FABRICANT - INTEGRATEUR - FRANÇAIS DEPUIS 1988

Cible de sécurité CSPN

XSECUR’

V1.05

Référence : SYN-CIBLE-XSECUR-1.05

Date : jeudi 19 juillet 2018

SYNCHRONIC
SECURITE ELECTRONIQUE

HISTORIQUE DES VERSIONS :

Version	Date	Auteur	Description des modifications
v1.05	18/07/2018	Laurent GALVAN	Corrections suite remarques ANSSI
v1.04	11/07/2018	Laurent GALVAN	Corrections suite remarques ANSSI
v1.03	01/12/2017	Laurent GALVAN	Corrections suite remarques ANSSI
v1.02	23/10/2017	Laurent GALVAN	Corrections suite remarques ANSSI
v1.01	16/08/2017	Laurent GALVAN	1ère révision
v1.00	07/06/2017	Laurent GALVAN	Version initiale

DIFFUSION :

Prénom	Nom	Société	Fonction
Guillaume	TÉTU	ANSSI	Certificateur
Olivier	MARY	OPPIDA	Directeur Associé
Nicolas	BIGNARD	SYNCHRONIC	Directeur Général
Laurent	GALVAN	SYNCHRONIC	Chef de Projets Bureau d’Etudes
Thomas	BELTRANDO	SYNCHRONIC	Ingénieur Systèmes Embarqués

COPYRIGHT :

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

Sommaire

1 INTRODUCTION

1.1 Identification de la cible de sécurité

Le présent document constitue la cible de sécurité du produit XSecur'. Cette cible a été élaborée en vue de l'obtention d'une certification de sécurité de premier niveau (CSPN) 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	XSecur'-CSPN
Version du produit évalué	1.0
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
AES	Advanced Encryption Standard, algorithme de chiffrement symétrique
AID	Identifiant d'application DESFire
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP	Auto-Protection
CA	Contrôle d'Accès
DES	Data Encryption Standard, algorithme de chiffrement symétrique
DESFire EV1/EV2	DES, Fast, Innovative, Reliable, and Enhanced **supportant** l'AES128 bits
FID	Numéro de fichier d'application DESFire
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
MGX	Matériel Gamme XPert
Pack Xpert Evolution	Suite de logiciels permettant la configuration et l'exploitation des produits de la gamme XPert
PIN	Personal Identification Number
RFID	Radio Frequency IDentification
Secur'Evolution	Logiciel de génération de fichiers de configuration de lecture RFID
SI CA	Système d'Information du Contrôle d'Accès
SROM	Secure ROM
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	Unité de Traitement de Porte Sécurisée

1.3.2 Références

N°	source	Référence	Description / lien
[1]	ANSSI		https://www.ssi.gouv.fr/uploads/IMG/pdf/Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf
[2]	ANSSI		https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf
[3]	NXP		http://www.nxp.com/documents/application_note/AN10922.pdf

2 ARGUMENTAIRE DU PRODUIT

2.1 Description générale du produit

2.1.1 Description des éléments constitutifs de la solution

La solution XSecur' est un système de contrôle d'accès physiques centralisé utilisant des technologies sans contact RFID conçue et fabriquée en France par Synchronic. Elle s'appuie sur deux parties bien distinctes, appelées :

- « SI CA » composée :
  - d'un serveur CA hébergeant les bases de données et les logiciels de gestion/exploitation
  - d'un serveur de certificats (non fourni par Synchronic)
  - de postes clients
- « MGX », composée :
  - de concentrateurs d'accès XSecur' composés de modules UTP-Sec
  - de lecteurs/claviers TCLDS-485
  - de badges MIFARE® DESFire EV1 ou EV2

2.1.2 Schéma d'architecture de la solution

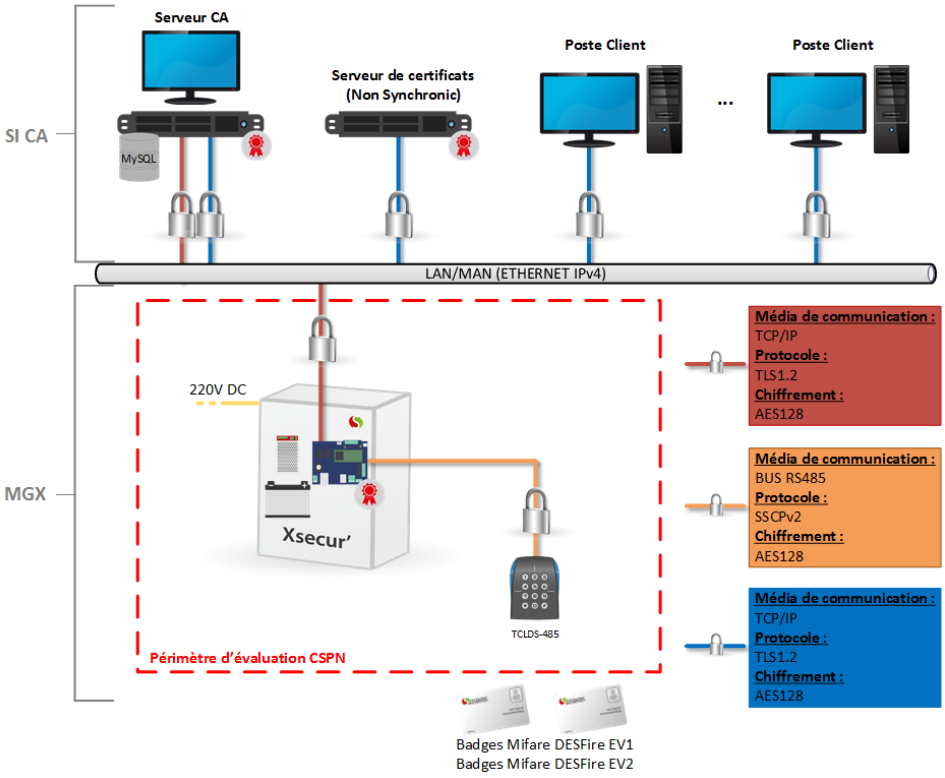

Figure 1 : Schéma d'architecture de la solution XSecur'

2.1.3 Description fonctionnelle de la solution

La solution XSecur' répond au besoin de sécurisation d'accès physiques. Cette sécurisation des accès est assurée par l'utilisation des technologies sans contact RFID 13,56MHz suivant la norme ISO 14443-A.

Le système XSecur' assure l'autorisation d'accès à une zone sécurisée par identification et authentification du badge puis authentification du porteur tel que défini dans le guide « Sécurité des technologies sans-contact pour le contrôle d'accès physiques » [1]. 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'. Combiné à une alimentation secourue, elle aussi au plus proche du concentrateur, la solution bénéficie d'une grande résilience.

L'ensemble, concentrateur XSecur' et son module UTP-Sec, est couramment nommé UTL.

Pour accéder à une zone sécurisée, l'utilisateur final de la solution, appelé porteur de badge, place son badge de type RFID MIFARE® DESFire EV1 ou EV2 dans le champ électromagnétique du lecteur. L'authentification du badge est assurée par la robustesse des mécanismes cryptographiques de la technologie DESFire EV1/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*). L'ensemble des données nécessaires à la lecture d'un badge, dont les clés cryptographiques, sont localisées dans la mémoire volatile du module UTP-Sec du concentrateur d'accès XSecur' et ne sont utilisées qu'en cas de nécessité.

La solution XSecur' assure de plus le déverrouillage d'accès par télé-action ainsi que la supervision de l'état physique d'accès. Pour cela elle s'appuie sur un Serveur CA, un Serveur de Certificats, de(s) poste(s) client(s), un concentrateur XSecur', des têtes de lecture (clavier) et des badges. La partie SI CA ainsi que le concentrateur XSecur' sont interconnectés sur le réseau Ethernet client tandis que la partie MGX est interconnectée en bus fila.

L'administration et la diffusion aux concentrateurs des éléments nécessaires à la lecture de badges (comprenant les clés cryptographiques) sont réalisées de manière centralisée depuis le poste serveur CA. Les utilisateurs finaux de la solution sont appelés des porteurs de badge et possèdent un support de type puce MIFARE® DESFire EV1 ou EV2 et facultativement un code PIN.

2.1.4 Description du réseau fédérateur LAN/MAN

Le réseau LAN/MAN constitue le réseau local Ethernet TCP/IP du client final sur lequel est interconnecté la partie SI CA de la solution XSecur', à savoir le Serveur CA, le Serveur de Certificats, les postes clients ainsi que les concentrateurs XSecur'. Son déploiement, sa mise en œuvre et sa maintenance sont assurés par le client final.

Ce réseau, appelé réseau fédérateur, permet la configuration, l'exploitation et la maintenance de la solution via la suite logicielle Pack Xpert Evolution présente sur le Serveur CA et les postes clients. Les échanges de données entre le serveur CA et l'UTL sont sécurisés via le protocole TLSv1.2.

Le réseau fédérateur LAN/MAN n'est pas inclus dans le périmètre de l'évaluation à l'exception de l'interconnexion du concentrateur XSecur' sur ce réseau.

2.1.5 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 physiques. La partie MGX de la solution XSecur', à savoir le module UTP-Sec des concentrateurs XSecur' 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 situé dans la zone de sécurité protégée par la solution XSecur', permet l'interface entre les lecteurs STid et l'UTL. Les échanges de données sur ce réseau sont sécurisés via le protocole propriétaire SSCPv2.

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

2.1.6 Description du Serveur CA

Le Serveur CA a pour rôle la configuration, l'exploitation et l'administration de la solution contrôle d'accès physiques XSecur' dans son intégralité via les applicatifs métiers développés par Synchronic constituant le Pack Xpert Evolution. Le poste serveur CA est composé d'un serveur informatique sous système d'exploitation Windows Serveur 2012 R2 ou 2016. 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.

Cette base de données contient l'ensemble des informations nécessaires à la gestion du contrôle d'accès physiques, 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. L'intégralité des échanges entre le Serveur CA et le concentrateur XSecur' sont eux aussi historisés avec horodatage dans cette base de données.

Le Serveur CA assure la diffusion des secrets nécessaires au concentrateur XSecur' afin d'établir le dialogue avec les lecteurs compatibles SSCPv2 ainsi que les paramétrages MIFARE® DESFire (dont les clés cryptographiques) pour un fonctionnement en mode « transparent ».

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

2.1.7 Description du Serveur de Certificats

Le Serveur de Certificats a pour rôle l’émission de certificats pour la mise en œuvre de la sécurisation TLSv1.2 entre le Serveur CA et le concentrateur XSecur’. Ce serveur n’est pas fourni avec la solution XSecur’ 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.

2.1.8 Description du poste client

Le poste client a pour rôle l’exploitation de la gestion du contrôle d’accès physiques. Il permet l’affectation et la propagation des droits d’accès au concentrateur XSecur’. Sa communication avec le serveur CA s’appuie sur un protocole HTTPS (TLSv1.2).

Le poste client, dans sa configuration station d’encodage, peut aussi avoir pour rôle la création de badges utilisateurs via un équipement USB d’encodage.

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

2.1.9 Description du concentrateur XSecur’

Le concentrateur XSecur’ a pour rôle de vérifier les droits d’accès des porteurs de badge MIFARE® DESFire EV1 ou 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 20 000 identifiants distincts. Afin de remplir son rôle, un concentrateur XSecur’ 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.

Le concentrateur XSecur’ est notamment composé d’un module UTP-Sec, cet ensemble est usuellement appelé dans le domaine du contrôle d’accès UTL. Celui-ci gère nativement un lecteur afin de contrôler un accès et peut gérer par ajout de cartes extensions filles UTP-Sec, jusqu’à 15 accès physiques soit 30 lecteurs. Son paramétrage réalisé par le Serveur CA lui permet une gestion des lecteurs en mode « transparent ». Il exécute les mécanismes cryptographiques nécessaires à la communication avec les badges MIFARE® DESFire EV1 ou EV2.

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

La sécurisation des échanges entre le concentrateur XSecur’ et les lecteurs reposent sur la solidité du protocole SSCPv2 basé sur les mécanismes d’authentification AKEPv2, un chiffrement AES128 et une signature HMAC-SHA256 respectivement pour l’authenticité, la confidentialité et l’intégrité. Une clé d’initialisation de la communication appelée clé K, est paramétrée d’usine et doit être personnalisée par le client final. Cela a pour effet de modifier la clé K du lecteur. Le concentrateur possède une adresse MAC-UT unique octroyée à sa production.

La sécurisation des échanges entre le concentrateur XSecur’ et son Serveur CA reposent sur le protocole TLSv1.2. Un certificat d’initialisation de la communication est assigné d’usine et doit être personnalisé par le client.

La sécurisation du fichier de configuration des secrets DESFire, généré par l’applicatif Secur’Evolution, est assurée par une clé privée AES de longueur 128 bits. Une clé de déchiffrement du fichier de configuration est assignée d’usine. 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 modifiée par le client final.

Le concentrateur XSecur’, usuellement situé en zone névralgique, possède des mécanismes de protection d’ouverture de coffret (AP). La confidentialité des clés et des paramètres DESFire est assurée dans le concentrateur XSecur’ par un mécanisme de séquestration des données développé par Synchronic reposant sur une SROM. (cf. *SYN-DES-MEC-CRY-XSECUR*). Cette SROM stocke la clé UTP-Sec nécessaire au déchiffrement de ces paramètres.

Information	Description
Dénomination	XSecur’
Dénomination technique	XL02-v5d
Version noyau	V5-04-00 (Linux 4.4)
Version logicielle (XSecur’/Module UTP-Sec/Module TLS)	V13-20-00 / V2-10-00 / V2-20-00
Microprocesseur	ARM cortex A5
Emplacement	Coffret alarme en zone névralgique
Données	Fichiers utilisateurs, fichier de configuration de lecture et clés en mémoire non volatile Base de données en Flash
AP	Détection d’ouverture coffret

Le concentrateur XSecur’ est inclus dans le périmètre de l’évaluation.

2.1.10 Description du lecteur/clavier TCLDS-485

Le lecteur/clavier TCLDS-485 a pour rôle de transmettre les échanges RFID entre le badge MIFARE® DESFire EV1 ou EV2 et le concentrateur XSecur’ sans les modifier. Il fonctionne en mode « transparent », et permet d’authentifier le porteur du badge en autorisant la saisie d’un code PIN. Cet équipement est fabriqué par le constructeur français de lecteur RFID STid.

Une clé d’initialisation de la communication SSCPv2 (clé K), est paramétrée d’usine et doit être personnalisée par le client final.

Information	Description
Dénomination	TCLDS-485
Dénomination technique	ARC-W33-B-PH5-7AD
Version logicielle	Z07
Microcontrôleur	NXP cortex M4
Emplacement	Zone publique ou zone sécurisée
Données	Clé K en EEPROM
AP	Accéléromètre et arrachement

Le lecteur/clavier TCLDS-485 est inclus dans le périmètre de l’évaluation.

2.1.11 Description du badge MIFARE® DESFire EV1 et EV2

Le badge MIFARE® DESFire EV1 ou EV2 détenu par les utilisateurs de la solution contient l’identifiant privé unique de l’utilisateur. L’intégralité des informations présentes dans le badge sont sécurisées par la méthode de diversification NXP-AN10922 [3] (clé AES 128 bits).

Aucune information visuelle à l’exception d’un code de traçabilité, et éventuellement la photo du porteur du badge, 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 à 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 se sont vu octroyer 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.

Dans l'optique de satisfaire un besoin croissant de ses clients en termes de haute sécurité basée sur les technologies sans contact RFID, Synchronic a développé une solution de contrôle d'accès physiques intégrant les recommandations ANSSI présentes dans le guide « Sécurité des technologies sans-contact pour le contrôle d'accès physiques » [1]. Les lecteurs proposés dans cette solution 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 n°1 du guide susdit. Les lecteurs ne possèdent donc aucune clé cryptographique nécessaire à la lecture de badges, et ce 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 permettant un pilotage du lecteur dynamique complet, une communication hautement sécurisée et une authentification du lecteur.

Cette solution est destinée à être déployée dans la zone qu'elle sécurise à l'exception des lecteurs. Elle assure à la fois l'interface avec l'environnement physique de porte et son informatique de gestion SI CA. En tant que solution ouverte et interopérable, XSecur' est amenée à être interconnectée avec des superviseurs graphiques de gestion de bâtiments afin d'avoir un suivi en temps réel de sites et de piloter des organes d'ouverture.

La solution XSecur' 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

La solution contrôle d'accès physiques XSecur' est basée sur l'utilisation de badge MIFARE® DESFire EV1 ou EV2. Ces badges sont prêts à l'emploi, ils ont été paramétrés afin de contenir une application propre au contrôle d'accès du client et dispose 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] permettant à partir d'une clé mère, 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 bits de l'ID Privé réalisée par le badge.

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/ou l'ID Privé chiffré en AES 128 bits au lecteur via la liaison filaire RS-485 utilisant le protocole SSCPv2.

Le module UTP-Sec possédant la clé mère, les paramètres de diversification, utilises l'UID transmit par le lecteur afin d'appliquer la méthode de diversification NXP-AN10922 [3] ayant servie à l'encodage du badge, pour recalculer la clé diversifiée et ainsi déchiffrer l'ID Privé. Le concentrateur XSecur' vérifie 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 remonté via sécurisation TLSv1.2 pour historisation sur le Serveur CA par le biais du réseau fédérateur.

Afin d'assurer une transition temporelle non immédiate de révocation de clé de lecture DESFire ou de pouvoir déchiffrer les ID Privés de deux populations de badges distinctes, la solution XSecur' permet la lecture d'une double configuration de paramètres RFID.

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 EV1 ou EV2, les lecteurs TCLDS-485 sont équipés d'un clavier. 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, son porteur saisit un code PIN qui est transmis par le lecteur/clavier TCLDS-485 au concentrateur XSecur' de manière sécurisée via la liaison filaire RS-485 utilisant le protocole SSCPv2. Il est chiffré en AES 128 bits jusqu'à l'UTL.

Le module UTP-Sec déchiffre le code PIN par le lecteur TCLDS-485 et l'UTL s'assure de sa validité en correspondance avec le badge préalablement authentifié par son porteur. Un ordre de déverrouillage peut alors être transmis par le concentrateur au dispositif de verrouillage de l'accès.

Cet événement de saisie de code PIN est simultanément remonté via sécurisation TLSv1.2 pour historisation sur le Serveur CA par le biais du réseau fédérateur.

L'activation de 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

Les exploitants de la solution XSecur' sont les personnes internes ou externes à l'organisation du client ayant été mandatées pour assurer la gestion de la sûreté. Ils ont pour mission l'utilisation au quotidien de la solution, à savoir, la configuration, l'adaptation des fonctionnalités du système et ainsi affecter les autorisations d'accès sur l'ensemble des accès contrôlés.

Les connexions aux applications du système de contrôle d'accès physiques XSecur' sont toutes tracées avec un détail des actions effectuées.

2.4.2 Les Agents Techniques

Les agents techniques de la solution XSecur' 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 la solution. Ils sont les seuls à disposer des procédures d'accès physique au concentrateur XSecur'.

Les ouvertures du coffret contenant le concentrateur et les connexions au système 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*).

2.4.3 Les Porteurs de Badge

Les porteurs de badge de la solution XSecur' sont toutes les personnes utilisatrices du dispositif de contrôle d'accès physiques du client. Selon leur profil, collaborateurs, prestataires, visiteurs, ils accèdent aux zones sécurisées voire névralgiques grâce :

- Au badge RFID de technologie MIFARE® DESFire EV1 ou EV2 remis par le service sûreté du client
- Accessoirement au code PIN remis par le service sûreté du client

2.5 Description des hypothèses d'environnement du produit

2.5.1 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, ayant suivi une formation constructeur.

2.5.1.1 Hypothèses d'environnement d'installation logique du produit

Les applications sur le Serveur CA et les postes clients sont installés sur des systèmes sains. 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'.

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.

Des certificats X509v3 ont été déployés sur le Serveur CA et dans le concentrateur XSecur' afin de personnaliser la sécurisation des échanges de données entre ces deux équipements. Leur génération ont été réalisées en conformité avec les recommandations présentes dans le guide Synchronic de « mise en œuvre XSecur'-CSPN ».

2.5.1.2 *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 SI et la solution de contrôle d'accès physiques.
- **Poste d'exploitation :** situé dans les locaux du client en zone sécurisée son accès est limité aux strictes personnes habilitées à exploiter et administrer la solution de contrôle d'accès physiques.
- **Concentrateur XSecur' :** situé en zone névralgique, le câblage de l'environnement de porte est réalisé sur le concentrateur en point à point.
- **Lecteur TCLDS-485 :** seul dispositif de la solution installé en zone non sécurisée, le câble de raccordement au concentrateur XSecur' doit pénétrer immédiatement en zone de sécurité afin de s'assurer d'aucun cheminement en zone non sécurisée. Cette liaison de type filaire réseau RS-485 est directe.

Une zone névralgique telle que défini dans le guide sur le contrôle d'accès de l'ANSSI [1], correspond à une zone entourée de barrières physiques comprenant un nombre restreint de point d'accès. Elle se situe dans une zone sécurisée et correspond à la zone la plus protégée.

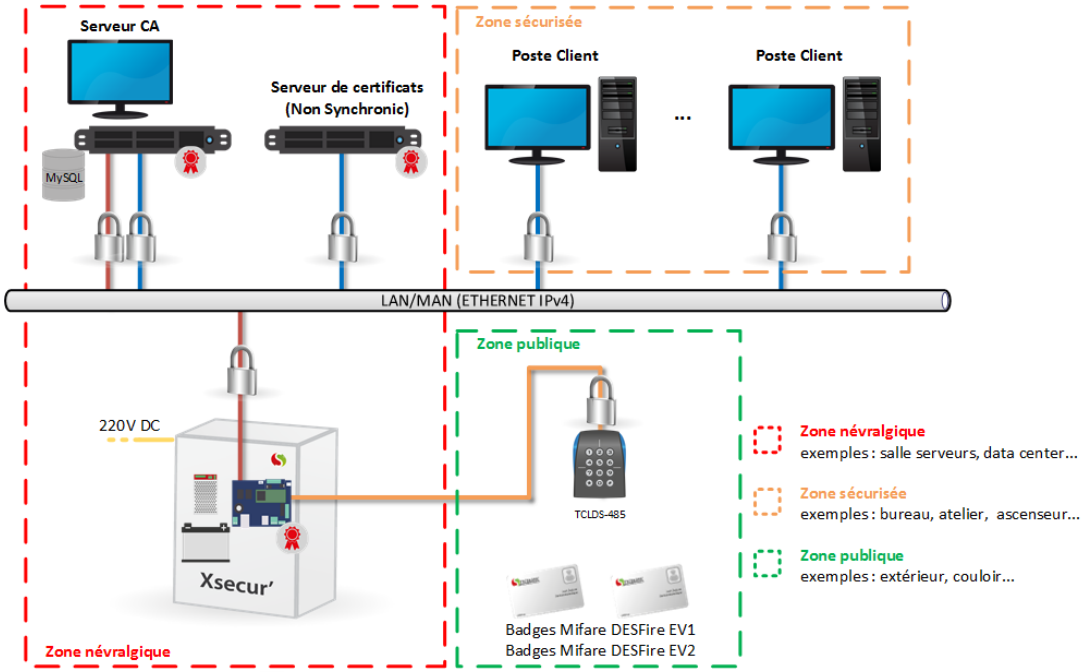

Figure 2 : Schéma de répartition des éléments de la solution

2.5.2 Hypothèses sur les réseaux du produit

- **Réseau fédérateur :** ce réseau, de type liaison filaire Ethernet catégorie 5 TCP/IP, est indépendant logiquement par le biais d'un VLAN dédié contrôle d'accès voire indépendant physiquement, ce réseau est administré intégralement par le SI du client final qui en a l'entière responsabilité.
- **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' y est raccordé. Il se situe tant que possible en zone sécurisée.

Ces 2 réseaux physiquement distincts sont totalement étanches et ne peuvent communiquer les moindres données entre eux. Le concentrateur XSecur' assure la séparation de ces deux réseaux.

2.5.3 Hypothèses sur les exploitants du produit

L'exploitation de la solution, 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 exploitants 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 se voit affecter un compte utilisateur lui permettant l'accès aux l'applicatifs de la solution XSecur' avec des droits d'accès restreints aux seuls opérations qui relèvent de sa responsabilité.

2.5.4 Hypothèses sur les utilisateurs finaux du produit

Les utilisateurs finaux de la solution, trivialement 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 EV1 ou EV2 dans une zone contrôlée par un lecteur. Ils peuvent appartenir, d'un point de vue du client final, à une population de :

- Collaborateurs
- Prestataires
- Visiteurs

De plus, ces porteurs de badge disposent optionnellement d'un code PIN permettant leur authentification. 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*).

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 est amené à réaliser l'authentification qu'impose l'accès même si l'accès est accessible sans cette procédure.

2.5.5 Hypothèses sur les attaquants de la solution

Les attaquants potentiels de la solution XSecur' sont :

- Les porteurs de badge
- Toute personne extérieure

Les exploitants ainsi que les agents techniques ne sont pas considérés comme attaquants.

2.5.6 Hypothèses sur les badges

Les badges sont de technologie MIFARE® DESFire EV1 ou 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 bits 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 spécifie 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 le numéro de matricule du porteur.

2.6 Description des dépendances/compatibilités

2.6.1 Matérielles

La solution XSecur'-CPSN est compatible avec les badges RFID de technologies MIFARE®. Il est fortement recommandé d'utiliser cette solution avec des badges MIFARE® DESFire EV1 ou EV2.

2.6.2 Logicielles

Le concentrateur XSecur' est compatible avec l'ensemble des équipements 7AD, communiquant via le protocole SSCPv2, du fabricant de têtes de lecture RFID STid.

2.7 Description du périmètre de l'évaluation

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

- Le concentrateur XSecur'
- Le lecteur/clavier TCLDS-485

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

Afin de procéder à l'évaluation les éléments ci-dessous sont nécessaires :

3.1 Dispositif d'accès

Le dispositif est composé de ce qu'on appelle couramment l'environnement de porte. Cela comprend 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)
- Un organe de commande d'ouverture soit par contact sec soit par alimentation (rupture : ventouse, émission : gâche électrique)
- Un lecteur RFID d'entrée

3.2 Postes informatiques

- Serveur CA : Microsoft Serveur 2016, MySQLv5.7 avec derniers correctifs
- Poste exploitation client : Windows 7, 8 ou 10 (32 ou 64 bits) avec derniers correctifs et navigateur Chrome 61 ou supérieur ou Firefox ESR 52 ou supérieur.

3.3 Badges

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

Les badges de technologies MIFARE® DESFire EV1 et EV2 répondent aux niveaux de sûreté ci-dessus.

4 DESCRIPTION DES DONNEES SENSIBLES

4.1 Liste des données sensibles de la solution

Les données sensibles protégées par la solution XSecur’ sont :

- Les données confidentielles du contrôle d’accès :
  - Les paramètres DESFire d’accès à l’identifiant privé :
    - AID
    - FID
    - Clé mère de lecture :
      - Index
      - Valeur
    - Clé de diversification
    - Paramètres de diversification
  - Les identifiant privés
  - Les codes PIN
  - Les droits d’accès des porteurs de badge
- Les éléments de sécurisation des communications de la solution :
  - Réseau bus terrain : la clé K de communication lecteur
  - Réseau fédérateur : les certificats TLSv1.2
- L’élément de sécurisation du module UTP-Sec de l’UTL :
  - La clé UTP-Sec

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

4.2 Répartition des données sensibles de la solution

Données Sensibles	Concentrateur XSecur’	Lecteur (TCLDS-485)
Paramètres DESFire Identifiant Privé	oui	non
Identifiant Privé	oui	non
Codes PIN	oui	oui (touche par touche)
Droits d’accès	oui	non
Clé K	oui	oui
Certificat TLSv1.2	oui	non
Clé UTP-Sec	oui	non

5 DESCRIPTION DES MENACES

Les menaces auxquelles est exposée la solution XSecur' peuvent être catégorisées en deux types :

- Les attaques physiques
- Les attaques logiques

Toute attaque en provenance de l'extérieur du périmètre de l'évaluation ne sont pas prises en compte (Serveur CA, postes d'exploitation, badges).

5.1 Attaques physiques

Les attaques physiques considérées concernent :

- Le lecteur/clavier TCLDS-485

Les attaquants peuvent être soit externes (en zone publique), soit internes (en zone sécurisée) et ont un accès direct aux éléments.

5.1.1 Attaques sur un lecteur/clavier TCLDS-485

Les attaques physiques sur le lecteur/clavier TCLDS-485 pouvant porter préjudice au service offert par la solution de contrôle d'accès physiques sont :

- La cryptanalyse visant au déchiffrement des données sensibles
- L'extraction de code source
- L'exécution de code frauduleux
- La substitution d'un lecteur/clavier TCLDS-485
- L'émulation d'un lecteur/clavier TCLDS-485

5.2 Attaques logiques

Les attaques logiques considérées concernent :

- Le réseau fédérateur TCP/IP : communication Serveur CA/concentrateur XSecur'
- La liaison filaire RS-485 : concentrateur XSecur'/lecteur RFID

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

Les attaquants peuvent être soit externes (en zone publique), soit internes (en zone sécurisée) 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, préméditées 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, préméditées 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 Attaques logiques sur le réseau fédérateur LAN/MAN

Les attaquants se trouvent en zone protégée, et sont connectés sur le réseau LAN/MAN 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

** : la duplication du badge n'est possible que si de plus les paramètres DESFire sont 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 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 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

6 DESCRIPTION DES FONCTIONS DE SECURITE

Les fonctions de sécurité offerte par la solution XSecur' 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 LAN/MAN
- des échanges de données sur le réseau MGX

6.1 Fonctions de sécurité en réponse aux menaces physiques

6.1.1 Protection du lecteur ①

Le lecteur est situé en zone publique. Il est supervisé par le serveur CA et possède des mécanismes de protection à l'arrachement via accéléromètre. Cela permet la remontée d'événement de tentative de fraude au concentrateur XSecur' 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. (cf. *SYN-DES-MEC-CRY-XSECUR*).

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 de l'ID Privé ②

La protection des transactions entre le badge et le lecteur contenant l'identifiant privé est assurée en confidentialité par un chiffrement AES 128 bits (clé diversifiée).

6.2.2 Protection du code PIN ③

La protection des transactions entre le lecteur/clavier TCLDS-485 et le concentrateur contenant le code PIN est assurée par les mécanismes de communication décrit *§6.2.3*.

6.2.3 Protection des échanges de données entre le concentrateur XSecur' et le lecteur ③

La protection des échanges de données entre le concentrateur XSecur' et le lecteur est assurée par le protocole SSCPv2 établissant un canal sécurisé suite à une authentification mutuelle via secret partagé dont résulte les clés de session AES 128 bits. Cette clé assure la confidentialité de tous les échanges entre le concentrateur XSecur' et le lecteur.

L'authentification, l'échange de clé de session, l'intégrité et la protection contre le rejeu sont assurés par les mécanismes décrits dans le document de description des mécanismes cryptographiques de la solution (cf. *SYN-DES-MEC-CRY-XSECUR*).

6.2.4 Protection des échanges de données entre le concentrateur XSexur' et le Serveur CA ④

La protection des échanges de données entre le concentrateur XSecur' et le Serveur CA est assurée par le protocole TLSv1.2 établissant un canal sécurisé suite à une authentification mutuelle via certificats X509v3 dont résulte une clé de session AES 128 bits. Cette clé assure la confidentialité de tous les échanges entre le concentrateur XSecur' et le Serveur CA.

L'authentification, l'échange de clés de session, l'intégrité et la protection contre le rejeu sont assurées par les mécanismes décrits dans le document de description des mécanismes cryptographiques de la solution (cf. *SYN-DES-MEC-CRY-XSECUR*).

7 LES FONCTIONS DE SECURITE FACE AUX MENACES

Le tableau ci-dessous met en exergue les fonctions de sécurité mises en œuvre par la solution afin de déjouer les menaces répertoriées :

Menaces	Fonction de sécurité			
	①	②	③	④
Menaces physiques				
Lecteur : cryptanalyse, extraction de code, extraction de données sensible, exécution de code frauduleux, substitution, émulation	X			
Menaces logiques : réseau fédérateur				
Interception d’une transaction contenant l’ID Privé		X		X
Interception d’une transaction contenant le PIN				X
Interception d’une commande d’affectation de droits				X
Interception d’une commande d’affectation de grille horaire				X
Interception d’une transaction contenant une commande d’ouverture ponctuelle				X
Interception d’une transaction contenant une commande d’ouverture permanente				X
Menaces logiques : réseau bus terrain				
Interception d’une transaction contenant l’ID Privé		X	X	
Interception d’une transaction contenant le PIN			X	
Interception d’une transaction contenant des paramètres DESFire			X	
Interception d’une transaction contenant une commande SSCPv2			X	

8 ANNEXES

8.1 Annexe 1 : Architecture n°1, hautement recommandée

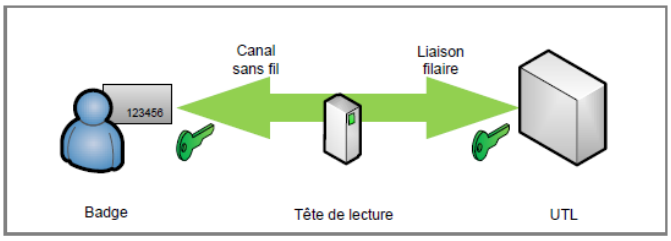

Figure 7 : Architecture n°1 : tête de lecture transparente, authentification de bout en bout

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

Niveau de sûreté	Résistance aux attaques logiques[12]	Méthode	Technologie	Caractéristiques
I	-	Identification du badge, ou information mémorisée, ou élément biométrique.	Transpondeurs 125kHz et assimilés, cartes ISO14443 ou ISO15693 sans usage de la cryptographie ou à cryptographie défaillante ou propriétaire.	Facilement clonable
II	L1	Authentification du badge.	Carte ISO 14443, authentification à cryptographie symétrique.	Authentification reposant sur une clef commune ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
III	L2	Authentification du badge, clefs dérivées recommandées.	Carte ISO 14443, authentification à cryptographie symétrique	Authentification reposant sur une clef dérivée d'une clef maîtresse ; algorithmes et protocoles d'authentification connus et réputés (3DES, AES).
IV	L3	Authentification du badge et du porteur par un second facteur (information mémorisée ou élément biométrique). Clef dérivées.	Carte ISO 14443, authentification à cryptographie symétrique. Saisie d'un code mémorisé ou d'un élément biométrique.	Authentification reposant sur une clef dérivée d'une clef maitresse ; Algorithmes et protocoles d'authentification connus et réputés (3DES, AES).

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

synchronic@synchronic.fr

www.synchronic.fr

SYNCHRONIC Rouen - Siège social
ZAC des Champs Fleuris,
393 R. des Manets
76520 - Franqueville Saint Pierre
Tél. : +33(0) 235 085 850
Fax : +33(0) 232 830 050

SYNCHRONIC I.D.F.
1 Place du village
92300 Gennevilliers

Tél. : +33(0) 147 999 281
Fax : +33(0) 232 830 050

SYNCHRONIC Sud Ouest
214 Rte. de Saint Simon
Imm. le Tertial - Bat. 1 - 1er étage
31100 - Toulouse
Tél. : +33(0) 582 950 548
Fax : +33(0) 232 830 050

SYNCHRONIC Sud Est
38, place des Pavillons
Bureau n°3
69007 Lyon
Tél. : +33(0) 472 808 241
Fax : +33(0) 232 830 050

Synchronic - SAS au capital de 133 200 € - RCS : ROUEN B 344 539 564 - VAT : FR90 344 539 564