Cible de sécurité CSPN

SMI - Identification, authentification pour le contrôle des accès physiques

AOY002

GUNNEBO®
For a safer world

Cible de sécurité CSPN : SMI - Identification, authentification pour le contrôle des accès physiques

Date	Version	Objet des modifications	Auteur
X/2014	00	Création Bases pour une démarche CSPN dans le domaine technique des contrôles d'accès physiques	F. DENEU
04/2015 10/2015	1 1-4	Cible de sécurité CSPN avec prise en compte des besoins des Ministères et secteurs AIT. Architecture d'accès avec SMI Server Démarche préparatoire avec ANSSI	F.DENEU
12/2015	2	Finalisation et publication	F.DENEU
03/2016	3	Prise en compte des remarques rapport pré-CSPN	F.DENEU
05/2016	4	Prise en compte des remarques ANSSI	F.DENEU
08/2016	4-1	Mises à jour des versions firmware	F.DENEU
09/2016	4-2	Ajout des références produits §2.1.8 à §2.1.11	F.DENEU

Liste des documents de référence

Source	Référence	Vers	Source/actualisation
ANSSI	ANSSI-CSPN-CER/P01.1		www.ssi.gouv.fr
ANSSI	GUIDES-ANSSI	V1.2	Guide de sécurité des technologies sans-contact pour le contrôle des accès physiques
ANSSI	Référentiels cryptographiques	RGS27	Annexe B1 cryptage de bout en bout
APSAD	Référentiel	D83	Contrôle d'accès-Documents techniques pour la conception et l'installation

Liste de diffusion

Nom	Prénom	Société	Contact
MUGUET	Romain	ANSSI	
NORTIER	Cédric	ANSSI	
BLAD	Christophe	OPPIDA	
ROSE	Philippe	OPPIDA	
DONG	Michel	OPPIDA	
KORCHIA	Gilbert	GUNNEBO	
AUVRAY	Dominique	GUNNEBO	
DITZ	Patrick	GUNNEBO	
KAPP	Frédéric	GUNNEBO	
LOEHLE	Guy	GUNNEBO	

GUNNEBO® For a safer world

Electronic Security
Gunnebo Electronic Security
23 route de Schwobsheim
67600 Baldenheim
France
www.gunnebo.com

Visiting address:
7 rue Paul Dautier
78140 Vélizy Villacoublay
France
Phone +33 810 000 800

Sommaire

1 INTRODUCTION

1.1 Identification de la cible de sécurité

Ce document constitue la cible de sécurité pour une évaluation CSPN dans la catégorie 6 : Identification, authentification pour le contrôle des accès physiques.

1.2 Identification du produit

1 Nom du produit : SMI-CSPN_01-01

Composé des équipements suivants :

- **SM400**
- **SM100+ et SM101+ (avec son antenne Smart S)**
- **Lecteurs ProStyl et ProStyl-Clavier AVL**

2 Constructeur : GUNNEBO Electronic Security

Site de Gunnebo : http://www.gunnebo.fr/

et http://www.gunnebo.fr/solutions-marches

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

1.3 Références & désignations

	Désignation	Description
Appli métier	SMI	Site Master Industrie
Equipement	SM400	Site Master modèle 400 (concentrateur)
Equipement	SM100+	Site Master modèle 100 (contrôleur de porte)
Equipement	ProStyl	Lecteur d'accès RFID
Equipement	ProStyl-Clavier	Lecteur d'accès RFID avec Clavier digital
Badges (techno)	DESFire	DES Fast innovative reliable enhanced (NXP)
Hard/Soft	Server	Machine host hébergeant des applications et des données
Software	VM	Virtual Machine
Software	AES 128	Advanced Encrypted Standard, clé 128 bits
Software	DH	Diffie Hellmann
Software	ECC	Elliptic Curve Cryptography
Protocole	SOP	Smart Open Protocol (propriétaire Gunnebo)
Hardware	AP	Auto Protection
Hard/soft	UTL	Unité de Traitement Locale
Code (donnée)	PIN ou CIP	Personal Identification Number/ Code Identification Personnel
Code (donnée)	ID	Identifiant
Système	CMS	Card Management System (Gestion des badges)
Système	SI	Système d'Information
Personne	RSSI	Responsable Sécurité Système d'Information

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 physiques.

Elle est composée :

- d'une partie appelée « **Server** » intégrant les applications, les bases de données et le serveur de terrain,
- d'une partie appelée « **SMI** » intégrant les équipements de terrain : concentrateurs d'accès, contrôleurs d'accès 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 d'accès (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.

Note : Ce document rentre dans le cadre de contrôle d'accès utilisant des technologies sans contact telles que définies par l'ANSSI dans le « Guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques ».

2.1.2 Schéma type

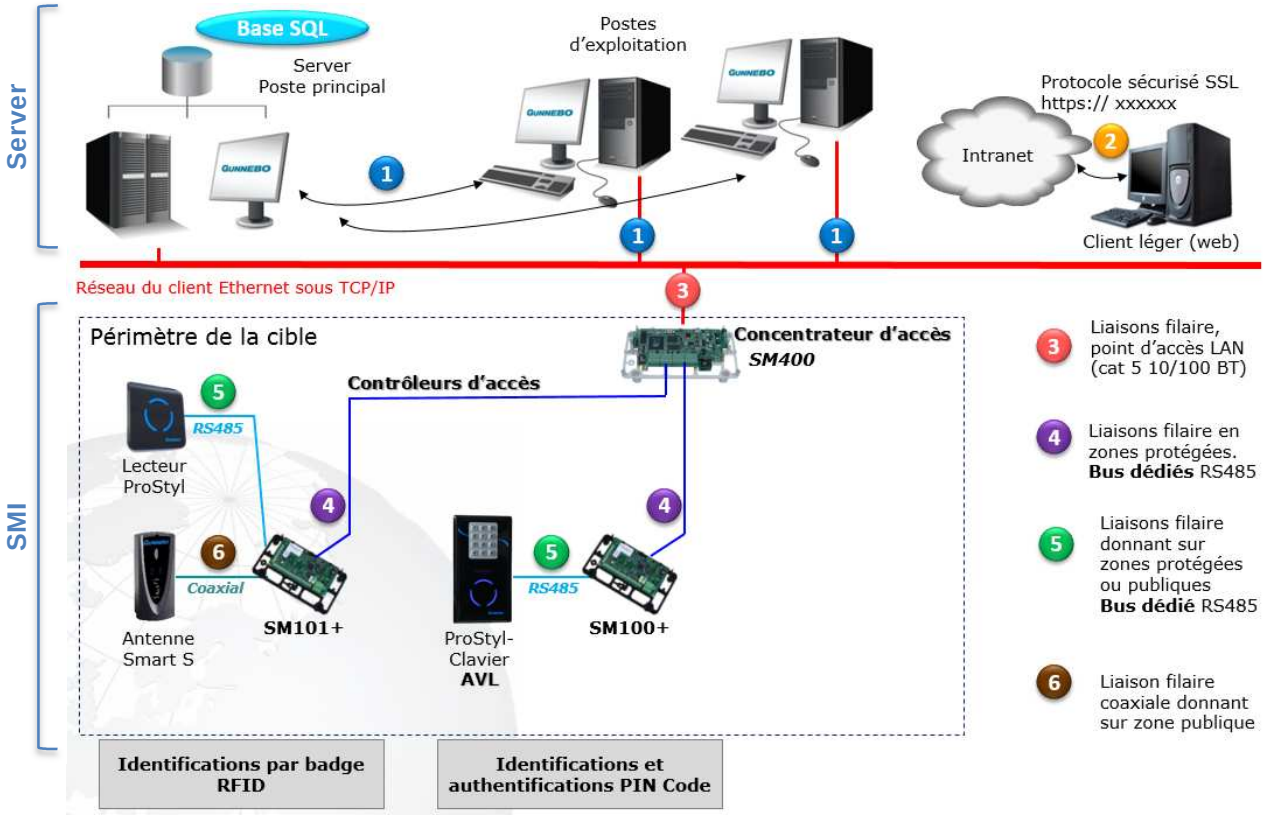


Figure 1 : SMI Server

2.1.3 Description fonctionnelle et utilisation

La solution SMI Server de Gunnebo 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 Gunnebo Electronic Security.

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 sécurisées 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 de terrain avec « application métier » et base de données centrale
- Des postes d'exploitation
- Des concentrateurs d'accès (SM400) avec leur système d'alimentation en énergie (alimentation secourue)
- Des contrôleurs de portes (SM100+) avec leur système d'alimentation en énergie (alimentation secourue)
- Des lecteurs de badges (gamme ProStyl)
- Des badges d'accès (badges basés sur la technologie Mifare® DESFire de NXP)

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

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

2.1.4 Raccordements & réseaux

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

Ce réseau est généralement un réseau Ethernet sous TCP/IP (IP V4 actuellement) 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 de terrain et les postes d'exploitation. Plusieurs postes d'exploitation peuvent être installés sur ce réseau.

Note : Le ***réseau du client*** est hors périmètre de l'évaluation CSPN. Ce réseau est repéré 1 sur la Figure 1Figure 1.

Le ***réseau LAN du client*** assure les échanges entre le Server et les concentrateurs d'accès (SM400). Les communications entre le Server et le SM400 transitant par ce réseau sont chiffrées (blocs de paquets IP chiffrés). Le segment de réseau qui aboutit au SM400 correspond à une liaison filaire LAN cat 5 en 10/100 BT qui est dédiée au contrôle d'accès.

Le point d'accès réseau, repéré 3 sur la Figure 1, fait partie du périmètre d'évaluation.

2.1.5 Réseaux dédiés

Les réseaux dédiés correspondent à des liaisons filaires utilisées exclusivement pour les installations de contrôles d'accès physiques.

Note : Les réseaux dédiés ne sont pas partagés avec d'autres équipements que ceux présentés dans la cible d'évaluation.

On distinguera 2 cas de réseaux dédiés :

a) Les interfaces bus RS 485 entre équipements ***SM400*** 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 et les contrôleurs d'accès SM100+ via des bus dédiés RS485 supportant un protocole propriétaire SOP développé par Gunnebo Electronic Security.

Note : Les bus de terrain sont repérés 4 sur la Figure 1 et font partie du périmètre d'évaluation.

b) Les interfaces bus RS 485 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 un protocole propriétaire SOP développé par Gunnebo Electronic Security.

Note : Les bus de terrain sont repérés 5 sur la Figure 1 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.

Note : 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'accès (SMI Server)

Rôle : Serveur applicatif pour une gestion centralisée de toutes les fonctions d'accès. SMI Server est développé par Gunnebo Electronic Security.

Le serveur peut être constitué d'un poste informatique sous Microsoft Windows et est doté d'une base de données centrale 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.

Le Server dispose de deux interfaces :

- **Configuration** : Celle-ci permet de définir l'architecture avec les différents équipements déployés sur site(s) (SM400/SM100+/Lecteurs) au travers d'échanges temps réel et centralisés.
- **Exploitation** : Celle-ci permet la gestion des accès, des droits des usagers, des alarmes, des événements.
  Cette interface permet, sous condition de droit d'administration, de charger, modifier des informations dans la base de données.

2.1.7 Postes d'exploitation

Rôle : Station de programmation et d'exploitation

2.1.8 Concentrateur d'accès SM400

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 dispose d'une capacité de gestion autonome en cas de rupture de sa connexion LAN avec le serveur SMI (repérée 3 sur la Figure 1).

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

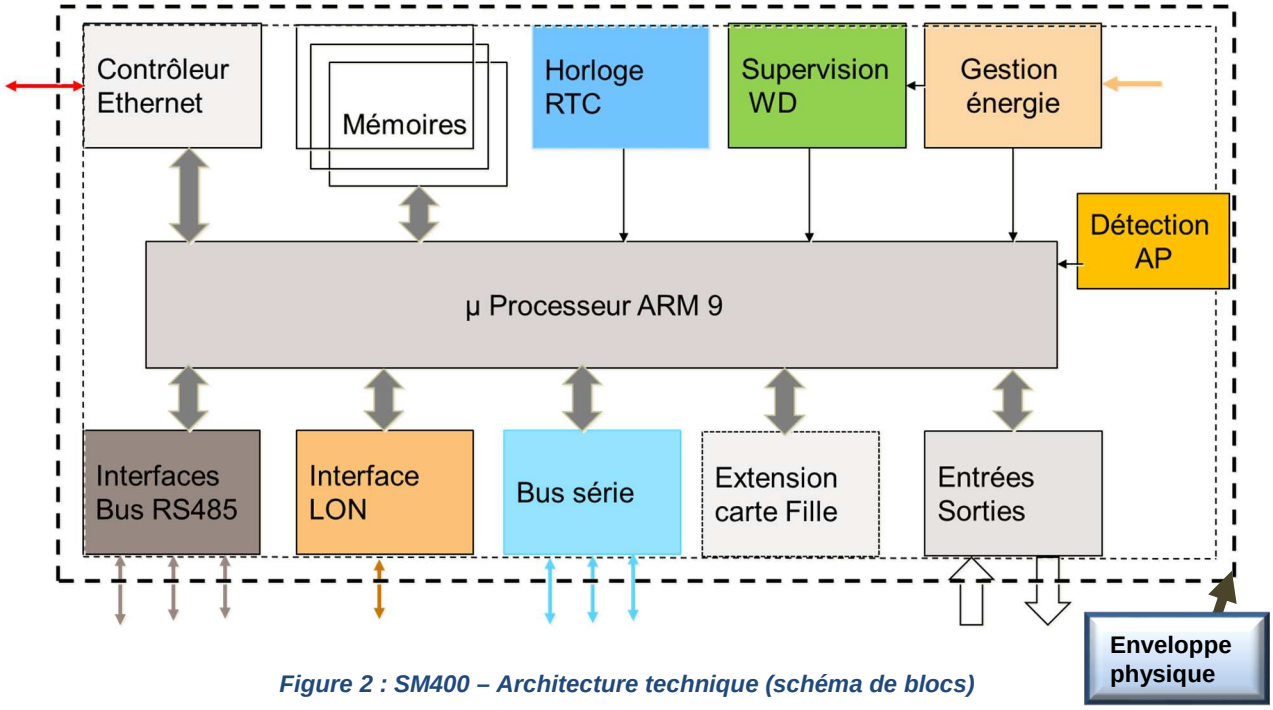


Figure 2 : SM400 – Architecture technique (schéma de blocs)

Caractéristiques techniques du SM400 :

Composant	Description
Désignation	**SM400**
Référence produit	**A19914H**
Version logiciel	V2.3.5 (mise à jour par téléchargement)
Emplacement	Zone sécurisée
Processeur	ARM 9 (AT91SAM9260)
OS embarqué	eCOS (Linux)
Base locale	Base propriétaire par système de fichiers
Données	Données névralgiques : Flash Données en Flash (binaire et système de fichier) et EEPROM
AP	Ouverture coffret

Liaisons & sécurisations :

- en lien avec l'application Server (repère 3)
- en lien avec des contrôleurs de porte SM100+ (repère 4) ; protocole SOP (propriétaire)
- 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 d'accès SM100+

Rôle : Le SM100+ assure les fonctions d'accès.
Le contrôleur est livré avec une application

Le SM100+ dispose d'une capacité de gestion autonome en cas de rupture de sa connexion avec le concentrateur SM400 (repérée 3 sur la Figure 1).

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

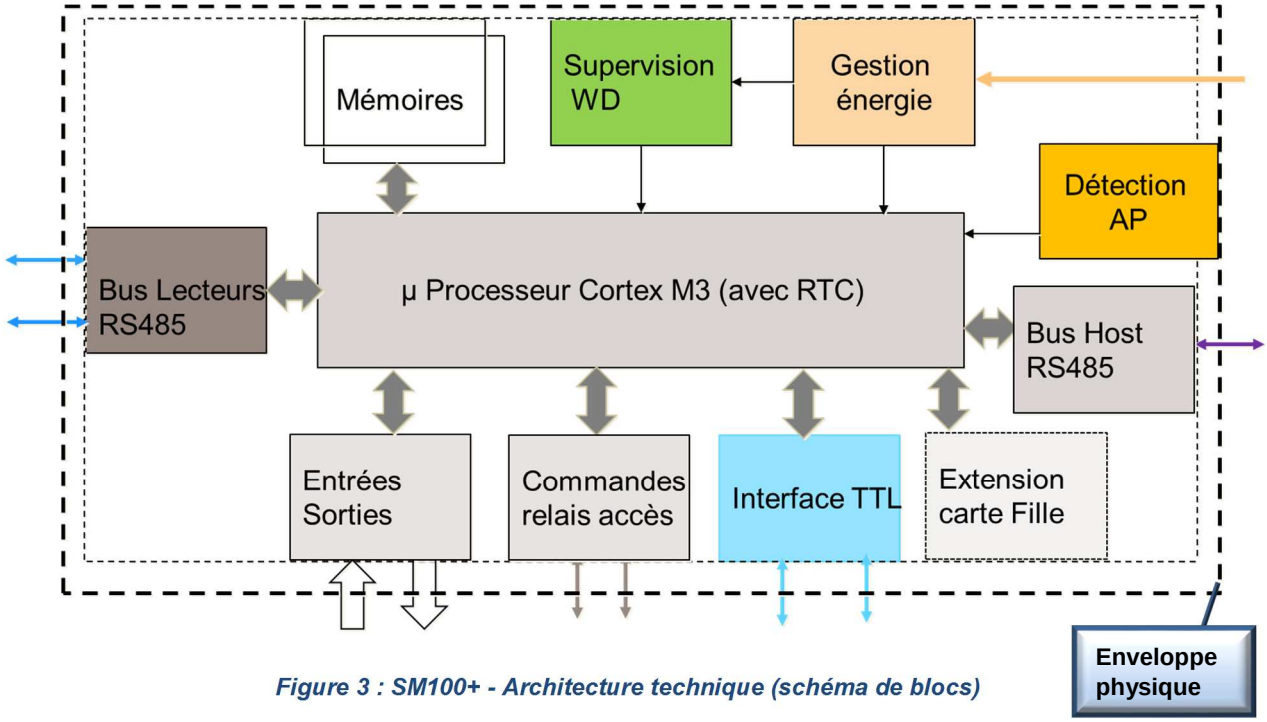


Figure 3 : SM100+ - Architecture technique (schéma de blocs)

Caractéristiques techniques du SM100+ :

Composant	Description
Désignation	**SM100+**
Référence produit	**A19A28J**
Référence logiciel	V3.0.19 (mise à jour par téléchargement)
Emplacement	Zone protégée ou sécurisée
Processeur	Cœur ARM Cortex
OS embarqué	OS TR MT (Temps Réel & Multi Tâches)
Base locale	Fichiers
AP	Ouverture coffret et arrachement

Liaisons & sécurisations :

- en lien avec le SM400 (repère 4)
- en lien avec 1 ou 2 têtes de lecture (repère 5 et 6) ; protocole SOP (propriétaire) ou lien liaison radio en bande de base pour les antennes.
- Dispose d'une clé usine (128 b) et d'un identifiant Hard unique (MIC)
- Embarque des algorithmes de chiffrement en cryptographie symétrique (AES et ECC)
- Protocole d'échange de clés (DH–ECC)

2.1.10 Lecteur de badges d'accès ProStyl

Rôle : Identification RFID en mode transparent

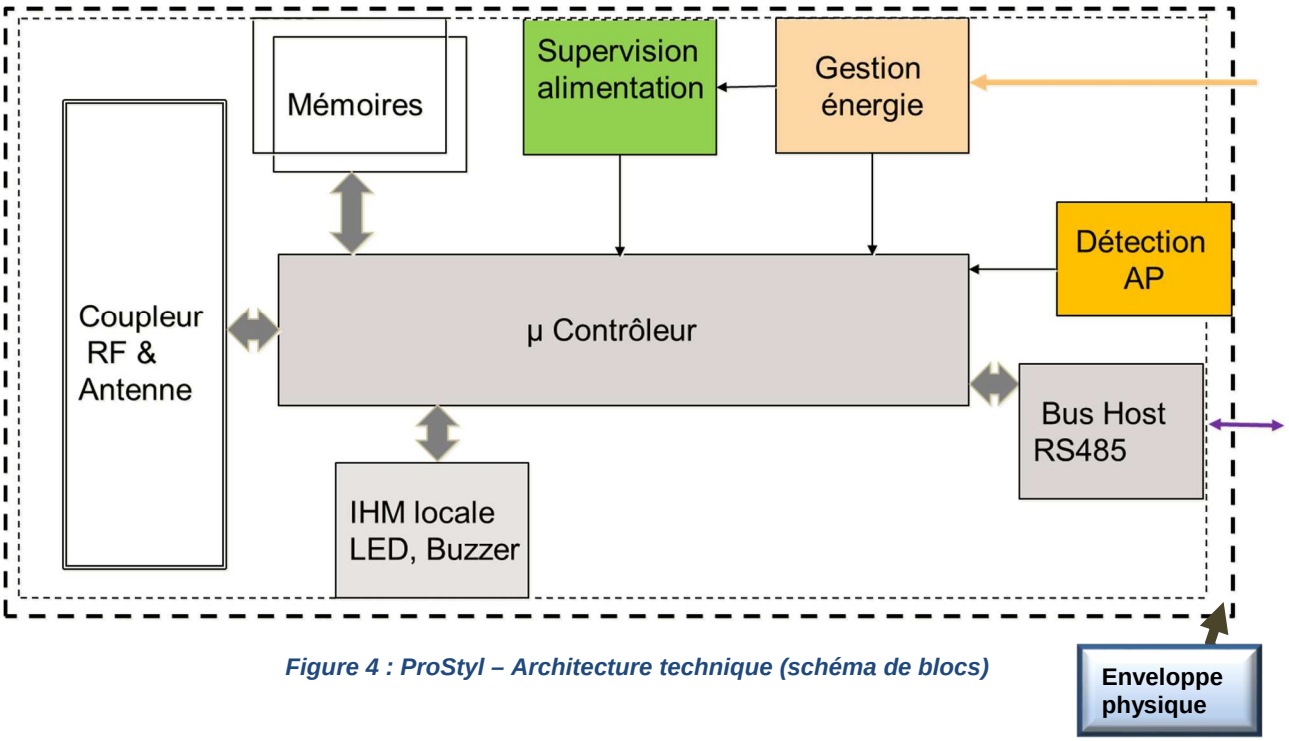


Figure 4 : ProStyl – Architecture technique (schéma de blocs)

Caractéristiques techniques du lecteur ProStyl :

Composant	Description
Désignation	**ProStyl**
Code produit	**A10512L**
Référence logiciel	V1.0.9
Emplacement	Zone publique ou zone protégée
Processeur	Cœur ARM µContrôleur
OS embarqué	NON
Mémoire locale	Flash dans µC
AP	Détection arrachement

2.1.11 Lecteur de badges d'accès ProStyl-Clavier

Rôle : Identification RFID mode transparent et authentification PIN code

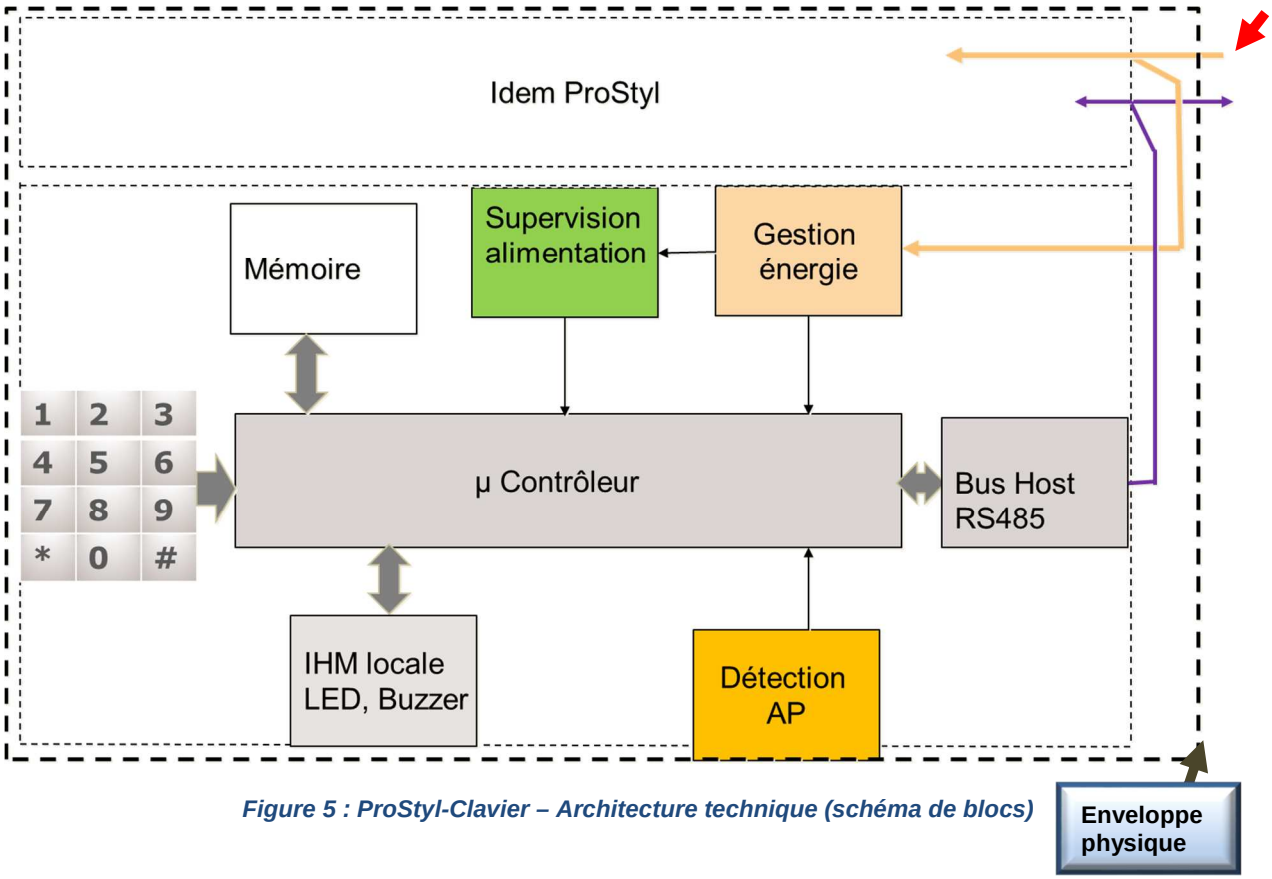


Figure 5 : ProStyl-Clavier – Architecture technique (schéma de blocs)

Caractéristiques techniques du ProStyl-Clavier :

Composant	Description
Désignation	**ProStyl-Clavier**
Code produit	**A10535A**
Référence logiciel	Appli WK V1.0.3
Emplacement	Zone publique ou zone protégée
Processeur	Cœur ARM µContrôleur
OS embarqué	NON
Mémoire locale	Flash dans µC
AP	Détection arrachement

Liaisons & sécurisations :

- en lien avec le SM100+ (repère 5)
- Clé d'authentification négociée avec SM100+ à l'installation
- Dispose d'une clé usine (128 b) et d'un identifiant Hard unique (MIC)
- 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 Gunnebo 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 EV1 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 128**
- Mode opératoire du lecteur ProStyl : **Transparent**
- Présence de clés de sécurité dans le lecteur ProStyl : **Aucune clé dans le lecteur ProStyl**
- Traitement des fonctions sécurisées des badges dans le contrôleur SM100+ : **toutes les fonctions sécurisées en lectures (*)**
- Données névralgiques et clés : **Téléchargées dans le SM100+ depuis le Server** :

Le mode transparent correspond au schéma de l'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 SM100+.

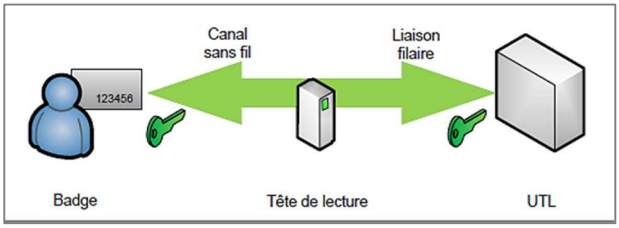


Figure 6

(*) Ces fonctions sont celles du Tableau 2 du document ANSSI « Guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques ». Ce tableau est renseigné en ANNEXE 2 de ce document.

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

Pour une installation dite « mono-site » :

- Le réseau fédérateur est le réseau LAN du client. Ce réseau est sous contrôle d'un DSI (plan d'adressage, configuration des switch et des routeurs).
- Le concentrateur d'accès SM400 n'intervient pas dans les fonctions de lecture sécurisée ci-dessus.
- Le contrôleur d'accès SM100+ est en charge d'effectuer les lectures sécurisées des badges d'accès.
- Le SM100+ est mis à la clé par téléchargement depuis le Server.

Pour une installation dite « multi-sites » :

- Le concentrateur d'accès SM400 peut être déployé sur un site distant. Ce dernier n'intervient pas dans les fonctions de lecture sécurisée ci-dessus.
- Le contrôleur d'accès SM100+ est raccordé aux SM400.
- Le contrôleur d'accès SM100+ est en charge d'effectuer les lectures sécurisées des badges d'accès et l'acquisition des PIN codes.
- Le SM100+ est mis à la clé par téléchargement depuis le Server.

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 Gunnebo. Dans ce cas, la sécurité du support est assurée 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 Server et conditionne la fonction de contrôle de l’accès au niveau du contrôleur SM100+ (Badge + code PIN).

2.3.3 Documents en référence

- Guide de configuration SMI Server (réf. A0U562)
- Guide d’utilisation SMI Server (réf. A0U563)
- Manuel de mise en conformité CSPN (réf. A0U565)

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 (comme 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 dont l'accès est strictement limité aux personnels habilités.

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

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

- **Installation du concentrateur SM400 :**

  Le SM400 ainsi que le système d'alimentation secourue sont installés dans un local technique sécurisé dont l'accès est limité.

- **Installation des lecteurs ProStyl :**

  Les lecteurs ProStyl sont installés de façon « représentative ».

  Pour un accès à partir d'une zone publique, le lecteur ProStyl anti-vandale (même niveau de sécurité que le lecteur ProStyl) est vivement recommandé (protection IK10).

  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 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 exploitants du produit

La solution d'accès SMI Server nécessite une exploitation (poste de surveillance, gestions des alarmes en temps réel ; ajout, suppression d'usagers, gestions 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 qui limite les droits d'accès au système.

- **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 7, Windows 8.1, Windows Server 2008, Windows Server 2012).

  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.

2.4.3 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 II ou III du tableau en ANNEXE 2.

Pour les sites sécurisés, la technologie Mifare® DESFire EV1 est vivement recommandée.

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

Les règles de sécurité sont censées 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 tout autre personne (tiers et collègues inclus).
- Ils sont supposés ne pas confier leur badge, ni communiquer leur code PIN personnel.

2.4.4 Hypothèses sur l'environnement technique du produit

SMI Server intègre différents logiciels (Configuration et Exploitation).

- L'application Server fonctionne dans un environnement MS Windows qui est régulièrement protégé des virus et ne permet pas l'exécution de code malveillant.
- Les mises à jour de sécurité et les outils Windows sont installés.
- Le niveau de protection du canal d'échange entre le Server et le concentrateur SM400 est décrit dans le document « Fournitures cryptographiques » (réf. AOY003).
- 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 réseaux :

Le réseau du client et les **réseaux dédiés** sont physiquement et logiquement séparés.

Aucune passerelle, informatique ou de transmission de données, ne peut être mise en œuvre entre ces deux réseaux.

Les échanges de données entre les deux réseaux passent systématiquement par le concentrateur SM400. Dans le cas de téléchargements depuis le Server vers des SM100+, les données sont routées via SOP (protocole d'échanges propriétaire de Gunnebo décrit dans le document « Fournitures cryptographiques » (réf. AOY003)).

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 EV1).

Cet ID est protégé en lecture par un chiffrement en AES 128 bits avec clé AES 128b (niveau II) ou clé diversifiée (niveau III).

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 EV1 (APDU et cryptographie DESFire EV1).

Sécurisation du réseau LAN et des réseaux dédiés :

Le réseau LAN du client est placé en zone protégée et technique.

Sécurisation des postes :

Les postes d'exploitation sont placés en zone sécurisée.

La prise de poste se fait via une session Windows avec politique des mots de passe (mots de passe sécurisés, changements périodiques des mots de passe, …).

2.5 Description des usagers (utilisateurs types)

2.5.1 Exploitants

Voir 2.4.2 « Hypothèses sur les exploitants 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).

Aucun exploitant n'est amené à se connecter directement et indirectement sur les contrôleurs ; c'est une prérogative des agents techniques.

Toute connexion au contrôleur 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 protégées ou aux zones sécurisées, ils disposent de badges sans contact (RFID) DESFire EV1 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 II et III** du tableau 2 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 concentrateur SM400 avec son segment final
- Les contrôleurs SM100+ et SM101+ (avec son antenne Smart S)
- Les lecteurs ProStyl et ProStyl-Clavier

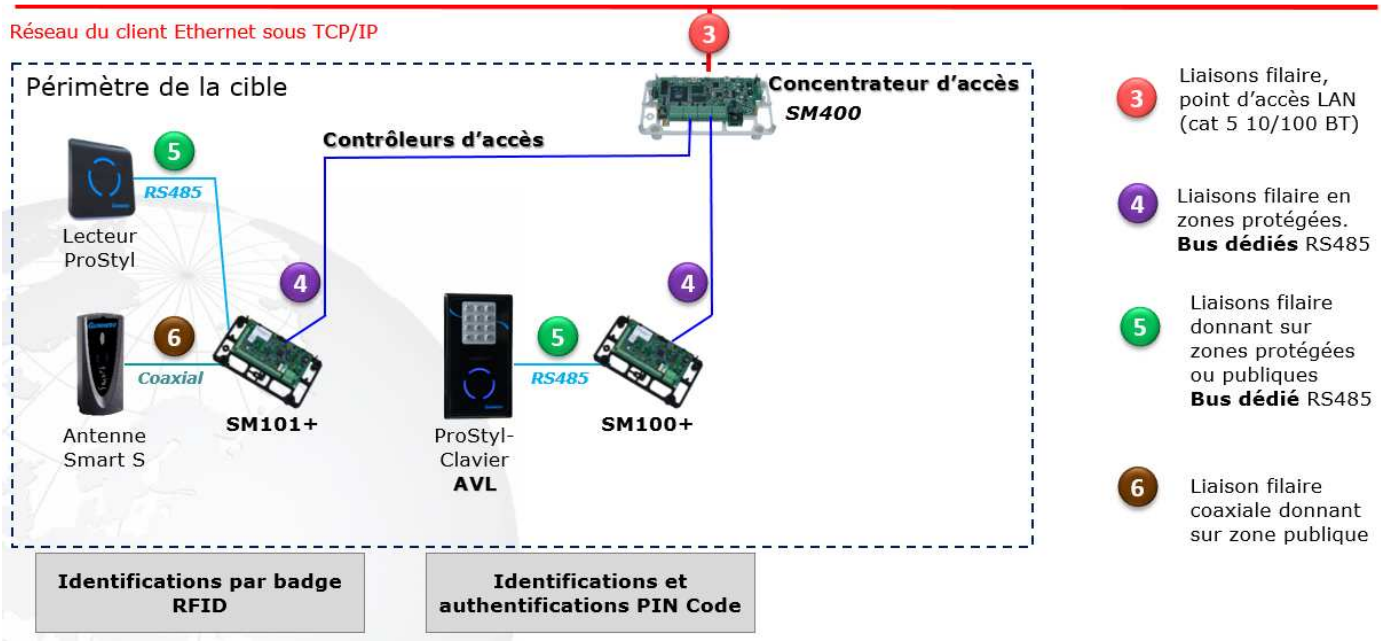


Figure 7 : Périmètre d'évaluation

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)
- Sortie par lecture de badge (lecteur en sortie)
- 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 et sont numérotés dans le schéma la cible de sécurité (voir page précédente).

S'y ajoutent :

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

3.3 Poste informatique

- SMI Server (Configuration & Exploitation)
- Microsoft Windows 2008 Server, 2008 Server R2
- Microsoft Windows 7 (64 bits), Windows 8, …
- Microsoft Windows SQL 2012 R2 (base MS SQL Server)

3.4 Badges

Badges d'accès sécurisés basés sur la technologie NXP Mifare® DESFire EV1 :

- 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 II et III** du tableau des niveaux de sûreté présenté en ANNEXE 2.

Note : Les fonctions de lectures sécurisées avec clés diversifiées font appel à différents algorithmes de calculs de clés (exemples : AES128 CBC, AES128 CMAC, etc.). Pour répondre aux différents besoins liés aux calculs des clés, ces fonctions sont traitées au niveau du contrôleur d'accès SM100+.

4 DONNEES NEVRALGIQUES & SENSIBLES

4.1 Descriptions

Les données névralgiques confidentielles regroupent plusieurs types d'informations :

- Clés :
  - Clés AES 128 bits de lecture/écriture liées à la sécurité des badges d'accès décrits au chapitre 3.4
  - Clés mères
  - Clés fixes
- Identifiant d'accès :
  - ***AID*** DESFire pour les applications du badge d'accès
  - ***Access ID*** pour une application d'accès à partir de mobiles NFC doté d'un SE (SIM sécurisées) (hors périmètre de l'évaluation).

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.
- Les clés fixes sont utilisées par la solution SMI Server et servent à la sécurisation des liaisons filaires repérées 3, 4, 5 et 6 sur la Figure 1 (liaisons chiffrées).

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 et le contrôleur SM100+).

4.2 Données sensibles dans le contrôleur d'accès SM100+

Les données sensibles protégées par le SM100+ sont :

	Usages
Clés DESFire	Lectures
AID	Accès à une application du badge
Clé mère	Calcul de clé(s) diversifiée(s)
Diversifiant	Calcul de clé(s) diversifiée(s)
ID	Identifiant d'accès
PIN code	Authentification

Dans le SM100+, la confidentialité des clés et diversifiant repose sur un mécanisme de protections développé par Gunnebo Electronic Security.
Les données sensibles destinées aux lectures sécurisées sont protégées dans « un coffre firmware » qui contient une table chiffrée.

Note : Le mécanisme de protection de la table chiffrée du SM100+ est décrit dans le document « Fournitures Cryptographiques » (AOY003).

Note : 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. Il peut être issu du serveur au même titre qu'une clé.

4.3 Données sensibles dans le lecteur d’accès ProStyl

Aucune donnée sensible n’est présente dans le lecteur ProStyl (fonctionne en mode tunnel/transparent).

4.4 Données sensibles dans le lecteur d’accès ProStyl-Clavier

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

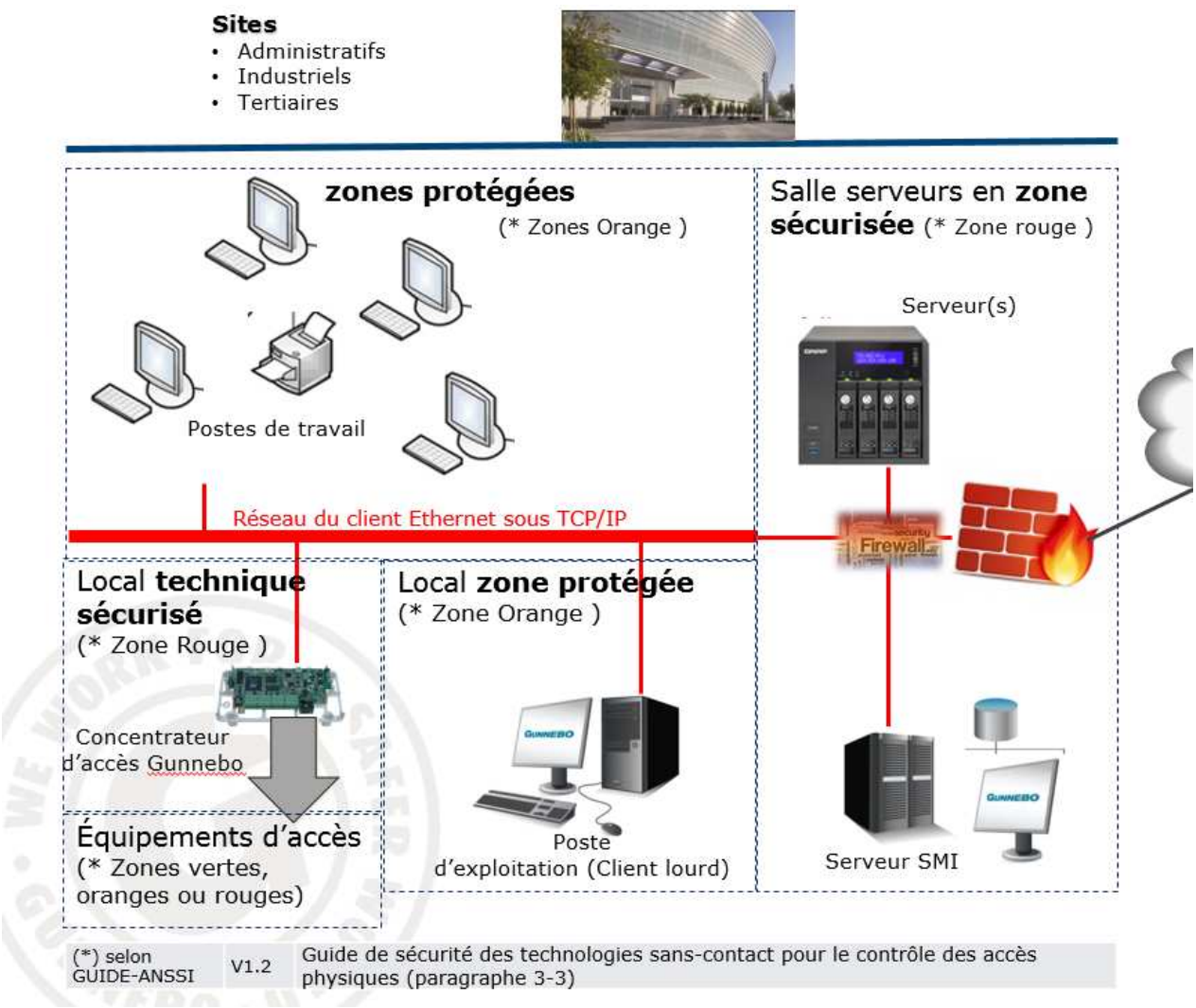
5 MESURES D'ENVIRONNEMENT

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



- 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 jours des logiciels, gestion des mots de passe)
- Opérateur(s) (surveillance des écrans sur les postes, prise en compte des alarmes, gestion/signalement des incidents)

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, sous forme papier (circulaire, notes, documents confidentiels).

- La remise des clés ou « cérémonie des clés » fait partie des mesures sécuritaires :
  - Actuellement, cette procédure est manuelle et matérialisée (documents ou SAM physique).
  - Dans un proche avenir, cette procédure sera dématérialisée (serveur de clés).
- 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)

Note : Les consignes de sécurité sont décrites dans le guide « **Manuel de mise en conformité CSPN** » (réf. A0U565).

6 DESCRIPTION DES MENACES

Différentes **attaques logiques** sont considérées :

- Attaquant sur le réseau TCP/IP établi entre le Server et le concentrateur SM400
- Attaquant sur le réseau dédié RS485 entre le Concentrateur SM400 et les contrôleurs d'accès SM100+
- Attaquant externe sur la liaison RS485 établie entre le lecteur ProStyl et le contrôleur SM100+
- Attaquant externe sur la liaison coaxiale entre l'antenne Smart S et le contrôleur SM100+

Pour ces attaques, les agents menaçants sont :

- de type interne : tout utilisateur autorisé se situant en zone protégée,
- de type externe : toute personne extérieure à la zone protégée.

Différentes **attaques physiques** sont considérées :

- Attaque sur un concentrateur SM400
- Attaque sur un contrôleur SM100+
- Attaque sur un lecteur ProStyl ou ProStyl-Clavier ou une antenne Smart S

6.1 Intrusion externe

Cette intrusion concerne le réseau LAN Ethernet TCP/IP (repères 3 ou 1 sur la Figure 1) 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 de sécurité des technologies sans contact pour le contrôle des accès physiques » (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 SM400

6.2 Intrusion sur les réseaux dédiés

Cette intrusion concerne la topologie des bus RS485 (repères 4 et 5 sur la Figure 1) 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 de sécurité des technologies sans contact pour le contrôle des accès physiques » (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 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 SM400	Emulation d'un ou plusieurs SM100+

6.3 Attaque sur SM400

Tentative de cryptanalyse et lecture du code exécutable.

Substitution d'un concentrateur.

6.4 Attaque sur SM100+

Tentative de cryptanalyse.

Substitution d'un contrôleur.

6.5 Attaque sur lecteur ou lecteur-clavier

Tentative de remplacement du lecteur.

Emulation/substitution.

7 DESCRIPTION DES FONCTIONS DE SECURITE

7.1 Hypothèses sur les administrateurs

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels.

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 point 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)

Les protections :

P1 : **Protection en transmission du code PIN**

Les codes PIN sont protégés en confidentialité par chiffrement AES 128 bits réalisé par lecteur ProStyl-Clavier.

Les codes sont remontés chiffrés (AES 128b).

P2 : **Protection des données échangées entre le Server et le Concentrateur SM400**

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 sont protégées en confidentialité.

Pour les tentatives de rejeu, la protection passe par la mise en œuvre des mécanismes cryptographiques décrits dans le document « Fournitures Cryptographiques » (AOY003).

Note : Les mécanismes d'authentification sont décrits dans le document « Fournitures Cryptographiques » (AOY003).

Note : Le protocole d'échange de clés est décrit dans le document « Fournitures Cryptographiques » (AOY003).

P3 : **Protection des données échangées entre le concentrateur SM400 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.

L'identification du SM100+ par le SM400 est gérée de façon native par le protocole SOP.

Les commandes et les transactions échangées entre le Server et le concentrateur SM400 sont protégées en confidentialité.

Les tentatives de rejeu sont limitées par la mise en œuvre d'un protocole SOP propriétaire et entièrement crypté et déterministe.

Note : Les mécanismes d'échange, d'authentification et les aspects déterministes sont décrits dans le document « Fournitures Cryptographiques » (AOY003).

Note : Le protocole d'échange de clés est décrit dans le document « Fournitures Cryptographiques » (AOY003).

P4 : **Sécurisation du contrôleur d'accès SM100+**

Le contrôleur SM100+ est placé en zone protégée.

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

Cette détection concerne 3 types de défaut :

- AP (arrachement),
- OC (Ouverture Coffret),
- Défaut communication du bus RS485 (repère 5 sur la Figure 1). Le défaut communication est analysé par le SM400.

P5 : **Sécurisation du concentrateur SM400**

Le concentrateur SM400 est placé en zone sécurisée.

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

Cette détection concerne 2 types de défaut :

- OC (Ouverture Coffret),
- Défaut communication du LAN (repère 3 sur la Figure 1). Le défaut communication est analysé par le serveur.

P6 : **Sécurisation du lecteur ProStyl-Clavier**

ProStyl-Clavier utilise une clé de session déterminée lors de l'échange initial de clés (« Initial Key exchange » décrit dans « Fournitures cryptographiques » (AOY003)) 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 ProStyl-Clavier : il y a appairage.

  Note : La mise en place d'une négociation de clé entre le contrôleur SM100+ et le ProStyl-Clavier est documentée dans « Fournitures cryptographiques » (AOY003) à travers les échanges SOPKE.

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

  Note : Dans ces deux cas, les procédures à appliquer sont décrites dans le guide « **Manuel de mise en conformité CSPN** » (réf. A0U565).

8 INFORMATIONS SUR LES MENACES ET LA SURETE

Le tableau ci-dessous est extrait du « Guide de sécurité des technologies sans contact pour le contrôle des accès physiques » (Chapitre 3.4) :

Niveau de sûreté	**Menaces potentielles**		
	QUI ?	***Quels moyens ?***	***Quelles connaissances ?***
II Franchissement par attaque mécanique et/ou logique simple	Pénétration préméditée de personnes faiblement équipées	Matériels et méthode obtenus dans le commerce ou sur Internet	Connaissances basiques du système acquises au travers de documents publicitaires ou technico-commerciaux émis par le fabricant ou par les distributeurs.
III Franchissement par attaque mécanique et/ou logique simple	Pénétration préméditée de personnes initiées et équipées	Matériels ou maquette électronique spécifique facilement réalisable	Connaissances recueillies à partir de l'examen d'un dispositif
IV Franchissement par attaque mécanique et/ou logique sophistiquée	Pénétration préméditée de personnes initiées fortement équipées et renseignées	Matériels comprenant des moyens de cryptanalyse et/ou maquette électronique spécifique conçus spécialement pour neutraliser la sûreté en place	Connaissances sur la conception, l'exploitation du système. Ceci implique d'avoir accès à des informations confidentielles du fabricant

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 (commercialisation sans publicité). De ce fait, les connaissances du produit sont non diffusées et s'adressent uniquement à des professionnels. Les outils d'aide à la mise en œuvre ne sont pas commercialisés par Gunnebo, ni mis en ligne via internet.
- **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) ; de substitution d'un équipement (ex : remplacement d'un contrôleur SM100+ ou d'un lecteur ProStyl par une maquette spécifique).
  Ces alarmes peuvent générer des alertes vers l'extérieur.
- **Pour le niveau IV** : les utilisateurs devront s'assurer que les mécanismes cryptographiques mis en œuvre sur les réseaux LAN et dédiés sont activés et conformes aux recommandations faites dans la notice d'exploitation (NEX).

9 ANNEXES

9.1 Annexe 1 : Architecture SMI Server avec les échanges

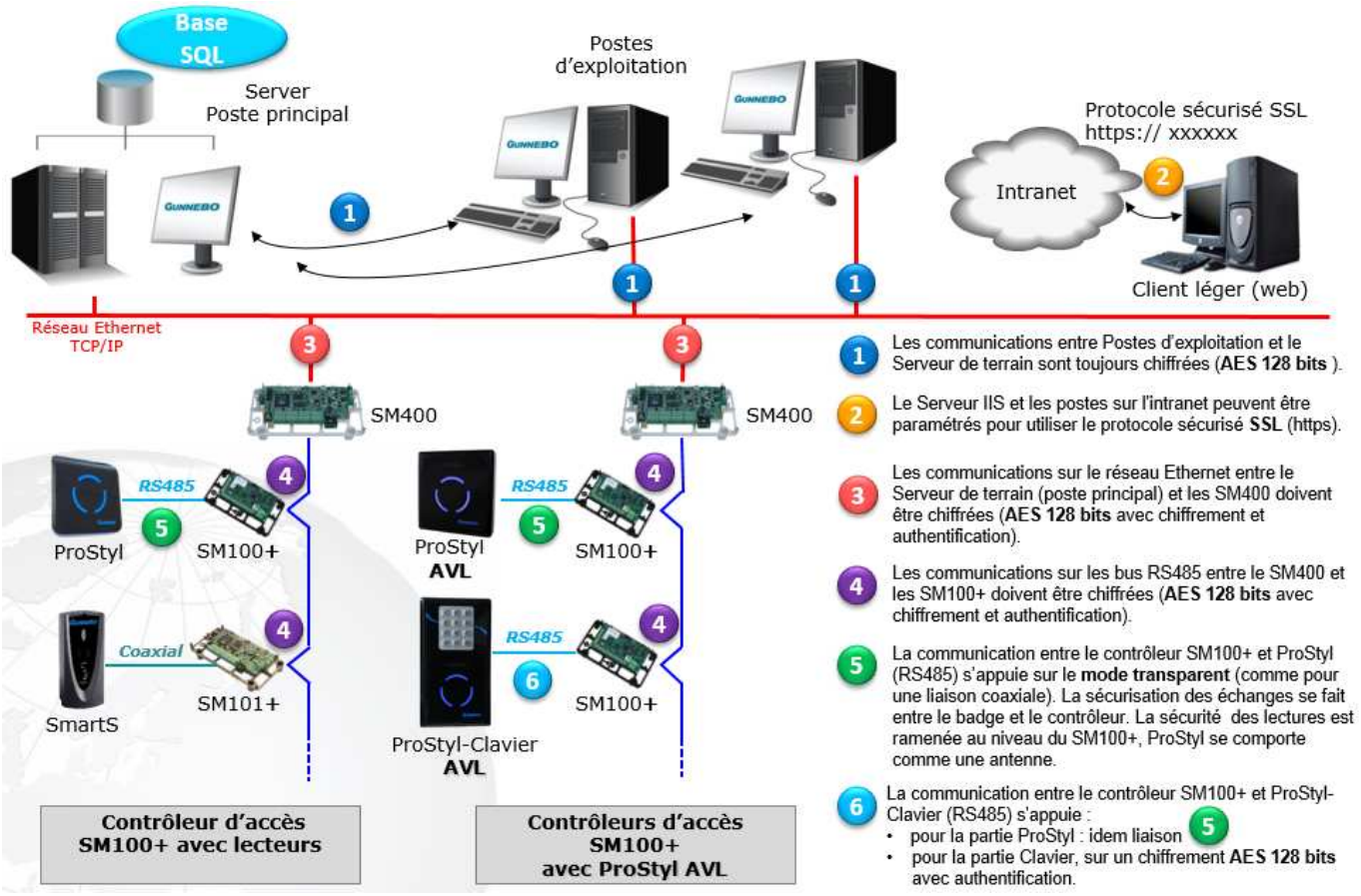


Figure 8 : Architecture SMI Server et échanges

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

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).

Nos réponses avec SM100+

OUI en AES

OUI en AES

OUI en AES et avec PIN codes

GUNNEBO
For a safer world®

Source ANSSI : « Guide sur la sécurité des technologies sans contact pour le contrôle des accès physiques »

9.3 Annexe 3 : Badges d'accès

Les badges d'accès basés sur la technologie NXP Mifare® DESFire EV1 sont hors périmètre de l'évaluation.

Pour comprendre la façon dont ces badges sont lus par les contrôleurs SM100+, la figure ci-dessous représente la structure Mifare® DESFire :

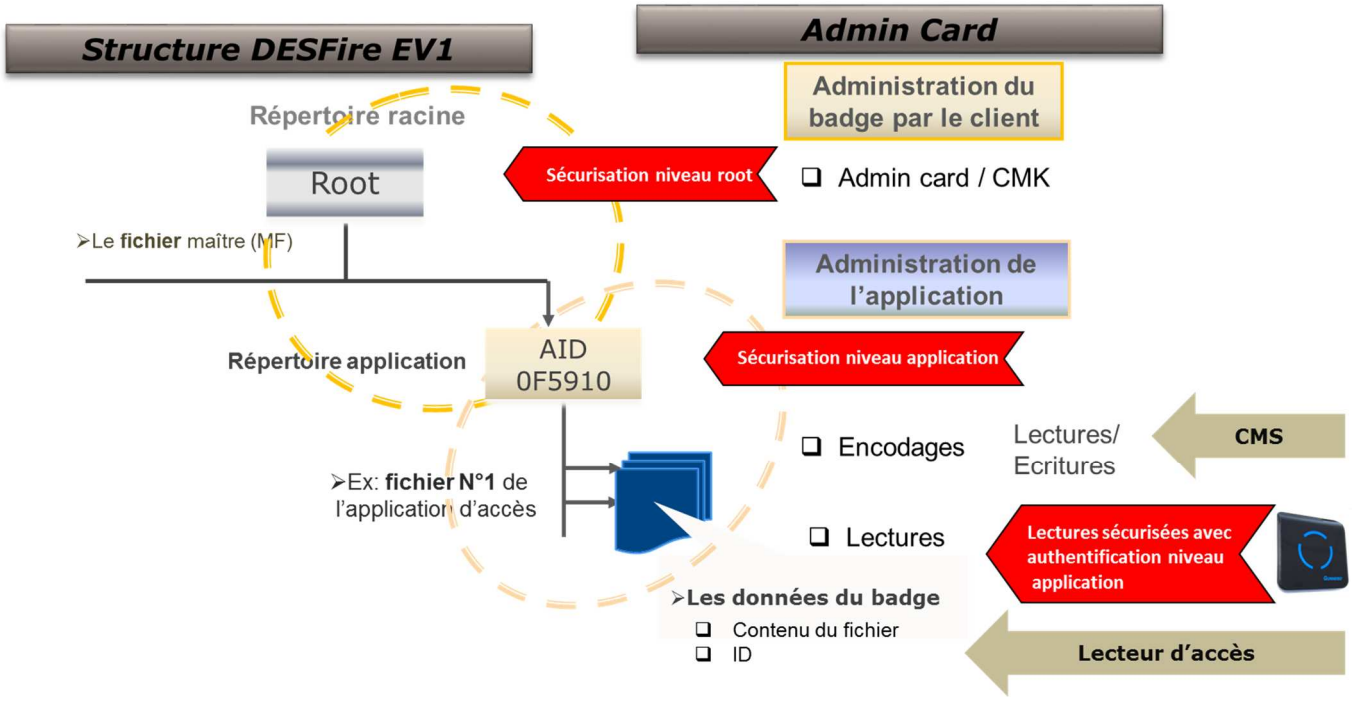


Figure 9 : Structure Mifare® DESFire

1) Le badge reçoit une personnalisation électrique :
   - Cette opération est réalisée au niveau d'un poste d'encodage. Ce poste fait partie d'un dispositif le « Card Management System (CMS) », qui est sous contrôle d'un responsable sûreté habilité et qui est gardien des secrets.
   - Le CMS est soit intégré à l'application SMI Server (ex : badges encodés par le client), soit complètement externalisé (ex : badges encodés par une société tierce).
2) La lecture sécurisée des badges par les lecteurs d'accès passe par un mécanisme d'authentification mutuelle entre le badge et le lecteur. Cette authentification se fait au niveau de l'application d'accès du badge.
3) La lecture dépend de la façon dont le badge a été administré niveau root et niveau application. Il est à noter que les fonctions de lectures sécurisées avec clés diversifiées font appel à différents algorithmes de calculs de clés possibles.
4) Cette lecture peut être réalisée de deux façons :
   a. avec une clé de lecture commune correspondant au niveau II (*)
   b. avec une clé diversifiée qui est une clé unique et correspondant au niveau III (*)

(*) Dans tous les cas, les badges correspondront **aux niveaux II et III** du tableau des niveaux de sûreté.

Note : Pour répondre aux différents besoins liés aux calculs des clés, ces fonctions sont traitées au niveau du contrôleur d'accès SM100+ et à partir d'algorithmes reconnus tels que AES, AES CBC, AESCMAC.