVO, clé K' protocole SBus pour dialogue concentrateur/UTP-SEC-EVO
  - Réseau IP (support, fédérateur, centre de gestion) : les clés privées TLSv1.2
  - Communication SAM-SE : les clés privées SAM-SE, les clés SCP03 du SAM-SE et du module UTP-SEC-EVO
- Les éléments logiciels sensibles :
  - Firmwares des concentrateurs XSecur'-Evo
  - Firmwares des UTP-SEC-EVO

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

4.2 Besoin de sécurité et emplacement des données sensibles

Données Sensibles		Besoin de sécurité de la donnée :			Emplacement de la donnée :
		Confidentialité	Authenticité	Intégrité	
DS1	Clé maître de lecture	X	X	X	SAM-SE
DS2	Clé de diversification	X	X	X	SAM-SE
DS3	Paramètres de diversification	X	X	X	SAM-SE sauf l'UID
DS4	ID Privé MIFARE® DESFire	X	X	X	Concentrateur
DS5	Codes PIN	X		X	Concentrateur
DS6	Droits d'accès des porteurs	X		X	Concentrateur
DS7	Journaux d'événements	X		X	Concentrateur
DS8	Clé K SSCPv2	X	X*	X*	SAM-SE* Lecteur (EEPROM)
DS9	Clé K' SBus	X	X	X	UTP-SEC-EVO (Stockage diversifié) Concentrateur
DS10	Clé privée TLS	X	X	X	Concentrateur
DS11	Clés SCP03	X	X*	X*	SAM-SE* UTP-SEC-EVO
DS12	Firmware Concentrateur	X	X	X	Concentrateur
DS13	Firmware UTP-SEC-EVO	X	X	X	UTP-SEC-EVO
DS14	Certificats (dont autorité et CRL)	X	X	X	Concentrateur

5 DESCRIPTION DES MENACES

Les menaces auxquelles est exposée l'UTL pour 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 (Serveur CA, postes d'exploitation, badges).

5.1 Attaques 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 lecteur/clavier 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.

5.1.1 AP1 : 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
- 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

5.1.2 AP2 : 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

5.1.3 AP3 : Attaques sur un lecteur/clavier

Les attaques physiques sur le 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

5.2 Attaques logiques

Les attaques logiques considérées concernent :

- Le réseau fédérateur TCP/IP : communication Serveur CA/concentrateur XSecur'-Evo
- La liaison filaire RS-485 :
  - concentrateur XSecur'-Evo ←→ lecteur RFID
  - concentrateur XSecur'-Evo ←→ carte UTP-SEC-EVO
  - UTP-SEC-EVO ←→ lecteur RFID
  - UTP-SEC-EVO ←→ UTP-SEC-EVO
- L'usurpation d'identité d'un serveur CA
- Les données contenues dans le concentrateur (BDD, journaux d'événements)

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

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 §8.3 Annexe 3 : Niveau de sûreté et types de menaces :

- **Niveau III** : franchissement par attaque logique évoluée, préméditée de personnes initiées et fortement 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.

5.2.1 AL1 : Attaques logiques sur le réseau fédérateur

Les attaquants se trouvent en zone protégée, et sont connectés sur le réseau fédérateur du client. 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
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

** : 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*

5.2.2 AL2 : Attaques logiques sur la liaison bus terrain RS-485

Les attaquant 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

5.2.3 AL3 : 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.

5.3 Hypothèses sur les attaquants de l'UTL pour XSecur'-Evo

Les attaquants potentiels de l'UTL pour XSecur'-Evo à considérer pour l'évaluation sont :

- Les porteurs de badge
- Les agents techniques et toute personne pouvant accéder physiquement aux éléments de la cible alors qu'elle est en exploitation.
- Toute personne malveillante connectée sur le réseau BUS RS485 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 RS485.
- Toute personne malveillante connectée au réseau support et pouvant agir avec le concentrateur via son interface réseau.

Les exploitants et les administrateurs GAC **ne sont pas** considérés comme attaquants.

L'ensemble des hypothèses d'installation physique et logique du produit permettent de considérer que le GAC **n'est pas** un attaquant potentiel de l'UTL pour XSecur'-Evo.

6 DESCRIPTION DES FONCTIONS DE SECURITE

Les fonctions de sécurité offerte par l'UTL pour XSecur'-Evo doivent permettre la sécurisation des accès physiques tout en conservant la confidentialité :

- Des identifiants nécessaires au déverrouillage d'accès : badges, PIN
- Des échanges de données sur le réseau fédérateur
- Des échanges de données sur le réseau bus terrain

6.1 Fonctions de sécurité en réponse aux menaces physiques

6.1.1 FSP1 : 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 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 de protection remonte une alarme au Serveur CA et rend inopérant les lecteurs.

6.1.2 FSP2 : Sécurisation de la carte d'extension SAM-SE

Le SAM-SE du concentrateur est situé en zone protégée. Il est supervisé par le concentrateur XSecur'-Evo et intègre un mécanisme d'anti tamper NXP EAL6+.

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 le protocole SCP03 (cf. « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo*» [6]).

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

6.1.3 FSP3 : 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. « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo*» [6]).

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 FSL1 : 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.

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 décrits dans le document *« Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo* » [6].

Ce protocole intervient dans la protection des échanges de données entre le module UTP-SEC-EVO et son SAM-SE, que le module soit intégré au concentrateur (déclinaison « Système ») ou déporté (déclinaison « classique »).

6.2.2 FSL2 : 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. Cette clé assure la confidentialité de tous les échanges entre le concentrateur XSecur'-Evo et le 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 décrits dans le document *« Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo* » [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 FSL3 : Protection des échanges de données par le protocole TLS

Le protocole TLSv1.2 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 dont les spécificités sont décrites dans le document *« Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo* » [6].

Ce protocole intervient dans la protection des échanges de données entre le concentrateur XSecur'-Evo et le Serveur CA.

6.2.4 FSL4 : Protection des Firmwares

Pour ce qui concerne 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 *« Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo* » [6].

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

6.2.5 FSL5 : 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 et 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 *« Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo* » [6].

6.2.6 FSL6 : 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).

L'autorité de certification racine est également protégée par un mécanisme de signature décrit dans le document « *Description des mécanismes cryptographiques de l'UTL pour XSecur'-Evo* » [6].

6.2.7 FSL7 : 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.

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 l'UTL pour XSecur'-Evo afin de déjouer les menaces répertoriées :

Menaces et Fonctions de Sécurité		Autoprotection des coffrets	Sécurisation de la carte d'extension SAM-SE	Sécurisation du lecteur	Protection des échanges de données par le protocole SCP03	Protection des échanges de données par le protocole SSCPv2	Protection des échanges de données par le protocole TLS	Protection des Firmwares	Protection des données du concentrateur	Vérification des certificats	Authentification des équipements par RADIUS
		FSP1	**FSP2**	**FSP3**	**FSL1**	**FSL2**	**FSL3**	**FSL4**	**FSL5**	**FSL6**	**FSL7**
Attaques sur un coffret UTL contenant l'XSecur'-Evo	**AP1**	x	x		x				x		x
Attaques sur un coffret contenant le module UTP-SEC-EVO	**AP2**	x	x		x						
Attaques sur un lecteur/clavier	**AP3**			x							
Attaques logiques sur le réseau fédérateur	**AL1**						x	x		x	x
Attaques logiques sur la liaison bus terrain RS-485	**AL2**					x					
Usurpation d'identité du serveur CA	**AL3**							x		x	

7.2 Menaces et données sensibles

Le tableau ci-dessous met en exergue les données sensibles contenues dans l'UTL pour XSecur'-Evo vulnérables face aux menaces répertoriées :

Menaces et Données Sensibles		Clé maître de lecture	Clé de diversification	Paramètres de diversification	ID Privé MIFARE® DESFire	Codes PIN	Droits d'accès des porteurs	Journaux d'événements	Clé K SSCPv2	Clé K' SBus	Clé privée TLS	Clés SCP03	Firmware Concentrateur	Firmware UTP-SEC-EVO	Certificats (dont autorité et CRL)
		DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9	DS10	DS11	DS12	DS13	DS14
Attaques sur un coffret UTL contenant l'XSecur'-Evo	AP1	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Attaques sur le module UTP-SEC-EVO	AP2	X	X	X					X	X		X		X	
Attaques sur un lecteur/clavier	AP3								X	X					
Attaques logiques sur le réseau fédérateur	AL1				X	X	X	X					X	X	X
Attaques logiques sur la liaison bus terrain RS-485	AL2				X	X								X	
Usurpation d'identité du serveur CA	AL3				X	X	X	X					X	X	X

8 ANNEXES

8.1 Annexe 1 : Architecture n°1, hautement recommandée

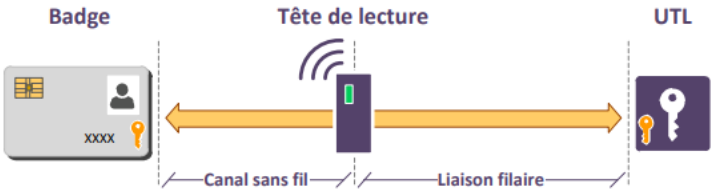

FIGURE 6.2 – Configuration type n°1 : tête de lecture transparente, authentification de bout en bout

8.2 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 ; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES [43]).	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 ; Algorithmes et protocoles d'authentification connus et conformes au RGS (AES [43]) ; 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 D.1 – Correspondance entre niveau de sûreté et niveau de résistance aux attaques logiques

8.3 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 3.1 – Les quatre niveaux de sûreté

8.4 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

8.5 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)

8.6 Annexe 6 : Liste des tâches associées aux utilisateurs

8.6.1 Exploitant

L'exploitant du système réalise les tâches suivantes :

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

8.6.2 Administrateur

L'administrateur du système réalise les tâches suivantes :

- Déclaration des équipements terrain sur le serveur CA
- Maintien en conditions opérationnelles des applications de la gamme Air'Evolution sur le GAC
- Mise à jour du firmware des concentrateurs et des UTP-SEC-EVO
- Octroi des habilitations d'accès des exploitants aux applications de la gamme Air'Evolution
- 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'exploitant
- Programmation des SAM-SE en vue de leur déploiement physique par l'agent technique
- Consultation de l'ensemble des journaux d'événements techniques générés par la solution

8.6.3 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

8.6.4 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.