Cible de Sécurité
SMI Server v4.6

Solution SMI Server v4.6, SM400 v2.8.6, SM100+ v4.0.100

Identification, authentification pour le contrôle des accès physiques

A0Y011

FICHET

Cible de Sécurité - Solution SMI Server v4.6
Solution SMI Server - Identification, authentification pour le contrôle des accès physiques

Date	Version	Objet des modifications	Auteur
Mai 2022	00	Création de la Cible de Sécurité sous référence A0Y011 pour la Solution SMI Server - 2023	F.Mir
20/06/2022	01	1ère version	F.Mir
01/07/2022	02	Version complétée.	F.Mir
12/07/2022	03	Compléments suite remarques OPPIDA	F.Mir
26/07/2022	04	Finalisation	F.Mir
28/10/2022	05	§1.1, §2.1.8, §2.1.9, §2.1.10, §2.1.11, §2.1.12 : versions logiciel Tableau §2.6 : références et versions des composants	F.Mir
21/11/2022	06	Correction tableau §2.6	F.Mir
04/04/2023	07	Mise à jour versions firmwares	F.Anin
07/12/2023	08	Modification ref SMI & versions firms / librairies crypto §1.1, §1.2, §2.1.8, §2.1.9, §2.6, §5.2	F.Anin
27/10/2024	09	Précisions sur la gestion des certificats sur le réseau du client. Changement nom du document et des numéros de versions des logiciels des équipements mis à jour pour implémenter les correctifs suite au rejet de qualification de SMI 2023.	F. Kapp
19/12/2024	10	Ajout des références du SM400 et SM400-L et du kit d'update capteur de vibration pour les SM100+/SM400/SM400-L.	J. Riberolles
23/01/2025	11	Mise à jour des numéros de versions des logiciels suite à une phase de correction de bug et de mise à jour des librairies. Uniformation des références (les 0 ont parfois été remplacés par des O)	J. Riberolles
24/07/2025	12	Changement du nom de produit suite à l'octroi de la certification (SMI Server 2024 devient SMI Server v4.6). MàJ bibliographie.	J. Riberolles

Liste des documents de référence

Source	Référence	Vers	Source/actualisation
ANSSI	ANSSI-CSPN-CER-P-01	V5.0	cyber.gouv.fr
ANSSI	GUIDES-ANSSI	V2.2	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection
ANSSI	Référentiels cryptographiques	RGS27	Annexe B1 Chiffrement de bout en bout
ANSSI	GUIDES-ANSSI	SDE-NT-35 v1.2	Recommandations de sécurité relatives à TLS.
ANSSI	ANSSI-CSPN-NOTE-07_v2.1	2.1	Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN
ANSSI	ANSSI-PG-078	V2.0	Recommandations relatives à l'authentification multifacteur et aux mots de passe
APSAD	Référentiel	D83	Contrôle d'accès - Documents techniques pour la conception et l'installation
APSAD	Référentiel	D32	Cybersécurité – Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique »

Cible de Sécurité : SMI Server v4.6
Identification, authentification pour le contrôle des accès physiques

A0Y011 – Ed. 12 – juillet 2025

Sommaire

INTRODUCTION

1.1 Identification de la Cible de Sécurité (CdS)

Ce document constitue la **Cible de Sécurité** pour le système de contrôle d'accès basé sur le logiciel SMI Server V4.6, les concentrateurs d'accès SM400/SM400-L, les contrôleurs de portes SM100+ et les lecteurs de la gamme ProStyl. Le terme SM400 désigne, dans toutes nos documentations, indifféremment le SM400 ou le SM400-L car fonctionnellement identiques. La seule différence entre ces équipements est le déséquipement d'un bus échelon non utilisé sur le SM400-L par rapport au SM400, et qui ne rentre pas dans le cadre de la certification où seuls les bus RS485 sont concernés.

Usages : Identification, authentification pour le contrôle des accès physiques.

1.2 Identification du produit

1 **Nom du produit : Solution SMI Server v4.6**

Composé des équipements suivants :

- **SMI Server**
- **Concentrateur d'accès SM400 (et/ou SM400-L indifféremment)**
- **Contrôleurs de portes SM100+ avec l'Extension SAM**
- **SAM AV2/AV3**
- **Gamme des lecteurs ProStyl**
- **Kit d'update capteur de vibration sur chaque SM400/SM400-L/SM100+**

2 **Constructeur : Fichet Technologies**

Site de FICHET : https://www.fichetgroup.com

3 **Utilisations : Contrôles d'accès sécurisés de sites administratifs, industriels et tertiaires.**

1.3 Références & désignations

Désignation	Description
AES	Advanced Encrypted Standard
AP	Auto Protection
DESFire	DES Fast innovative reliable enhanced (NXP)
DH	Diffie Hellmann
ECC	Elliptic Curve Cryptography
GAC	Gestion des accès contrôlés
ID	Identifiant
PIN ou CIP	Personal Identification Number/ Code Identification Personnel
ProStyl Clavier et ProStyl K	Lecteur d'accès RFID avec Clavier digital
ProStyl S et B	Lecteur d'accès RFID
RSSI	Responsable Sécurité Système d'Information
SAM	Secure Access Module
Server	Machine host hébergeant des applications et des données
Serveur d'applications	Serveur avec « applications métier » et base de données
Serveur de présentation	Serveur permettant l'interface entre les Postes d'exploitation et le Serveur d'applications
SI	Système d'Information
SM100+	Contrôleur de portes
SM400/SM400-L	Concentrateur d'accès
SMI Server	Système de Management Intégré
SOP	Smart Open Protocol (propriétaire FICHET)
UTL	Unité de Traitement Locale
VM	Virtual Machine

2 ARGUMENTAIRE DU PRODUIT

2.1 Description générale du produit

2.1.1 Architecture de la solution d'accès

La solution **SMI Server** correspond à une solution intégrée pour une gestion centralisée de contrôle d'accès physique.

Elle est composée :

- d'une partie appelée « **Server** » intégrant les applications, les bases de données et les serveurs d'applications et de présentation, située en zone névralgique,
- d'une partie appelée « **SMI** » intégrant les équipements de terrain : concentrateurs d'accès, contrôleurs de portes et lecteurs.

Le système est architecturé autour des équipements représentés ci-dessous et a pour objectif de filtrer les flux d'individus (usagers) autorisés ou non à pénétrer sur un site, un bâtiment ou des locaux.

Pour assurer les contrôles sur les accès, le système d'accès remplit les fonctions suivantes :

- *Identification* par badge RFID (sans contact) et *authentification* PIN Code
- Traitements des droits d'accès au niveau du contrôleur de portes (UTL)
- Automatisme d'accès (déverrouillage, séquencement d'opérations de contrôle de l'ouvrant, état de l'accès physique)
- La solution SMI Server peut être implantée dans différents secteurs tels que les Administrations, l'Industrie et le Tertiaire.

Ce document rentre dans le cadre de contrôle d'accès utilisant des technologies sans contact telles que définies par l'ANSSI dans le Guide « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection ».

2.1.2 Schéma type

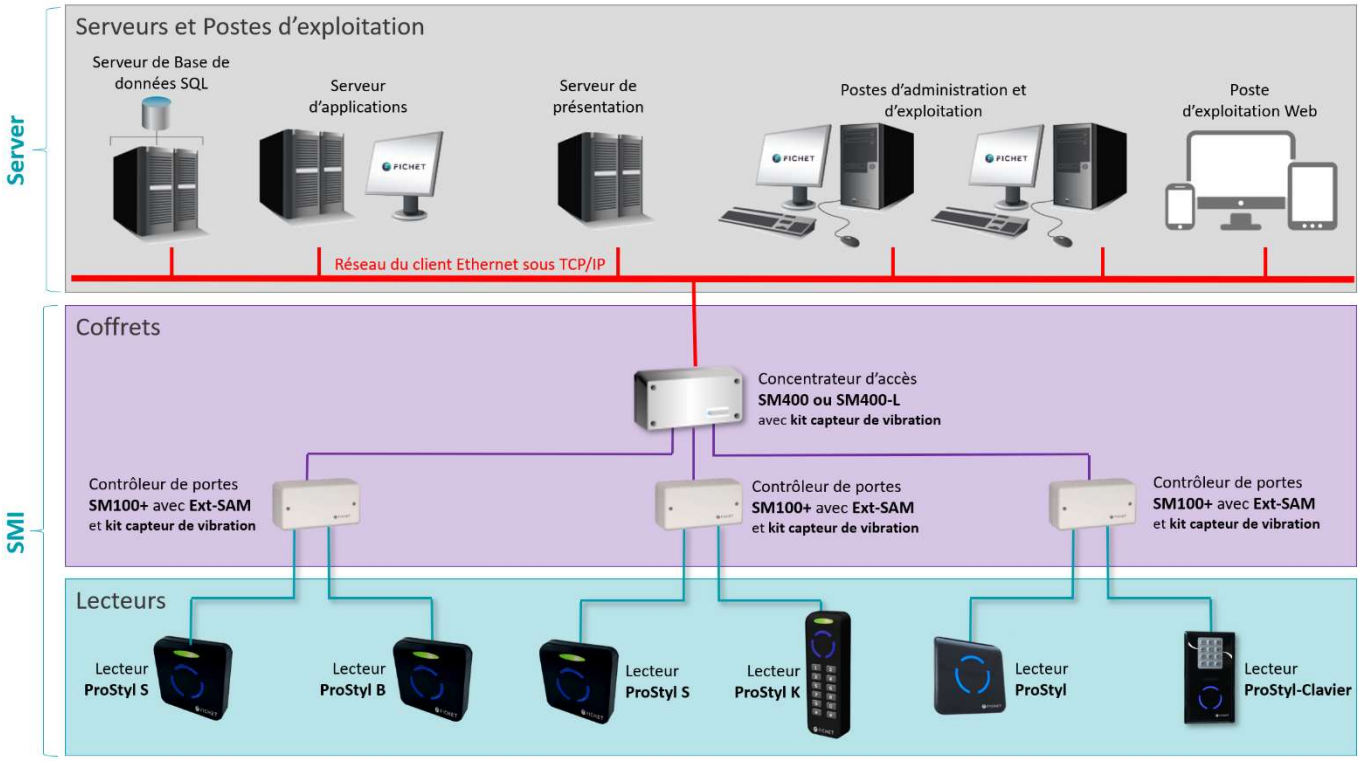

Figure 1 : SMI & Server

2.1.3 Description fonctionnelle et utilisation

La solution SMI Server de FICHET permet une gestion centralisée et en temps réel des accès physiques. Les fonctions d'accès sont gérées par une application « métier » nommée « **Server** » et développée par Fichet Technologies.

Cette application est utilisée, chez le client final, par des responsables de sécurité (des exploitants préalablement formés) qui gèrent toutes les fonctions d'accès à des zones névralgiques ou protégées via des moyens d'identification d'usagers afin de leur attribuer des droits d'accès.

Les droits d'accès sont préalablement définis par le client pour la sécurisation des sites.

L'application Server est entièrement sous contrôle de responsable(s) de sécurité (client final, RSSI).

Cette application répond aux problématiques classiques du Contrôle d'Accès « QUI, QUAND, OU » et permet :

- de définir tous les types d'accès physiques,
- de référencer de façon unique les usagers dans la base de données du Serveur,
- de donner des droits d'accès aux usagers et aux visiteurs,
- de référencer les éléments de sécurité SI (droits d'administration, droits d'accès au SI, clés de sécurité, …).

Pour répondre à ces besoins, la solution SMI Server repose sur les équipements suivants :

- Un Serveur d'applications avec « application métier » et base de données
- Un Serveur de présentation permettant l'interface entre les Postes d'exploitation et le Serveur d'applications
- Des postes d'administration et d'exploitation
- Des concentrateurs d'accès (SM400/SM400-L) avec leur système d'alimentation en énergie (alimentation secourue) et leur kit d'update capteur de vibration obligatoire
- Des contrôleurs de portes (SM100+) avec leur système d'alimentation en énergie (alimentation secourue) et leur kit d'update capteur de vibration obligatoire
- SAM AV2/AV3 de NXP
- Des lecteurs de badges de la gamme ProStyl
- Des badges d'accès (badges basés sur la technologie Mifare® DESFire de NXP)

L'accès à une zone névralgique ou protégée nécessite une identification préalable qui peut être parfois complétée d'une **authentification** via PIN Code (code personnel).

La notion d'authentification PIN Code correspond à la fonction d'accès qui consiste à traiter un élément complémentaire à l'identification tel que défini par l'ANSSI (voir Annexe 2 : niveau de sûreté **IV**).

2.1.4 Raccordements & réseaux

Le serveur et les Postes d'administration et d'exploitation sont raccordés au ***réseau du client***.

Ce réseau est généralement un réseau Ethernet sous TCP/IP qui est établi, maintenu et entièrement administré par le client final.

Ce réseau constitue le réseau fédérateur qui assure les interfaces entre les différents équipements comme le Serveur d'applications et les Postes d'administration et d'exploitation. Plusieurs postes d'administration et d'exploitation peuvent être installés sur ce réseau.

Le **réseau du client** est hors périmètre de l'évaluation CSPN. Ce réseau est repéré 4 sur la Figure 5.

Le **réseau LAN du client** assure les échanges entre le « Server » et les concentrateurs d'accès (SM400/SM400-L).
Les communications entre le « Server » et SM400/SM400-L transitant par ce réseau sont chiffrées en AES conformément aux recommandations de l'ANSSI (Guide « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection »).

2.1.5 Liaisons des équipements

Les liaisons des équipements correspondent à des liaisons filaires basées sur le bus RS485 utilisées exclusivement pour les installations de contrôles d'accès physiques.

Les liaisons ne sont pas partagées avec des équipements autres que ceux présentés dans la cible d'évaluation.

On distinguera 2 cas de liaisons dédiées :

1) **Les liaisons entre équipements SM400/SM400-L et SM100+ :**

   Ces bus de terrain correspondent à des liaisons filaires situées en zones protégées.

   Ces bus assurent des communications sécurisées entre le concentrateur SM400/SM400-L et les contrôleurs de portes SM100+ via des bus dédiés RS485 supportant le protocole SOP.

   Ces bus de terrain sont repérés 6 sur la Figure 5 et font partie du périmètre d'évaluation.

2) **Les liaisons entre les contrôleurs SM100+ et les lecteurs d'accès ProStyl :**

   Ces bus de terrain correspondent à des liaisons filaires donnant généralement sur des zones publiques (*).

   Ces bus assurent des communications sécurisées entre les SM100+ et les lecteurs ProStyl via un bus dédié RS485 supportant le protocole SOP.

   Ces bus de terrain sont repérés 7 sur la Figure 5 et font partie du périmètre d'évaluation.

   (*) Ce cas n'est pas systématique, car cette liaison peut aussi être en zone protégée. D'un point de vue sûreté, une liaison donnant sur une zone publique présente le niveau de vulnérabilité maximum.

Dans les deux cas ci-dessus, les bus RS485 sous protocole SOP présentent un caractère déterministe avec des échanges d'informations en temps réel et permanents.

2.1.6 Serveur d'applications

Rôle : Serveur d'applications pour une gestion centralisée de toutes les fonctions d'accès. Il est développé par Fichet Technologies.

Le serveur d'applications peut être constitué d'un poste informatique sous Microsoft Windows et est doté d'une base de données sous Microsoft SQL. Ce serveur peut aussi être hébergé sous forme de VM dans l'infrastructure du client. Dans ce cas, la VM est implantée/hébergée dans un serveur.

L'installation, la mise à jour et le durcissement du système d'exploitation du serveur sont sous la responsabilité du client final.

Le serveur d'applications dispose d'une interface permettant :

- **La configuration** : Celle-ci permet de définir l'architecture avec les différents équipements déployés sur site(s) au travers d'échanges temps réel et centralisés.
- **L'exploitation** : Celle-ci permet la gestion des accès, des droits des usagers, des alarmes, des événements.

2.1.7 Postes d'administration et exploitation

Rôle : Poste de configuration et d'exploitation

Composés d'un poste informatique sous Microsoft Windows ou à partir d'un navigateur Web.

L'installation, la mise à jour et le durcissement du système d'exploitation des Postes d'administration et exploitation sont sous la responsabilité du client final.

2.1.8 Concentrateur d'accès SM400 / SM400-L

Rôle :

Concentrateur d'accès (gère jusqu'à 16 contrôleurs SM100+ et 32 lecteurs).
Point d'accès LAN pour l'architecture de terrain
Base locale de 50 000 usagers avec leurs droits d'accès
Gestion d'alarmes
Gestion de l'énergie

Le SM400 / SM400-L dispose d'une capacité de gestion autonome en cas de rupture de sa connexion LAN avec « Server » (repérée 5 sur la Figure 5).

Cette capacité repose sur la gestion temps réel des usagers, des droits d'accès, des alarmes et de l'historisation des événements.

Caractéristiques techniques de SM400 :

Composant	Description
Désignation	**SM400 / SM400-L**
Référence produit	**A19914 / A19B74** (ou A19914_8/ A19914_16/A19914_24/A19B74_8/ A19B74_16/A19B74_24 si présence d'une licence logicielle restreignant le nombre d'équipements pouvant être connectés)
Version logiciel	V2.8.6
Emplacement	Zone protégée
Processeur	ARM 9 (AT91SAM9260)
OS embarqué	eCOS (Linux)
Base locale	Base propriétaire par système de fichiers
Données	Données en Flash externe : binaire et système de fichier Secrets et données névralgiques : EEPROM
JTAG / SWD	Désactivé matériellement
AP	Ouverture coffret ; manipulation du coffret accéléromètre (cf §2.1.10)

Liaisons & sécurisations :

- En lien avec l'application « Server » (repère 5 sur la Figure 5)
- En lien avec des contrôleurs de porte SM100+ (repère 6) ; protocole SOP
- Dispose d'une clé usine et d'un identifiant hard unique (MAC)
- Embarque des algorithmes de chiffrement en cryptographie symétrique (AES et ECC)
- Protocole d'échange de clés (DH–ECC)

2.1.9 Contrôleur de portes SM100+ avec son Extension SAM

Rôle : Le SM100+ assure les fonctions d'accès.

Le SM100+ dispose d'une capacité de gestion autonome en cas de rupture de sa connexion avec le concentrateur SM400 (repérée 6 sur la Figure 5).

Cette capacité repose sur la gestion temps réel des usagers, des droits d'accès, des alarmes et de l'historisation des événements.

Caractéristiques techniques du SM100+ :

Composant	Description
Désignation	**SM100+**
Références produit	**A19A28 (Contrôleur SM100+)** **A19A98 (Kit d'extension SAM pour SM100+)** **A19B71 (SM100+SAM)**
Référence logiciel	V4.0.100
Emplacement	Zone protégée
Processeur	Cœur ARM Cortex-M3
OS embarqué	OS TR MT (Temps Réel & Multi Tâches)
Données	En flash interne au processeur
JTAG / SWD	Désactivé
AP	Ouverture coffret ; arrachement ; manipulation du coffret (cf §2.1.10)

Liaisons & sécurisations :

- en lien avec le concentrateur SM400 (repère 6 sur la Figure 5)
- en lien avec 1 ou 2 lecteurs ProStyl (repère 7) ; protocole SOP
- dispose d'une clé usine et d'un identifiant Hard unique (MID)
- embarque des algorithmes de chiffrement en cryptographie symétrique (AES et ECC)
- protocole d'échange de clés (DH–ECC)

2.1.10 Kit obligatoire d'amélioration de la sécurité matérielle

Rôle : Ce kit d'update par capteur de vibration pour SM100+/SM400/SM400-L est un élément de sécurité matérielle obligatoire qui vient protéger les SM100+, les SM400 et les SM400-L contre les attaques par perçage ou manipulation du boitier.

Il est composé d'un boitier métallique venant s'insérer dans le coffret plastique et d'un capteur de vibration fixé à l'intérieur de ce boitier métallique.

Il rend les tentatives d'accès au matériel pour mettre en place des attaques basées sur l'accès à la carte électronique très complexe.

Caractéristique technique du capteur de vibration :

Composant	Description
Désignation	**Kit update CAP DE VIB SM100+/SM400**
Références produit	**A19B86 (Kit tôlerie + capteur + fixation + notice)**
Nature de la protection	Mécanique Vibratoire
Installation	Obligatoire

Protection additionnelle	Détection de la déconnexion du capteur

2.1.11 Lecteurs de badges d'accès ProStyl

Rôle : Identification RFID en mode transparent

Caractéristiques techniques des lecteurs de la gamme ProStyl :

Composant	Description
Désignation	**Lecteurs ProStyl**
Codes produits	**A10553 (ProStyl S)** **ou A10532 (ProStyl à visser)** **ou A10512 (ProStyl à clipser)** **ou A10523 (ProStyl AVL)**
Référence logiciel	V1.1.6
Emplacement	Zone publique ou zone protégée
Processeur	Cœur ARM Cortex-M3 µContrôleur
JTAG / SWD	Désactivé
OS embarqué	OS TR MT (Temps Réel & Multi Tâches)
Mémoire locale	Flash dans µC
AP	Détection arrachement

Liaisons & sécurisations :

- en lien avec le SM100+ (repère 7 sur la Figure 5)
- communication avec le badge en mode transparent

2.1.12 Lecteurs de badges d'accès ProStyl B

Rôle : Identification RFID ou Bluetooth en mode transparent

Caractéristiques techniques des lecteurs de la gamme ProStyl :

Composant	Description
Désignation	**Lecteurs ProStyl**
Codes produits	**A10558 (ProStyl B)**
Référence logiciel	V1.8.9
Emplacement	Zone publique ou zone protégée
Processeur	Cœur ARM Cortex-M4 µContrôleur
OS embarqué	OS TR MT (Temps Réel & Multi Tâches)
Mémoire locale	Flash dans µC
JTAG / SWD	Désactivé
AP	Détection arrachement
BLE	5.0

Liaisons & sécurisations :

- en lien avec le SM100+ (repère 7 sur la Figure 5)
- communication avec le badge en mode transparent

2.1.13 Lecteurs claviers de la gamme ProStyl

Rôle : Identification RFID mode transparent et authentification PIN code

Caractéristiques techniques des lecteurs claviers de la gamme ProStyl :

Composant	Description
Désignation	**ProStyl K et ProStyl-Clavier**
Code produit	**A10554 (ProStyl K) et A10535 (ProStyl-Clavier)**
Référence logiciel du lecteur RFID	V1.1.6
Référence logiciel du clavier	V1.0.6
Emplacement	Zone publique ou zone protégée
Processeur	Cœur ARM µContrôleur
OS embarqué	OS TR MT (Temps Réel & Multi Tâches) pour la partie lecture et NON pour la partie clavier
Mémoire locale	Flash dans µC
JTAG / SWD	Désactivé
AP	Détection arrachement

Liaisons & sécurisations :

- en lien avec le SM100+ (repère 7 sur la Figure 5)
- Clé d'authentification négociée avec SM100+ à l'installation
- Dispose d'une clé usine et d'un identifiant Hard unique (MID)
- Embarque des algorithmes de chiffrement en cryptographie symétrique (AES et ECC)
- Protocole d'échange de clés (DH–ECC)

2.2 Description de l'environnement d'utilisation du produit

L'approche de la *sécurité électronique* amène FICHET à travailler avec ses clients pour prendre en considération différents points importants tels que :

- La gestion de la sécurité (moyens techniques et organisationnels)
- Le référencement des identités
- Le Système d'Information (SI)
- Une implantation sur différents sites (pays/langues ou territoires/multi-sites)
- Un système de contrôle des accès répondant aux règles de sûreté

Pour répondre aux besoins actuels du marché de contrôles d'accès physiques et sécurisés par badges RFID basés sur la technologie Mifare® DESFire EV2/EV3 de NXP avec mécanismes de chiffrements, nous prenons en considération les bases suivantes :

- Chiffrements de l'interface air entre le badge d'accès et le lecteur ProStyl : **AES**
- Mode opératoire des lecteurs ProStyl : **Transparent**
- Présence de clés de sécurité dans le lecteur ProStyl : **Aucune clé dans les lecteurs ProStyl, sauf une clée de session en RAM pour le chiffrement du PIN sur les parties clavier des ProStyl K et ProStyl-Clavier.**
- Traitement des fonctions sécurisées des badges dans le contrôleur SM100+ : **Toutes les fonctions sécurisées en lectures (*)**
- Données névralgiques et clés : **Dans le composant SAM**

Le mode transparent correspond au schéma de l'architecture hautement recommandée par l'ANSSI :

Figure 2 : Architecture hautement recommandée par l'ANSSI

Cette architecture regroupe le canal sans fil (Interface RF avec le badge) et la liaison filaire avec l'UTL.

L'UTL correspond au contrôleur de portes SM100+.

(*) Ces fonctions sont celles du Tableau de l'annexe D.1 du Guide ANSSI « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection ». Ce tableau est renseigné en Annexe 2 de ce document.

Pour l'évaluation, les niveaux de sûreté sont les **niveaux III et IV.** Les données névralgiques et les clés sont **protégées au niveau du contrôleur de portes SM100+**.

2.3 Descriptions des fonctions d'accès

2.3.1 Identification RFID

Les badges d'accès ont plusieurs origines possibles :

- Fournisseur spécialisé et retenu pour des marchés gouvernementaux (par exemple : un Ministère, un opérateur de téléphonie)
- Achat par le client final. Solution badge Corporate multi applicatif
- Fournisseur FICHET. Dans ce cas, la sécurité du support est assurée par un marquage au verso. Ce marquage permet d'assurer la traçabilité des lots de badges livrés au client.

2.3.2 Identification avec confirmation par PIN Code

Cette fonction est paramétrable depuis l'application SMI Server et conditionne la fonction de contrôle de l'accès au niveau du contrôleur SM100+ (Badge + code PIN).

2.3.3 Documents en référence

- Manuel de mise en conformité CSPN (réf. A0U609)

2.4 Descriptions des hypothèses sur l'environnement du produit

« Le système de contrôle d'accès est un système d'informations (SI) à part entière. Il doit donc être sécurisé comme tout SI et ce, d'autant plus qu'il traite des informations personnelles sensibles » (Source ANSSI pour le contrôle des accès physiques).

La solution SMI Server fait partie du SI du client final. Dans ce sens, elle hérite des protections mises en place. Dans certains cas (tels que les ministères), un audit préalable de sûreté est conduit par des autorités compétentes et ce, avant la mise en service d'une solution d'accès sécurisée. Cet audit porte sur la sécurisation des locaux et sur la sécurisation du SI.

2.4.1 Hypothèses sur l'environnement physique du produit

- **Installation du serveur :**

  Il est supposé que le serveur est installé dans un local informatique sécurisé en zone névralgique dont l'accès est strictement limité aux personnels habilités.

- **Installation des postes d'administration et d'exploitation :**

  Les équipements d'administration, ainsi que tous supports contenant des données sensibles (papier ou clés USB, sauvegardes, ...) doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

- **Installation du concentrateur SM400 ou SM400-L :**

  Le concentrateur d'accès SM400/SM400-L ainsi que le système d'alimentation secourue sont installés dans un local technique sécurisé dont l'accès est limité aux personnels habilités.

  Les SM400 et SM400-L sont installés sur des parois robustes et sans vibrations.

- **Installation du concentrateur SM100+ :**

  Les contrôleurs de portes SM100+ sont installés sur des parois robustes et sans vibrations.

- **Installation des lecteurs ProStyl :**

  Les lecteurs de la gamme ProStyl sont installés en zone publique, protégée et névralgique.

  Aucun câble, ni aucun équipement ne sont posés/installés en zone non protégée, à l'exception du lecteur de badge.

  Le câble de raccordement des lecteurs de badge doit être traversant. Il ne doit pas courir le long de la porte en zone non protégée, même au travers d'une goulotte ou d'un tube de protection.

  Le Bus RS485 assurant la liaison entre les lecteurs de la gamme ProStyl et les contrôleurs SM100+ est supposé direct.

  Le câblage de l'ensemble des équipements constituant les environnements de porte est direct, point à point.

2.4.2 Hypothèses sur les administrateurs du produit

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels et sont supposés de confiance.

2.4.3 Hypothèses sur les exploitants du produit

La solution d'accès SMI Server nécessite une exploitation (poste de surveillance, gestion des alarmes en temps réel ; ajout, suppression d'usagers, gestion des exceptions, …). Un exploitant est soit un employé du client, soit un employé d'une société de service en contrat avec le client. Un ou plusieurs exploitants peuvent agir sur SMI Server.

Dans tous les cas, l'exploitant reçoit une formation sur le système. D'autre part, le ou les exploitants dispose(nt) des prérogatives déterminées par le responsable sûreté du client qui limite les droits d'accès à la solution. Le responsable sûreté du client peut être l'administrateur de la solution.

- **Maitrise de la configuration :**

  L'administrateur dispose des moyens de contrôler la configuration matérielle et logicielle de l'ensemble du dispositif.

  Des sauvegardes régulières des configurations et de la base de données sont vivement recommandées.

- **Maitrise du système :**

  Le système d'exploitation Microsoft Windows est maintenu à jour et configuré dans ses différentes versions (exemples : Windows 10, Windows 11, Windows Server 2019 et 2022).

  En particulier, les accès aux différents composants tels que la base de données, les drivers, les paramétrages des connexions, ne sont accessibles qu'aux seuls utilisateurs autorisés.

  L'installation, la mise à jour et le durcissement des systèmes d'exploitation sont sous la responsabilité du client final. Il convient notamment de changer régulièrement les mots de passes. SMI l'imposera automatiquement et régulièrement.

2.4.4 Hypothèses sur les usagers (porteurs de badges)

Les usagers correspondent soit à des employés, des visiteurs, soit à des sous-traitants externes.

La solution SMI Server permet au responsable de la sécurité d'affecter à ces différents types d'usagers des badges sans contact avec le même niveau de sécurité. Ces niveaux correspondent aux Niveaux III ou IV du tableau en Annexe 2.

La technologie retenue par FICHET pour les sites sécurisés est Mifare® DESFire EV2/EV3.

Le PIN code personnel est attribué par le responsable de la sécurité et selon une logique de référencement des usagers.

Les règles de sécurité doivent être appliquées (bonnes pratiques) :

- Pas de prêt d'un badge.
- Passage uniquement.
- Ces porteurs sont supposés ne réaliser de demande d'accès que pour leur usage personnel et ne pas permettre l'accès à toute autre personne (tiers et collègues inclus).
- Ils sont supposés ne pas confier leur badge, ni communiquer leur code PIN personnel.

2.4.5 Hypothèses sur l'environnement technique du produit

- L'application SMI Server fonctionne dans un environnement Windows qui est protégé des virus et ne permet pas l'exécution de code malveillant. Ses protections sont maintenues à jour.
- Les mises à jour de sécurité et les outils Windows sont installés dès que disponibles.
- Seules les suites cryptographiques recommandées par l'ANSSI sont activées sur les postes Windows (pour plus de détails sur la configuration, voir « Manuel de mise en conformité CSPN » (réf. A0U609)).
- Le niveau de protection du canal d'échange entre le « Server » et le concentrateur SM400 ou SM400-L est décrit dans le document « Fournitures cryptographiques » (réf. A0Y010).
- Il existe un compte administrateur doté de tous les privilèges de configuration et exploitation.
- Il existe un compte exploitant doté de privilèges restreints, et réservé à l'utilisation courante du système.
- Les certificats sont gérés par le client conformément aux recommandations en vigueurs par l'ANSSI.
- Le serveur utilise les API Windows et le Framework .NET pour les opérations cryptographiques. L'implémentations de ces fonctions est supposée robuste.
- Les communications utilisant TLS et HTTPS utilisent des certificats générés par le client et conformes aux préconisations de l'ANSSI.

Les réseaux :

Le réseau LAN du client est placé en zone protégée.

Le réseau du client LAN et la **liaison des équipements** sont physiquement et logiquement séparés, aucune passerelle informatique ou de transmission de données ne peut y être installée.

Les échanges de données passent systématiquement par le concentrateur SM400 (ou SM400-L). Dans le cas de téléchargements depuis « Server » vers des SM100+, les données sont routées via les concentrateurs SM400 (ou SM400-L).

Protection en transmission de l'identifiant d'accès (ID) :

L'ID (identifiant personnel) d'un usager est encodé dans une application de son badge d'accès (application d'accès dans un badge DESFire EV2/EV3).

Cet ID est protégé en lecture par un chiffrement en AES avec clé diversifiée.

La confidentialité, lors de la transmission dans l'interface air (badge/lecteur) et jusqu'au SM100+, est assurée par les mécanismes d'échanges Mifare® DESFire EV2/EV3 (APDU et cryptographie DESFire EV2/EV3).

Sécurisation des clés dans le contrôleur de portes SM100+

Les clés sont stockées dans un composant physique hautement sécurisé, le Secure Access Module (SAM).

Les modules SAM de type NXP SAM AV2/AV3 héritent d'une certification CC EAL5+. Les fonctions de sécurité liées aux lectures sécurisées via le SAM sont décrites dans le document « Fournitures Cryptographiques » (A0Y010).

Voir 9.4 « Annexe 4 : Certification du SAM » pour les certificats SAM AV2/AV3.

Sécurisation des postes :

Les postes d'administration et d'exploitation sont placés en zone protégée.

L'utilisation de ces postes est soumise à l'ouverture d'une session Windows avec une politique conforme aux recommandations de l'ANSSI : mots de passe sécurisés, changements périodiques des mots de passe, … (voir Guide ANSSI « Recommandations relatives à l'authentification multifacteur et aux mots de passe »).

2.5 Description des utilisateurs types

2.5.1 Exploitants

Voir 2.4.2 « Hypothèses sur les administrateurs du produit ».

L'exploitant a pour fonction de configurer et adapter au quotidien les différentes fonctions du système qui concourent à attribuer des autorisations d'accès sur l'ensemble des portes et obstacles physiques contrôlés.

Toute connexion des exploitants au système de gestion est tracée dans l'historique des événements.

2.5.2 Agents techniques

Les agents techniques sont des personnes intervenant dans le cadre des opérations de mise en service (déploiements) et de maintenance (techniciens) et à ce titre, peuvent être amenés à intervenir sur les différents équipements du système.

Toute connexion des agents techniques au système de gestion est tracée dans l'historique des événements.

2.5.3 Usagers

Les usagers sont les utilisateurs finaux de la solution SMI Server. Pour accéder aux zones névralgiques ou aux zones protégées, ils disposent de badges sans contact (RFID) DESFire EV2/EV3 et éventuellement de code PIN personnel.

Trois populations d'usagers sont concernées par les accès avec badges RFID :

- Employés ou résidents,
- Visiteurs,
- Prestataires, intervenants ou stagiaires.

Pour les accès véhicule, deux cas sont à considérer :

- Gestion de badges de proximité et sécurisés, **niveaux III et IV** du tableau en Annexe 2.
- Gestion d'accès avec lecture de plaques d'immatriculation ou de badges longue portée (hors périmètre de l'évaluation).

2.6 Description du périmètre d'évaluation

La Cible de Sécurité prévoit l'évaluation de la sécurité des fonctions de contrôle d'accès gérées par les équipements suivants :

- Le logiciel SMI Server
- Le concentrateur d'accès SM400 / SM400-L, équipé du kit d'update par capteur de vibration
- Les contrôleurs de portes SM100+ dotés de l'Extension SAM et du kit d'update par capteur de vibration
- Les lecteurs de badges de la gamme ProStyl

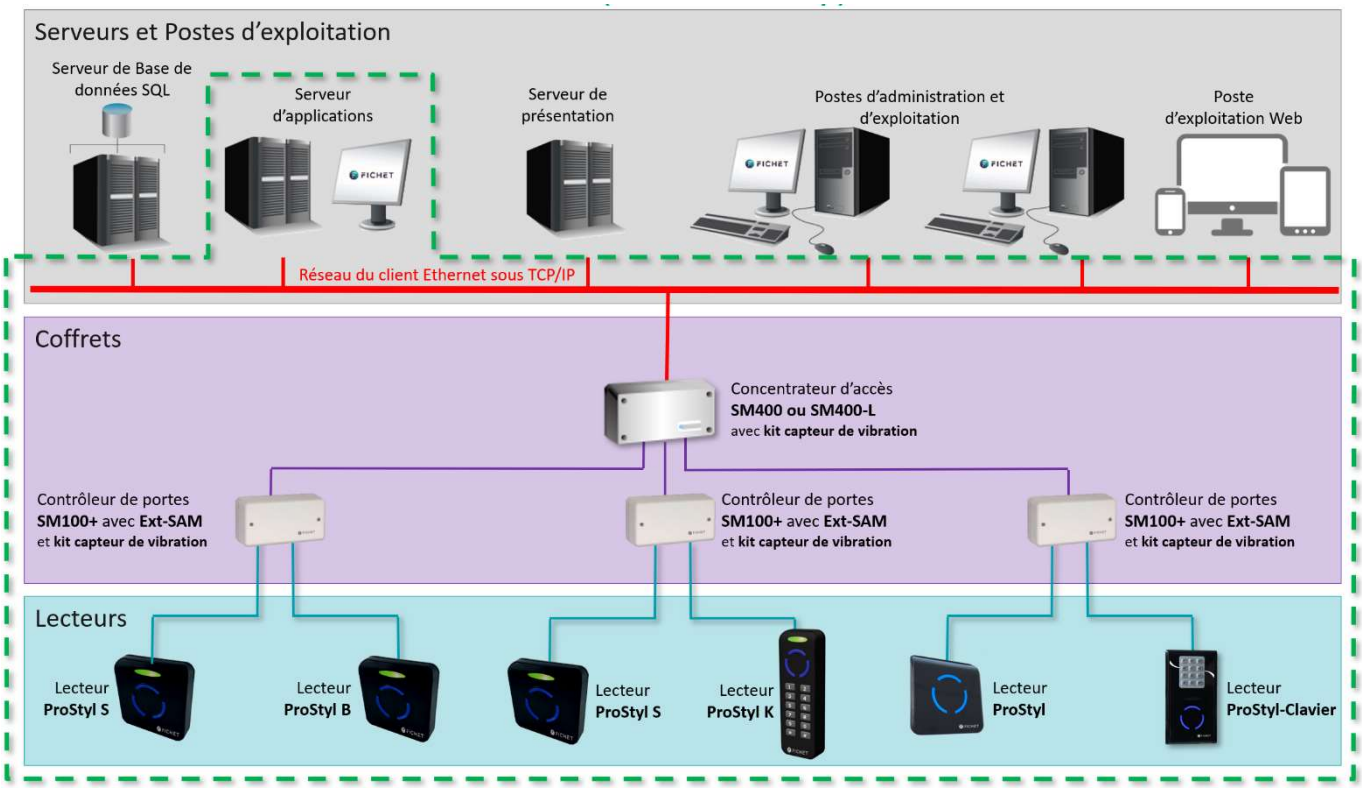

Figure 3 : Périmètre d'évaluation

Configuration d'évaluation 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 10 Windows 11 Windows Server 2019 Windows Server 2022**	
	Serveur d'applications	**SMI Server 4.6**		
	Fonctions cryptographiques	**.Net 4.8 LibCom 4.0.10**		
	Bases de données et annuaires		**SQL Server 2019 SQL Server 2022**	
UTL	Système d'exploitation	**SM400 / SM400-L : Ecos 3.0 SM100+ : Keil RTX 4.80**		
	Applicatifs	**SM400(-L) : 2.8.6 SM100+ : 4.0.100**		
	Fonctions cryptographiques	**OpenSSL 3.0.15 WPA supplicant 2.11 LibCom 4.0.10 Mongoose 7.12**		
	SAM		**SAM NXP AV2/AV3**	
Lecteurs	Lecteurs simples	**ProStyl S 1.1.6 ProStyl 1.1.6 ProStyl AVL 1.1.6 ProStyl B 1.8.9**		
	Lecteurs-clavier	**Logiciel du clavier du ProStyl K : 1.0.6 Logiciel du lecteur du ProStyl K : 1.1.6 Logiciel du clavier du ProStyl-Clavier 1.0.6 Logiciel du lecteur du ProStyl-Clavier : 1.1.6**		
Badges			**DESFire EV2/EV3**	

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 Dispositif d'accès

Gestion d'environnement d'accès disposant des équipements minimums :

- Détecteur d'ouverture de porte (état de la porte / contact de verrouillage)
- Contact sec de confirmation de passage pour les obstacles physiques
- Sortie libre par bouton poussoir (commande de sortie)
- Entrée/Sortie par lecture de badge (lecteur)
- Organe de serrurerie condamnant l'accès (commande par contact sec et alimentation secourue)

3.2 Dispositifs de raccordements et d'alimentation

Les raccordements des équipements figurent dans le schéma la Cible de Sécurité (voir Figure 1).

S'y ajoutent :

- Les raccordements des équipements mentionnés au paragraphe 3.1 ci-dessus.
- Les alimentations secourues.

3.3 Poste informatique

- SMI Server
- Windows 10, Windows 11, Windows Server 2019 et Windows Server 2022
- Microsoft Windows SQL Server 2019 ou 2022
- Microsoft .NET Framework 4.8

3.4 Badges

Badges d'accès sécurisés basés sur la technologie NXP Mifare® DESFire EV2/EV3 :

- Badges livrés pré-encodés selon les différents niveaux de sécurité
- Badges encodés à partir de l'application d'accès SMI Server

Dans tous les cas, les badges correspondront **aux niveaux III et IV** du tableau des niveaux de sûreté présenté en Annexe 2.

Le traitement des algorithmes et des clés est réalisé par le SAM qui se trouve dans le SM100+.

4 DONNEES NEVRALGIQUES & SENSIBLES

Biens et données sensibles	Intégrité	Confidentialité	Disponibilité
Identifiants des usagers		X	
Codes PIN des usagers		X	
Droits d'accès des usagers	X	X	
Droits des opérateurs	X	X	
Mots de passe des administrateurs		X	
Clés	X	X	
Logs des usagers	X		X
Logs du GAC	X		X
Firmwares SM400/SM400-L, SM100+, gamme **ProStyl**	X		

4.1 Descriptions

Les données névralgiques confidentielles regroupent plusieurs types d'informations :

- Clés :
  - Clés AES de lecture/écriture liées à la sécurité des badges d'accès décrits au chapitre ·
  - Clés mères

Note :
Les clés AES et les clés mères sont sous contrôle de responsable(s) de la sécurité (Exploitant(s) ou RSSI) et protégées par la solution SMI Server.

- Identifiant d'accès :
  - **AID** DESFire pour les applications du badge d'accès

Les données confidentielles sensibles regroupent en plus :

- Les identifiants individuels (ID) des usagers
- Les codes PIN des usagers
- Les droits d'accès des usagers (gérés par le concentrateur SM400/SM400-L et le contrôleur SM100+)
- Les logs et événements
- Les firmwares des SM400/SM400-L, SM100+, de la gamme des ProStyl

4.2 Données sensibles dans le contrôleur de portes SM100+

Les données sensibles protégées par le SM100+ sont les suivantes :

Donnée sensible	Usages
Clé de déverrouillage du SAM	Déverrouillage du SAM
AID	Accès à une application du badge
Clé mère	Calcul de clé(s) diversifiée(s)
Diversifiant	Calcul de clé(s) diversifiée(s)
ID	Identifiant du badge
PIN code	Authentification

Les données sensibles destinées aux lectures sécurisées sont protégées dans « un module SAM Physique » qui contient un coffre de clés. Ce module s'intègre au niveau du SM100+ via son Extension SAM.

Les modules SAM de type NXP SAM AV2/AV3 héritent d'une certification CC EAL5+. Les fonctions de sécurité liées aux lectures sécurisées via le SAM sont décrites dans le document « Fournitures Cryptographiques » (A0Y010).
Voir 9.4 « Annexe 4 : Certification du SAM » pour les certificats SAM AV2/AV3.

Le diversifiant est une donnée utilisée, selon l'algorithme de diversification, pour le calcul des clés sécurisées tel qu'indiqué dans le tableau des niveaux de sûreté présenté en Annexe 2.

4.3 Données sensibles dans les lecteurs d'accès de la gamme ProStyl

Aucune donnée sensible n'est présente dans les lecteurs de la gamme ProStyl (fonctionne en mode tunnel/transparent).

4.4 Données sensibles dans le lecteur clavier ProStyl

Pour les fonctions clavier, les services de sécurité assurent :

- La protection en confidentialité de l'identifiant personnel (ID)
- La protection en confidentialité du code PIN

4.5 Données sensibles dans SMI Server

- Identifiants opérateur (ID et mot de passe)
- Profils opérateur
- Données utilisateurs (identifiant du badge, code PIN, droits d'accès)
- Evènements de contrôle d'accès
- Evènements du GAC

5 MESURES D'ENVIRONNEMENT

5.1 Environnement

La solution SMI Server s'intègre dans l'environnement du client final.

En tant que solution d'accès, la solution SMI Server s'intègre ou est couplée au SI du client.

- Pour répondre aux exigences de sécurité, les équipements doivent être installés en respectant les emplacements ci-dessous :

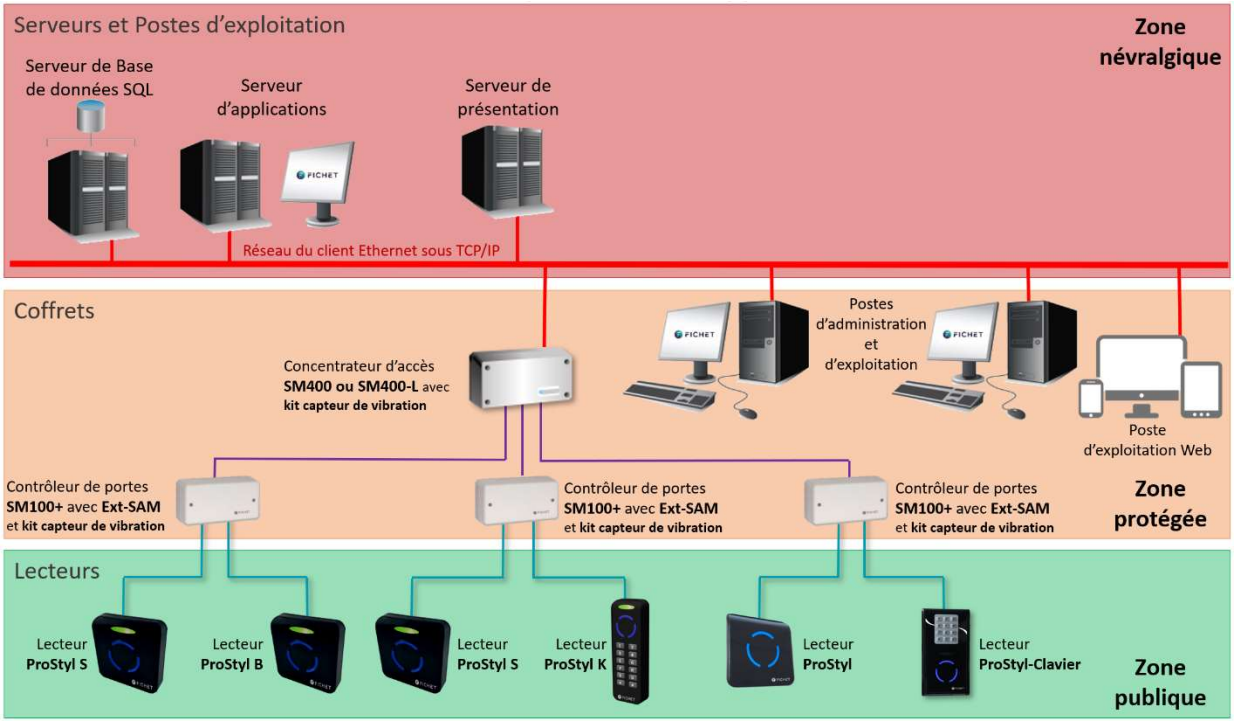

Figure 4 : Mesures d'environnement

- Dans certains cas, un audit de sécurité est établi afin de vérifier les zones et la sécurisation du SI.

5.2 Organisations

La solution SMI Server est une solution centralisée qui nécessite un minimum d'organisation :

- Responsable sûreté avec des droits d'administration
- RSSI (topologie du réseau, plan d'adressage, mise à jour des logiciels, gestion des mots de passe ; création et déploiement des certificats X509v3)
- Opérateur(s) (surveillance des écrans sur les postes, prise en compte des alarmes, gestion/signalement des incidents, verrouillage des postes non utilisés)

5.3 Mesures de sécurité

Sur un plan organisationnel, les mesures de sécurité font partie des « bonnes pratiques ». Elles doivent être portées à la connaissance des personnes en charge de la sécurité des sites.

Selon l'organisation du client, ces mesures sont diffusées via intranet ou sous forme papier (circulaire, notes, documents confidentiels).

- La remise des clés ou « cérémonie des clés » fait partie des mesures sécuritaires
- Les consignes font partie des mesures sécuritaires :
  - Cas de perte ou de vol d'un badge
  - Cas d'un oubli d'un badge ou d'un PIN code
  - Cas des interventions sur les équipements de la cible de sécurité
  - Cas des alarmes techniques (coupure d'alimentation, autoprotections, défaut de communications).
- Les mises à jour régulières font partie des mesures sécuritaires :
  - Suppression d'un usager et de ses droits
  - Suppression d'un badge
  - Ajout d'un usager avec son badge
  - Vérifications régulières de l'unicité des couples (ID, PIN)

Les consignes de sécurité sont décrites dans le « Manuel de mise en conformité CSPN » (réf. A0U609).

6 DESCRIPTION DES MENACES

Différentes **attaques logiques** sont considérées :

- Attaquant sur le réseau TCP/IP établi entre le « Server », le concentrateur SM400 (ou SM400-L) et les postes d'administration et d'exploitation
- Attaquant sur le réseau dédié RS485 entre le concentrateur SM400 (ou SM400-L) et les contrôleurs de portes SM100+
- Attaquant externe sur la liaison RS485 établie entre les lecteurs de la gamme ProStyl et le contrôleur SM100+

Pour ces attaques, les agents menaçants sont :

- de type interne :
  - tout utilisateur autorisé se situant en zone névralgique ou protégée,
  - exploitant : disposant de droits d'accès limités et souhaitant augmenter ses droits
  - toute personne ayant accès au réseau TCP/IP qui relie le « Server », le concentrateur SM400/SM400-L et les postes d'administration et d'exploitation
- de type externe : toute personne extérieure à la zone névralgique ou protégée

Différentes **attaques physiques** sont considérées :

- Attaque sur un concentrateur SM400 / SM400-L équipé du kit update capteur de vibration obligatoire (réf. A19B86)
- Attaque sur un contrôleur SM100+ équipé du kit update capteur de vibration obligatoire (réf. A19B86)
- Attaque sur un lecteur de la gamme ProStyl

6.1 Intrusion externe

Cette intrusion concerne le réseau LAN Ethernet TCP/IP (repères 1, 2, 3, 4 et 5 sur la Figure 5) et correspond à une Intrusion sur le réseau LAN du client.

Les **attaques logiques** portent sur l'interception de données sensibles ou d'injection de données /commandes.

L'attaquant dispose de moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes.

Selon le Guide ANSSI « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » (Chapitre 3.4), l'intrusion correspond au :

- **Niveau III** avec franchissement par attaque logique simple. L'attaquant dispose de matériels ou maquette électronique spécifique facilement réalisable.
- **Niveau IV** avec franchissement par attaque logique sophistiquée. L'attaquant dispose de matériels comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place.

Ecoute transactions échangées sur le LAN	Menaces
Ecoute d'une transaction contenant l'ID	Copie du badge
Ecoute d'une transaction contenant le Code PIN	Usurpation d'identité (Authentification PIN par le malveillant)
Ecoute d'une transaction contenant les plages horaires	Elargir des périodes d'accès
Ecoute d'une transaction contenant l'affectation des droits	Modifier/étendre des droits
Ecoute d'une transaction contenant des commandes	Ouverture d'un accès
Ecoute des transactions avec le Host	Emulation d'un concentrateur SM400(-L)
Ecoute des communications des postes opérateurs vers le SMI Server	Usurpation droits et extension de droits
Ecoute des communications des postes web vers le SMI Server	Usurpation droits et extension de droits
Ecoute des communications des postes opérateurs vers le SMI Server	Usurpation droits et extension de droits
Ecoute des communications entre le serveur d'applications et le serveur de présentation	Usurpation droits et extension de droits
Compromission de SMI Server	Menaces
Elévation de privilège d'un opérateur	Etendre des droits
Usurpation d'un opérateur	Etendre des droits
Altération de SMI Server	Menace
Altération du serveur d'applications	Etendre des droits
Altération du serveur de présentation	Etendre des droits
Altération/saturation des événements du contrôle d'accès	Masquer/modifier des évènements
Altération/saturation des évènements applicatifs	Masquer/modifier des évènements
Altération des données utilisateurs	Usurpation droits et extension de droits
Altération des profils opérateurs	Usurpation droits et extension de droits
Rejeu de commande	Usurpation droits et extension de droits

6.2 Intrusion sur les liaisons des équipements

Cette intrusion concerne la topologie des bus RS485 (repères 6 et 7 sur la Figure 5) et correspond à une intrusion sur des infrastructures filaires (bus).

Les **attaques logiques** portent sur l'interception de données sensibles ou d'injection de données /commandes.

L'attaquant dispose de moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction ou de commandes.

Selon le Guide ANSSI « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » (Chapitre 3.4), l'intrusion correspond au :

- **Niveau III** avec franchissement par attaque logique simple. L'attaquant dispose de matériels ou maquette électronique spécifique facilement réalisable.
- **Niveau IV** avec franchissement par attaque logique sophistiquée. L'attaquant dispose de matériels comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place.

Transaction /échanges	Menaces
Ecoute/ rejeu d'une transaction contenant l'ID	Copie du badge
Ecoute/rejeu d'une transaction contenant le Code PIN	Usurpation d'identité (Authentification PIN par le malveillant)
Ecoute/ génération d'une transaction contenant les plages horaires	Elargir des périodes d'accès
Ecoute/ génération d'une transaction contenant l'affectation des droits	Modifier/étendre des droits
Ecoute/ rejeu d'une transaction contenant des commandes	Ouverture d'un accès
Ecoute/ rejeu des transactions avec le concentrateur SM400/SM400-L	Emulation d'un ou plusieurs SM100+

6.3 Attaque sur SM400 / SM400-L

Tentative de cryptanalyse.

Substitution d'un concentrateur.

Ouverture de boîtier avec neutralisation du capteur de vibration.

6.4 Attaque sur SM100+

Tentative de cryptanalyse.

Substitution d'un contrôleur.

Ouverture de boîtier avec neutralisation du capteur de vibration.

6.5 Attaque sur lecteur de la gamme ProStyl

Tentative de remplacement du lecteur.

Emulation/substitution.

Ouverture de boîtier.

7 DESCRIPTION DES FONCTIONS DE SECURITE

7.1 Hypothèses sur les administrateurs

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels et sont supposés de confiance.

Les postes d'administration et d'exploitation sont accessibles uniquement par des personnes habilitées et considérées de confiance.

Pour plus de détails, voir le « Manuel de mise en conformité CSPN » (réf. A0U609).

7.2 Fonctions de sécurité

La fonctionnalité principale de SMI Server est de fournir au client la capacité de mettre en œuvre une solution d'accès sécurisée dans sa propre infrastructure réseau.

Cette mise en œuvre passe par :

- La définition des sites, des zones et leur niveau de sécurité, des points d'accès (locaux ou portes)
- La définition d'une architecture adaptée au contrôle des flux (transfert d'informations)
- L'adoption d'une politique de sécurité cohérente et non ambiguë par rapport aux moyens organisationnels
- L'application d'une politique d'identification (identifiant unique et code PIN pour chaque usager)
- L'exploitation des audits analyse/consultation des historiques
- La mise en place d'une politique de sécurité pour les clés (génération, protection, mise à la clé des contrôleurs d'accès)

En dehors de la mise en œuvre du système SMI Server, le système intègre des fonctions de sécurité :

- Authentification des opérateurs
- Protection des communications entre les postes opérateurs et le Serveur d'applications
- Protection des communications entre les Postes web et le Serveur de présentation
- Protection des communications entre le Serveur de présentation et le Serveur d'applications
- Définition de la gestion des droits et des profils opérateurs
- Protection contre l'altération des événements de contrôle d'accès
- Protection contre l'altération des logiciels embarqués et accès au mode debug
- Protection contre l'altération des évènements du GAC

Les protections :

P1 : Protection des codes PIN et des identifiants des badges

Les codes PIN (CIP) et les identifiants des badges sont chiffrés en AES.

P2 : Protection des données échangées entre le « Server » et le concentrateur SM400 (ou SM400-L)

Cette protection passe par l'établissement d'un canal de communication chiffré, les deux parties ayant ouvert une session avec une authentification mutuelle au préalable.

Les commandes et les transactions échangées entre le « Server » et le concentrateur SM400 (ou SM400-L)sont protégées en confidentialité et intégrité.

Pour les tentatives de rejeu, la protection passe par la mise en œuvre des mécanismes cryptographiques décrits dans le document « Fournitures Cryptographiques » (A0Y010).

- Les mécanismes d'authentification sont décrits dans le document « Fournitures Cryptographiques » (A0Y010).
- Le protocole d'échange de clés est décrit dans le document « Fournitures Cryptographiques » (A0Y010).

P3 : Protection des données échangées entre le concentrateur SM400(-L) et le contrôleur SM100+

Cette protection passe par l'établissement d'un canal de communication chiffré, les deux parties ayant ouvert une session avec une authentification mutuelle au préalable.

Les commandes et les transactions échangées entre le concentrateur d'accès SM400 (ou SM400-L) et le contrôleur de portes SM100+ sont protégées en confidentialité et intégrité.

Pour les tentatives de rejeu, la protection passe par la mise en œuvre des mécanismes cryptographiques décrits dans le document « Fournitures Cryptographiques » (A0Y010).

- Les mécanismes d'échange, d'authentification et les aspects déterministes sont décrits dans le document « Fournitures Cryptographiques » (A0Y010).
- Le protocole d'échange de clés est décrit dans le document « Fournitures Cryptographiques » (A0Y010).

P4 : Sécurisation du contrôleur de portes SM100+

Le contrôleur de portes SM100+ est placé en zone protégée. Il est équipé obligatoirement du kit update par capteur de vibration (réf. A19B86).

La détection de défauts génère systématiquement des alarmes techniques vers le serveur.

Cette détection concerne ces types de défaut :

- AP (arrachement),
- OC (Ouverture Coffret),
- Défaut communication du bus RS485 (repère 6 sur la Figure 5). Le défaut communication est analysé par le concentrateur SM400.
- Détection de vibrations inhabituelle dues au percement ou à la manipulation du boitier.

P5 : Sécurisation du concentrateur d'accès SM400 / SM400-L

Le concentrateur d'accès SM400 / SM400-L est placé en zone protégée. Il est équipé obligatoirement du kit update par capteur de vibration (réf. A19B86).

La détection de défauts génère systématiquement des alarmes techniques vers SMI Server.

Cette détection concerne ces types de défaut :

- OC (Ouverture Coffret),
- Défaut communication du LAN (repère 5 sur la Figure 5). Le défaut communication est analysé par SMI Server.
- Détection de vibrations inhabituelle dues au percement ou à la manipulation du boitier.

P6 : **Sécurisation des lecteurs claviers de la gamme ProStyl**

Les lecteurs claviers ProStyl utilisent une clé de session déterminée lors de l'échange initial de clés (« Initial Key exchange » décrit dans « Fournitures Cryptographiques » (A0Y010)) pour assurer la sécurisation des remontées des codes PIN vers le contrôleur SM100+.

- A l'installation, une clé d'authentification est négociée entre le contrôleur SM100+ et chaque lecteur clavier ProStyl : il y a appairage.

  La mise en place d'une négociation de clé entre le contrôleur SM100+ et le lecteur clavier ProStyl à travers les échanges SOPKE est documentée dans « Fournitures Cryptographiques » (A0Y010).

- En cas de substitution d'un lecteur clavier ProStyl, la communication du contrôleur SM100+ est bloquée avec cet équipement et un « **défaut authentification ProStyl-Clavier** » est remonté vers SMI Server.
- Pour débloquer la communication du contrôleur SM100+ avec un lecteur clavier ProStyl (cas d'un échange d'un lecteur clavier ProStyl en maintenance par exemple), **une intervention d'une personne habilitée doit être réalisée** au niveau du contrôleur SM100+.

  Dans ces deux cas, les procédures à appliquer sont décrites dans le « Manuel de mise en conformité CSPN » (réf. A0U609).

P7 : **Protection des clés**

Les clés sont stockées et chiffrées par une clé asymétrique RSA.

P8 : **Authentification des opérateurs**

L'authentification des opérateurs repose sur un principe d'identifiant et mot de passe.

Ce mode répond à des paramètres de complexité et de durée de vie répondant aux standards recommandés par le Guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe ».

P9 : **Protection des mots de passe des opérateurs**

Au niveau de la base de données, les mots de passe des usagers sont sécurisés à l'aide d'un algorithme de hachage.

P10 : Protection des communications

- **Protection des communications entre les Postes d'administration et d'exploitation, et le Serveur d'applications**

  Les communications entre le Serveur d'applications et les Postes d'administration et d'exploitation sont chiffrées grâce au protocole TLS 1.2, gérées par l'OS (Windows), et l'authentification mutuelle est réalisée par l'utilisation de certificats.

  Ces éléments permettent de garantir la confidentialité et l'intégrité de la liaison.

  Seules les suites cryptographiques validées par l'ANSSI sont actives sur les postes clients et serveurs.

  Ces suites sont spécifiées dans le guide ANSSI « Recommandations de sécurité relatives à TLS ».

  Pour plus de détails, voir le « Manuel de mise en conformité CSPN » (réf. A0U609).

- **Protection des communications entre le Serveur de présentation et les Postes d'exploitation web**

  Les communications entre le Serveur de présentation et les Postes d'exploitation web sont chiffrées grâce au protocole HTTPS et gérées par l'OS (Windows et IIS).

  Seules les suites cryptographiques validées par l'ANSSI sont actives sur le serveur.

  Ces suites sont spécifiées dans le guide ANSSI « Recommandations de sécurité relatives à TLS ».

  Pour plus de détails, voir le « Manuel de mise en conformité CSPN » (réf. A0U609).

- **Protection des communications entre le Serveur d'applications et le Serveur de présentation**

  La communication entre le Serveur d'applications et le Serveur de présentation utilise une liaison sécurisée via TLS 1.2 gérée par l'OS (Windows).

  Seules les suites cryptographiques validées par l'ANSSI sont actives sur le Serveur d'applications, le Serveur de présentation et les Postes d'administration et d'exploitation.

  Ces suites sont spécifiées dans le guide ANSSI « Recommandations de sécurité relatives à TLS ».

  Pour plus de détails, voir le « Manuel de mise en conformité CSPN » (réf. A0U609).

- **Protection des communications du serveur de base de données SQL**

  Les communications avec le serveur de base de données SQL sont chiffrées grâce au protocole TLS 1.2, gérées par l'OS (Windows), et l'authentification mutuelle est réalisée par l'utilisation de certificats.

  Ces éléments permettent de garantir la confidentialité et l'intégrité de la liaison.

  Seules les suites cryptographiques validées par l'ANSSI sont actives sur les postes clients et serveurs.

  Ces suites sont spécifiées dans le guide ANSSI « Recommandations de sécurité relatives à TLS ».

  Pour plus de détails, voir le « Chiffrement et authentification des communications – SMI Server » (réf. A0I542).

P11 : Protection de l'accès à la base de données

La base de données est sur un serveur dédié situé en zone névralgique. L'accès à la base de données est assuré via une authentification Windows. Aucune donnée sensible n'est nécessaire pour une connexion à la base de données.

P12 : Définition des droits

Les actions des opérateurs sur le système SMI Server sont régies par des droits. Il est donc nécessaire de définir les actions autorisées pour chacun d'entre eux selon des prérogatives disponibles dans le logiciel.

Proposition de rôles types à prévoir dans le GAC :

Fonctions du GAC	Rôles des opérateurs				
	Administrateur	Mainteneur	Exploitant Niveau 1	Exploitant Niveau 2	Exploitant Niveau 3
Administration du système	X				
Création des opérateurs	X				
Création des usagers	X		X	X	X
Visualisation du fil de l'eau	X	X	X	X	X
Saisie des données névralgiques	X				
Création et gestion des UTL	X	X			
Gestion des alarmes	X		X	X	X
Commandes sur les accès	X	X		X	X
Commandes sur les zones d'intrusion	X	X			X
Recherche d'historique	X	X	X		

Pour plus de détails sur le rôle des opérateurs et leur paramétrage, voir le « Manuel de mise en conformité CSPN » (réf. A0U609).

P13 : Protection des événements

- **Protection contre l'altération des événements de contrôle d'accès :**

  Limitation des accès à la base de données.

  Limitation des actions possibles dans SMI Server selon profil opérateur (voir tableau ci-dessus).

  Le moteur de la base de données autorise la modification et la suppression des événements uniquement par le Serveur d'applications situé en zone névralgique.

- **Protection contre l'altération des évènements du GAC :**

  Limitation des accès à la base de données.

  Limitation des actions possibles dans SMI Server selon profil opérateur (voir tableau ci-dessus).

  Le moteur de la base de données autorise la modification et la suppression des événements uniquement par le Serveur d'applications situé en zone névralgique.

P14 : Génération des événements du GAC

Sur le GAC, un ensemble d'événements liés à la sécurité du logiciel permettent de contrôler le bon fonctionnement de la solution.

Exemples d'événements permettant la traçabilité dans le système :

- Ouverture permanente d'accès
- Ouverture temporaire d'accès
- Badge perdu/volé/détruit
- Connexion opérateur
- Déconnexion opérateur
- Avertissement échec connexion operateur
- Verrouillage échec connexion operateur

P15 : Protection de l'accès au mode debug des microcontrôleurs

L'accès au JTAG ou SWD est bloqué afin d'empêcher l'accès au mode débug ou la modification et la rétro ingénierie des logiciels embarqués par le SM400, le SM400-L, le SM100+ ou les lecteurs ProStyl.

Pour plus de détails, voir « Annexe 3 : Argumentaire sur les menaces ».

8 INFORMATIONS SUR LES MENACES ET LA SURETE

Le tableau ci-dessous est extrait du guide ANSSI « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » (Chapitre 3.4) :

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**

Ce tableau regroupe les principales menaces avec les informations suivantes :

- **Pour le niveau II** : la solution SMI Server est une solution professionnelle avec une communication sous contrôle. De ce fait, les connaissances du produit ne sont pas publiques et s'adressent uniquement à des professionnels formés et habilités.
- **Pour le niveau III** : la solution SMI Server permet de générer des alarmes en cas de ruptures momentanées des liaisons (ex : alarmes défauts de communications) ou de substitution d'un équipement (ex : remplacement d'un contrôleur de portes SM100+ ou d'un lecteur de la gamme ProStyl par une maquette spécifique). Ces alarmes peuvent générer des alertes.
- **Pour le niveau IV** : les utilisateurs devront s'assurer que les mécanismes cryptographiques mis en œuvre sur les réseaux LAN et les liaisons des équipements sont activés et conformes aux recommandations faites dans la notice d'exploitation.

9 ANNEXES

9.1 Annexe 1 : Architecture SMI Server avec les échanges

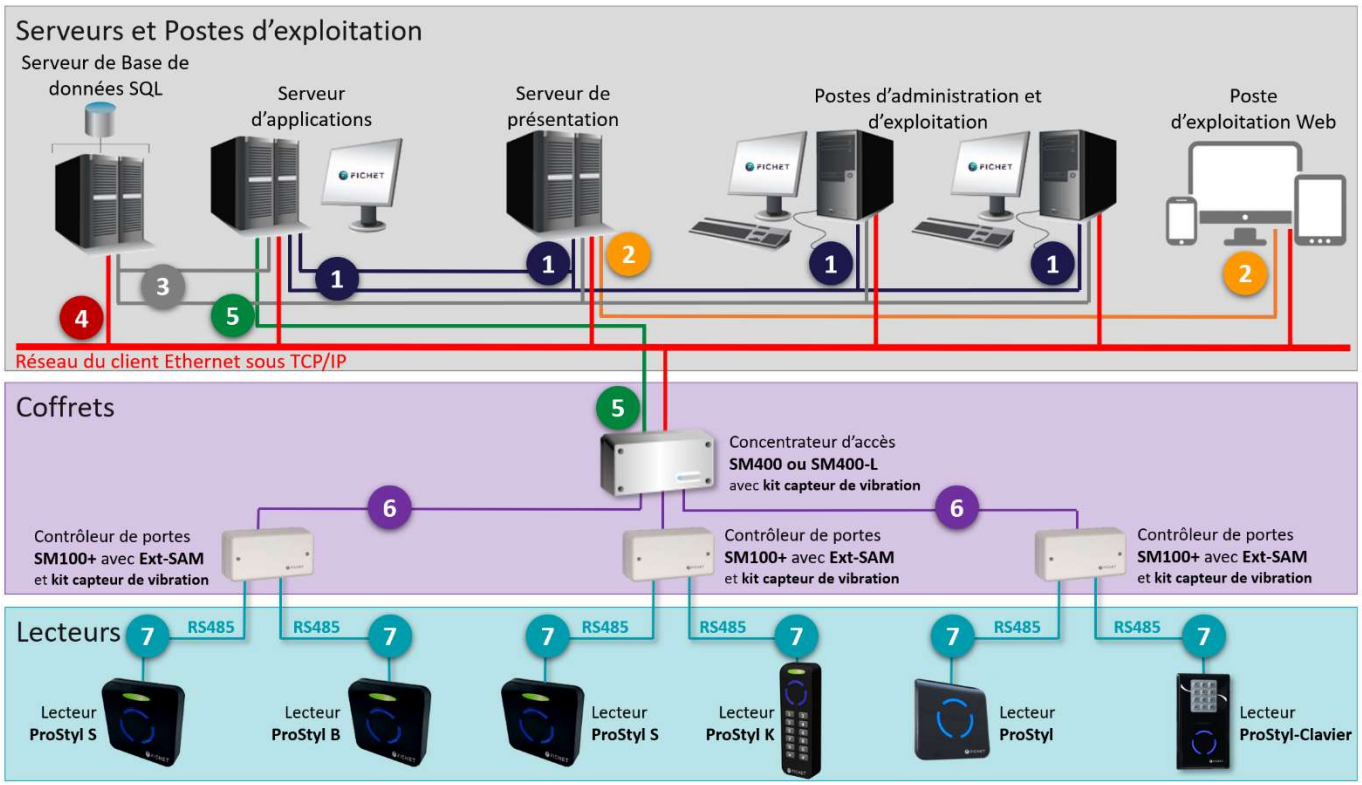

Figure 5 : Sécurisation des échanges et communications

1. Les communications entre le Serveur d'applications et le Serveur de présentation ainsi qu'entre le Serveur d'applications et les Postes d'administration et d'exploitation sont toujours chiffrées en TLS avec une authentification réalisée par des certificats mis en place par le client.

2. Le Serveur de présentation et les Postes d'exploitation Web utilisent le protocole sécurisé https.

3. La liaison avec la base de données est chiffrée en TLS avec une authentification réalisée par des certificats mis en place par le client.

4. Réseau Ethernet administré par le client et sous sa responsabilité.

5. Les communications sur le réseau Ethernet entre le Serveur d'applications et les concentrateurs SM400 sont chiffrées et authentifiées (chiffrement AES et authentification réseau 802.1x).

6. Les communications des SM100+ sur les bus RS485 sont chiffrées (chiffrement AES et authentification).

7. La communication entre le contrôleur de portes SM100+ et les lecteurs ProStyl (RS485) utilise le **mode transparent**. La sécurisation des échanges se fait entre le badge et le contrôleur. La sécurité des lectures est ramenée au niveau du SM100+.

   Remarque : La communication (RS485) entre le contrôleur SM100+ et les lecteurs claviers de la gamme utilise :
   - pour la partie ProStyl, le **mode transparent**. La sécurisation des échanges se fait entre le badge et le contrôleur. La sécurité des lectures est ramenée au niveau du SM100+.
   - pour la partie Clavier, un chiffrement AES avec authentification.

9.2 Annexe 2 : Niveaux de sûreté et niveaux de résistance aux attaques

Niveaux de sûreté	Niveaux de résistance aux attaques logiques	Méthode d'authentification	Technologies	Nos réponses avec SM100+
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.	OUI en AES
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.	OUI en AES
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.	OUI en AES et avec codes PIN

Source ANSSI : « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » (Annexe D – Tableau D.1)

SMI Server répond aux différents niveaux de sûreté. La Cible de Sécurité adresse uniquement les niveaux de sûreté **III** et **IV** conformément aux recommandations de l'ANSSI.

9.3 Annexe 3 : Argumentaire sur les menaces

	Intrusion externe	Intrusion liaisons équipements	Attaque SM400(-L)	Attaque SM100+	Attaque ProStyl
Hypothèses sur les administrateurs	X				
Hypothèses sur l'environnement physique	X	X	X	X	X
Hypothèses sur les exploitants	X				
Hypothèses sur les usagers	X				
Hypothèse sur la sécurisation des clés SM100+	X			X	
P1 - Protection des codes PIN et des identifiants des badges	X				
P2 - Protection communication Server – SM400(-L)	X	X	X	X	
P3 - Protection communication SM400(-L) – SM100+	X	X	X	X	
P4 - Sécurisation SM100+	X	X		X	
P5 - Sécurisation SM400	X	X	X		
P6 - Sécurisation Lecteur	X	X			X
P7 - Protection des clés	X				
P8 - Authentification des opérateurs	X				
P9 - Protection du mot de passe des opérateurs	X				
P10 - Protection des communications réseaux	X				
P11 - Protection de l'accès à la base de données	X				
P12 - Gestion des droits opérateurs	X				
P13 - Protection des évènements contrôle accès	X				
P14 - Protection des évènements GAC	X				
P15 : Protection de l'accès au mode debug des microcontrôleurs	X		X	X	X

9.4 Annexe 4 : Certification du SAM

9.4.1 SAM AV2

Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0410-2007-MA-05
NXP Smart Card Controller
P5CD080V0B, P5CN080V0B, P5CC080V0B, P5CC073V0B with specific IC Dedicated Software
from
NXP Semiconductors Germany GmbH

Common Criteria Recognition Arrangement
for components up to EAL4

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements*, version 1.0, February 2004 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0410-2007.

The change to the certified product is at the level of documentation, new delivery form, additional customer option (reset behaviour) and additional testcenter, a change that has no effect on assurance. The TOE description of BSI-DSZ-CC-410-2007 remains unchanged.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0410-2007 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0410-2007.

Bonn, 07 July 2009

Common Criteria

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

9.4.2 SAM AV3

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1059-V2-2019 (*)

Smartcard Controller

NXP Secure Smart Card Controller P6022y VB* including IC Dedicated Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ASE_TSS.2, ALC_FLR.1

SOGIS Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement recognition for components up to EAL 2 and ALC_FLR only

Bonn, 24 June 2019
For the Federal Office for Information Security

DAkkS

Bernd Kowalski L.S.
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

9.5 Annexe 5 : Certification des badges Mifare® DESFire EV2/EV3

9.5.1 Mifare® DESFire EV2

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2016/32

MIFARE DESFire EV2

Paris, le 26 mai 2016

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Guillaume POUPARD
[ORIGINAL SIGNE]

9.5.2 Mifare® DESFire EV3

Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number: **CC-20-0011955**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: **NXP Semiconductors Germany GmbH**
Troplowitzstrasse 20, 22529 Hamburg, Germany

Product and assurance level: **MF3D(H)x3**

Assurance Package:
- EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5

Protection Profile Conformance (if appropriate):
- Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

Project number: **0011955**

Evaluation facility: **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity: Date of 1st issue : **16-04-2020**
Certificate expiry : **16-04-2025**

Accredited by the Dutch Council for Accreditation

R.L. Kruit, LFM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.