Cible de sécurité CSPN
Gestion d'accès physique – lecteur transparent

Date : 26/02/2013
Version : R11
Auteur : Emmanuel FIGUEIREDO

1- Page de garde

1.1 - Statut du document

Date d'application Sans objet
Version actuelle : R11
Développeurs : NEDAP NL
Commanditaire : THALES Communication & Security
Evaluateur : OPPIDA

1.2 - Diffusion

NOM	Prénom	Société
WOLF	Philippe	ANSSI
COAT	Anne	ANSSI
ANSEAUME	Bertrand	THALES
CARDE	Christophe	THALES
SOT	Alain	NEDAP France
PAYENS	Kees	NEDAP France
FIGUEIREDO	Emmanuel	NEDAP France
SCHIPPER	Hans	NEDAP NL
DEHAIS	Eric	OPPIDA
MORCEL	Anthony	OPPIDA

1.3 - Historique des versions

26/07/12 0.x Version préliminaire
10/09/12 : révision et modification de l'architecture
19/11/12 : révision et présentation technique définitive
18/01/13 : modifications suivant commentaires ANSSI
14/02/13 : révision hypothèses/menaces
26/02/13 : révision hypothèses/menaces et corrections
28/03/13 : modifications suivant commentaires ANSSI

2- Sommaire

3- Introduction

3.1 - Identification de la cible de sécurité

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN [1].

3.2 - Identification du produit

Catégorie	**Identification, authentification et contrôle d'accès**
Nom commercial du produit	NEDAP AEOS
Numéro de la version évaluée	3.0.2
Editeur des logiciels intervenants dans la solution	NEDAP NL- Access control unit AET – SAM security embedded softwares
Type de produit	Solution assurant la reconnaissance et l'autorisation de passage, individuel, sur des accès physiques sécurisés

3.3 - Références

Code	**Référence**	**Description/lien**
[1]	CSPN	Certification de Sécurité de Premier Niveau http://www.ssi.gouv.fr/fr/certification-qualification/cspn/
[2]	Java	Langage de programmation informatique orienté objet développé par ORACLE/Sun Microsystems et employé dans les applications et équipements de la solution NEDAP AEOS
[3]	AES	Algorithme de chiffrement symétrique
[4]	SSL	Doc NEDAP AEOS_InstallMan_Advanced_E.pdf, chapitre 11
[5]	TLS	Protocole d'échange synchronisé Version 1.1
[6]	NXP DESFire	Technologie RFID sans contact 13,56MHz. norme 14443B http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/
[7]	JavaCard	Technologie de puces de surface (contact) sécurisées développées par ORACLE : http://www.oracle.com/us/technologies/java/embedded/card/overview/index.html

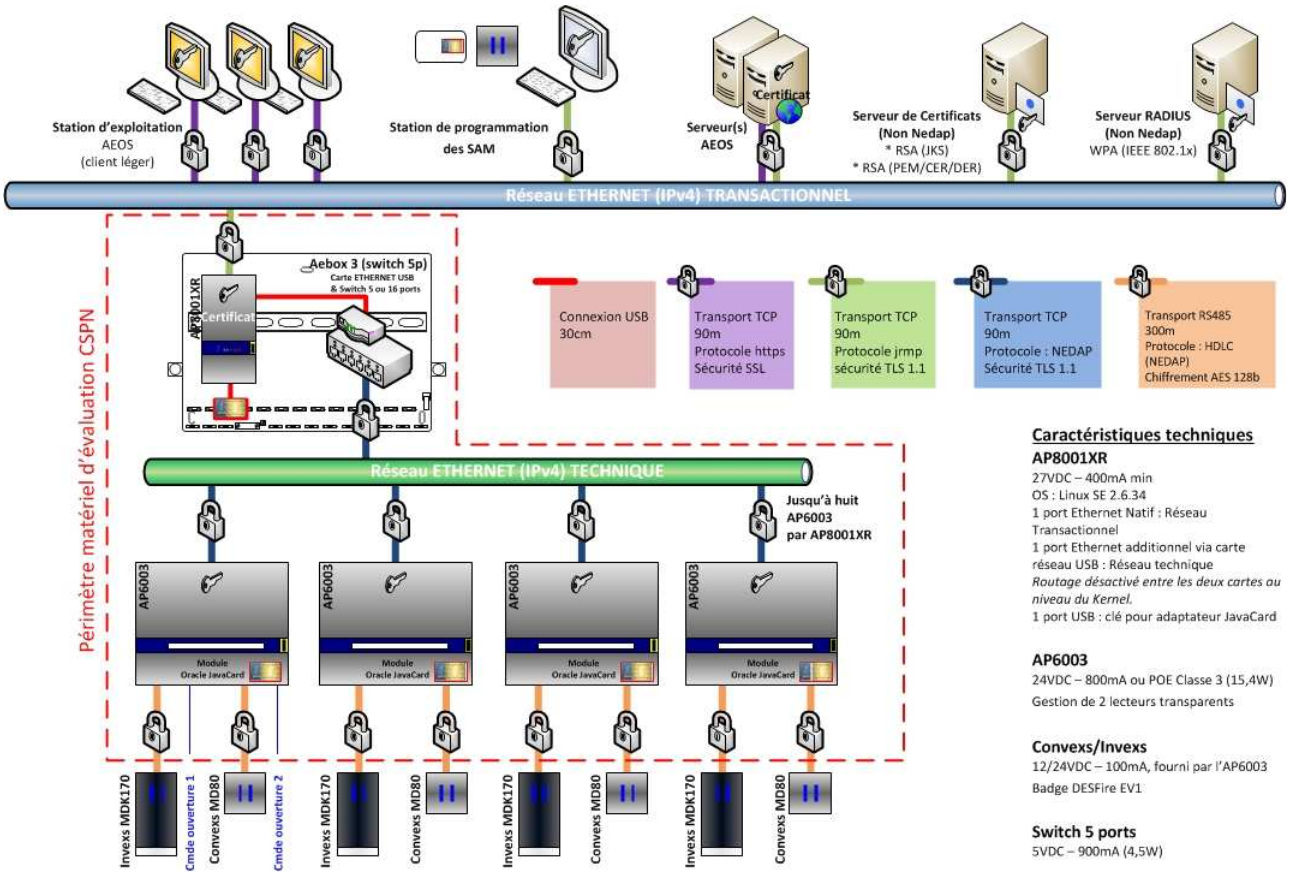
4- Argumentaire du produit

4.1 - Description générale du produit

4.1.1 - Liste des éléments constituant la solution de gestion des accès physiques sécurisée :

- Le serveur de gestion des accès AEOS
- Le serveur de certificat
- La station de programmation des SAM
- Le serveur d'authentification IEEE 802.1x, RADIUS
- Les postes (client léger) d'exploitation AEOS
- Les contrôleurs AP8001XR
- Les interfaces AP6003
- Les lecteurs Convexs et Invexs en configuration lecteur transparent
- Les badges DESFire EV1

4.1.2 - Schéma d'architecture



4.1.3 - Description fonctionnelle

La solution NEDAP AEOS est un système de contrôle d'accès physique, assurant la reconnaissance et la concordance d'actions/informations afin de déterminer si un utilisateur (porteur de badge) est autorisé à accéder à une zone sécurisé.

Les utilisateurs disposent de badges sans contact, en technologie RFID. Pour accéder à une zone sécurisée, un utilisateur doit présenter son badge dans le champ magnétique du lecteur de badge. Le système NEDAP AEOS accorde alors l'accès à la zone selon les autorisations de l'utilisateur.

La solution NEDAP propose deux procédures d'accès : une procédure d'accès sans confirmation par code PIN, et une procédure d'accès avec confirmation par code PIN.

Les lecteurs de badges sont installés en dehors de la zone à sécuriser. Ils ne disposent pas des clés en mémoire locale, ces dernières sont sécurisées dans le contrôleur qui les utilise dès qu'une opération le nécessite. Le terme « transparent » est utilisé pour qualifier le mode de fonctionnement, sans traitement, des lecteurs.

La solution NEDAP AEOS repose sur les équipements suivants : badge, lecteur de badge, module d'interface, contrôleur d'accès, serveur d'application, serveur de certificat, serveur d'authentification sur le réseau, station d'exploitation et station de programmation des SAM.

Ces équipements sont situés sur deux réseaux. Les serveurs et postes d'exploitation sont situés sur le réseau Ethernet TCP/IP transactionnel. Les équipements qui assurent l'interface avec les terminaux d'identification (lecteurs) et l'environnement physique des accès (serrures et/ou obstacles, alimentations, détecteurs, organes de sécurité) sont situés sur le réseau TCP/IP technique.

4.1.4 - Réseau Transactionnel (hors périmètre)

Le réseau Transactionnel est un réseau Ethernet (IPv4) établit et administré par le client final. Les différents serveurs de la solution sont déployés sur le réseau transactionnel ainsi que les postes d'exploitation de l'application AEOS et la station de configuration des SAM.

La configuration, l'administration et l'exploitation du système AEOS sont réalisés à partir des logiciels et IHM, hébergés par des postes informatiques, déployés sur le réseau Transactionnel.

Comme précisé dans l'hypothèse 4.4.1.1, ce réseau est installé dans un local sécurisé dont l'accès est strictement limité aux personnes habilités, par conséquent, ce réseau est hors du périmètre de l'évaluation.

Plusieurs serveurs sont installés sur ce réseau :

4.1.4.1 - Station de programmation des SAM

Rôle

La station de programmation des SAM permet l'encodage des SAM (JavaCard) implantées dans les contrôleurs et les interfaces, protégeant les données sensibles. (Les données sensibles sont décrites dans le chapitre 6 ainsi que dans l'annexe 1)

4.1.4.2 - Serveur applicatif AEOS

Rôle

Le serveur applicatif AEOS assure la gestion globale de la solution de sécurisation des accès développée par NEDAP. Le serveur AEOS est constitué d'un poste informatique sous environnement Microsoft Windows serveur et emploie une base de donnée professionnelle (Compatibilité : MS SQL ; Oracle ; PostgreSQL)
L'application AEOS a pour fonction de présenter une interface d'exploitation de gestion des accès complète, de centraliser les échanges avec les contrôleurs déployés sur le terrain et d'archiver toutes les informations sur configuration, les populations, les droits d'accès et les événements/alarmes horodatés dans une base de données.

Version des logiciels

L'installation du progiciel AEOS nécessite l'installation sur le poste serveur des logiciels suivants :

Developpeur	Désignation	Spécifications
Microsoft	**Windows 2012 server**	**Standard Edition**
Microsoft	**SQL 2012 server**	**Standard Edition**
Oracle	**Java RunTime Environment**	**/**

4.1.4.3 - Serveur de certificats

Rôle

Le serveur de certificats permet aux logiciels et aux contrôleurs de la solution NEDAP AEOS de faire générer les certificats intervenant dans les couches de sécurisation des communications.

Certificats mis en œuvre :

Protocole	Lien de communication	Type (format)	Réseau	Authentification
https	Serveur AEOS/Client web AEOS	PKCS#7 (PEM)	Transactionnel	Login/mdp
TLS 1.1	Station de configuration/Contrôleur AEOS	RSA (JKS)	Transactionnel	Mutuelle
TLS 1.1	Serveur AEOS/Serveur RADIUS*	WPA	Transactionnel	Mutuelle
TLS 1.1	Client web AEOS/Serveur RADIUS*	WPA	Transactionnel	Mutuelle
TLS 1.1	Contrôleur AEOS/Serveur RADIUS	WPA	Transactionnel	Mutuelle
TLS 1.1	SERVEUR AEOS/Contrôleur AEOS	RSA (JKS)	Transactionnel	Mutuelle
TLS 1.1	Contrôleur AEOS/Interface AEOS	RSA (JKS)	Technique	Mutuelle

* Certificats non déployés par NEDAP

4.1.4.4 - Serveur RADIUS d'authentification IEEE 802.1x

Rôle

Le serveur RADIUS a pour objectif d'identifier tous les équipements se connectant sur le réseau transactionnel, ce qui garantit contre toute connexion physique non autorisée. Les équipements actifs de type « switch » réalisent une isolation physique du port sur lequel l'équipement non identifié est connecté. Le serveur RADIUS est une mesure qui répond aux menaces identifiées au chapitre 7.

4.1.5 - Réseau Technique

Le réseau Technique est un réseau Ethernet (IPv4) établit et administré par l'intégrateur/mainteneur courant faible mandaté par le client final.

Comme cela est précisé dans la description des menaces, ce réseau est le point d'entrée des attaquants envisagés dans l'évaluation.

Sur ce réseau n'est déployé que les contrôleurs (AP8001XR) et interface UCP (AP6003) NEDAP

4.1.5.1 - Contrôleur d'accès AP8001XR

Rôle

Le contrôleur AP8001XR a pour fonction de contrôler la validité de passage d'une personne munie d'un badge DESFire sur un accès dont le franchissement est limité par un organe de serrurerie piloté. Son usage sert à restreindre l'accès à des zones sensibles. La nature des périphériques adjoints au contrôleur, lecteurs, identifiants, obstacles, est définie pour répondre à l'étanchéité de la zone à sécuriser.
Un contrôleur dispose d'une à huit interfaces (UCP : AP6003) qui lui permettent de gérer simultanément plusieurs lecteurs de badge et environnements d'accès.

Le contrôleur dispose d'une capacité de conservation de l'ensemble des données qui permettent d'autoriser/refuser un passage sur tous les accès gérés.
En cas d'indisponibilité du réseau transactionnel, le contrôleur est conçu pour assurer intégralement sa fonction sans dégrader le niveau de sécurité des accès contrôlés.

La perte du réseau transactionnel dégrade l'exploitation de la solution sur les points :

- Pas de mise à jour des autorisations et configuration des contrôleurs
- Pas de visualisation temps réel des passages, événements et alarmes.

Si des modifications sont entreprises par les opérateurs, au travers des postes d'exploitation, pendant que les contrôleurs sont isolés, les données et paramètres sont conservés par le serveur AEOS en base de données, pour être transférées automatiquement dès rétablissement de la connexion réseau.
Dans le même temps les contrôleurs conservent en mémoire locale l'ensemble des informations et alarmes horodatées qui ont eu lieu depuis la coupure pour un transfert complet vers le serveur après rétablissement du lien réseau.

Le contrôleur utilise le réseau Transactionnel pour remonter, en temps réel, l'ensemble des informations

de passage : événements, et alarmes techniques qui lui sont propres ainsi qu'aux équipements pilotés.

Le contrôleur fonctionne sur un principe événementiel. Si rien ne se produit ou ne change dans son environnement, aucun message n'est généré sur le réseau transactionnel en direction du serveur (UTC).

Architecture

L'UTL AP8001XR se présente sous 2 formats de boîtier. Le format est défini en fonction du nombre d'accès que l'unité est amenée à contrôler
1 à 8 lecteurs de badge : Coffret AEbox 3…
9 à 16 lecteurs de badge : Coffret AEbox 4
Les deux formats d'intégration de l'UTL sont constitués de :

Matériel	**Désignation**	**Quantité**	**Interchangeable ***
UTL, gestion de 1 à 8 lecteurs			
Coffret	AEbox3	x1	Oui
Contrôleur	AP8001XR	x1	Non
Carte réseau additionnelle	DUB-E100	x1	Oui
Adaptateur SAM	Omnikey 6121	x1	Oui
Switch 5 ports	DES-105	x1	Oui
SAM – JavaCard	JCOP v21 – J2A	x1	Non
UTL, gestion de 1 à 16 lecteurs			
Coffret	AEbox4	x1	Oui
Contrôleur	AP8001XR	x1	Non
Carte réseau additionnelle	DUB-E100	x1	Oui
Adaptateur SAM	Omnikey 6121	x1	Oui
Switch 16 ports	DES-1016d	x1	Oui
SAM – JavaCard	JCOP v21 – J2A	x1	Non

* Interchangeable : Par cette notion NEDAP spécifie que d'autres équipements de marque ou de séries différentes à celle préconisées, peuvent être utilisés pour un besoin d'adaptation spécifique.
Exemple 1 : il est possible de créer une UTL 1 à 8 LB en utilisant un switch 5 ports POE pour assurer l'alimentation des équipements.
Exemple 2 : L'UTL peut être intégrée dans un coffret, auto protégé, différent du coffret AEbox pour répondre à des contraintes d'implantation, de concentration, de sécurisations particulières.

L'AP8001XR embarque un SAM hardware (JavaCard) pour la protection des données sensibles identifiées dans le chapitre 6.

Caractéristiques techniques

Processeur : Marvell 88F6180
Linux version 2.6.34
Oracle JAVA SE Embedded 6

Version des logiciels

Les matériels NEDAP sont livrés avec des microprogrammes par défaut, chargés en usine.
La configuration de l'AP8001XR, pour assurer les fonctions de sécurisation des données et de gestion de

lecteurs transparents, nécessite le déploiement d'une version spécifique de microprogrammes.

Désignation		Microprogrammes à mettre en œuvre
AP8001XR	Kernel	KF8001_543v302
	Firmware	AP8001X_543v304
	Configuration	Eth1-update_V5.2

4.1.5.2 - Interfaces AP6003

Rôle

L'AP6003 a pour fonction de gérer la communication avec 1 ou 2 lecteurs de badges « transparent » ainsi que les informations et commandes techniques en provenance des environnements de portes pilotés.
L'AP6003 ne réalise aucune prise de décision locale concernant les autorisations d'accès, il ne fait que reporter au contrôleur auquel il est raccordé (AP8001XR – Réseau Technique) le statut des équipements supervisés

(Configuration d'accès standard)

- Lecteur de badge (protocole)
- Code PIN (protocole)
- Contact d'état de la porte (entrée d'acquisition)
- Bouton poussoir de sortie (entrée d'acquisition)
- Commande d'ouverture (sortie relais)

Architecture

L'AP6003 embarque un SAM hardware (JavaCard) pour la protection des données sensibles identifiées dans le chapitre 6. Le SAM est également sollicité dans les échanges chiffrés DESFire avec les badges présentés devant les lecteurs transparents.

Caractéristiques techniques

Processeur : NXP LPC2387

Version des logiciels

Les matériels NEDAP sont livrés avec des microprogrammes par défaut, chargés en usine.
La configuration de l'AP6003, pour assurer les fonctions de sécurisation des données et de gestion de lecteurs transparents, nécessite le déploiement d'une version spécifique de microprogrammes.

Désignation		Microprogrammes à mettre en œuvre
AP6003	Kernel	KF6003_2387v100
	Firmware	AP6003rs485HDLC_2387v100
	Configuration	NR172

Pré requis

L'AP6003 ne dispose d'aucun compte de connexion car l'ensemble de ses comportements sont définis par les microprogrammes chargés.

4.1.5.3 - Lecteurs de badge

Rôle

Les lecteurs de badge sont des lecteurs Convexs et Invexs de la gamme NEDAP AEOS.
Le qualificatif « transparent » signifie que le lecteur ne dispose d'aucune clé privée dans sa mémoire locale, les clés privées sont sécurisées dans un SAM hardware (JavaCard) implanté dans le contrôleur AP8001XR et l'interface AP6003, qui les sollicite lors des procédures d'autorisation d'accès.

Architecture

On distingue 2 types de lecteurs employés dans la solution :

- Les lecteurs de type Convexs qui permettent l'initialisation d'échange de données avec les badges DESFire qui leur sont présentés (RFID)
- Les lecteurs de type Invexs qui permettent l'initialisation d'échange de données avec les badges DESFire qui leur sont présentés (RFID) et propose un clavier numérique pour confirmer les porteurs de badge par code PIN (badge + code personnel).

Version logicielle

Les matériels NEDAP sont livrés avec des microprogrammes par défaut, chargés en usine.
La configuration des lecteurs Convexs et Invexs, afin d'assurer un comportement « transparent », nécessite le déploiement d'une version spécifique de microprogrammes.

Désignation		Microprogrammes à mettre en œuvre
Convexs Invexs	Kernel	KF_2138_HDLCv200
	Firmware	TRSRDR_2138v200

Le firmware spécifique TRSRDR 2138v200 désactive la fonction de programmation des lecteurs Convexs et Invexs par badge maître.

4.2 - Description de l'environnement d'utilisation du produit

Utilisation usuelle :
A l'heure actuelle dans les opérations de contrôle des accès, mettant en œuvre des badges RFID technologie NXP DESFire EV1 avec chiffrement des échanges par l'algorithme AES 128, les lecteurs disposent localement des clés privées.
Les lecteurs sont installés en dehors de la zone à sécuriser et présentent deux risques :

a) Communication avec le contrôleur par utilisation de protocoles standards (Volonté des clients de disposer d'une liaison non propriétaire pour faciliter tout changement de produit/fournisseur)
b) Information sensible (clés privées) enregistrées dans le lecteur

Utilisation du produit NEDAP AEOS (cible)

La solution NEDAP met en œuvre différentes fonctions afin de pallier à l'utilisation usuelle décrite ci-dessus, par l'emploi de lecteur dit « transparent » et d'équipement de gestion (contrôleur) disposant de mécanismes de protection des données sensibles.
Le qualificatif « transparent » signifie que les lecteurs Convexs et Invexs de la gamme NEDAP AEOS, ne disposent pas des clés privées en mémoire locale, elles sont sécurisées dans un SAM hardware. Les clés privées ne sortent jamais de l'espace sécurisé du SAM

4.3 - Description d'une procédure d'accès

Les badges sont fournis et encodés par un fournisseur (société spécialisé) prestataire du client final. Les badges sont de technologie DESfire EV1 et l'encodage consiste en la création d'une « application » dédiée au contrôle d'accès, qui comporte une clé diversifiée de 16 octets.
La diversification s'appuie sur l'algorithme AESCMAC (NIST 800 38B) appliqué à la clé maître/mère, des paramètres spécifiques et l'UID du badge. Il est ainsi obtenu une clé diversifiée ou dérivée, qui est encodée dans le badge. La clé diversifiée est employée pour le chiffrement AES128bits, réalisé par le badge avant toute transmission de l'identifiant.

4.3.1 - Sans confirmation par PIN code

Un badge DESfire valide est présenté par son détenteur devant un lecteur Convexs. Le lecteur est programmé pour rechercher une application spécifique dans le badge afin d'en obtenir un identifiant. Lorsque le badge est dans le champ du lecteur, l'application DESFire va transmettre au lecteur l'UID du badge en clair ainsi que l'identifiant chiffré en AES128bits en utilisant la clé diversifiée dont il dispose.
Ces informations sont communiquées à l'AP6003 via une liaison RS485 et un protocole HDLC. L'AP6003 dispose dans son module SAM (JavaCard) de la clé mère et des paramètres permettant d'utiliser l'algorithme ASECMAC afin de recalculer la clé diversifiée utilisée par le badge à partir de l'UID reçu.
L'identifiant est alors déchiffré (8 Caractères hexadécimaux - 4 octets). L'AP6003 sollicite le module SAM pour chiffrer de nouveau l'identifiant avant de le transmettre via le réseau Technique à l'AP8001XR. Sous sécurisation TLS 1.1.
L'AP8001XR déchiffre l'identifiant reçu, contrôle tous les paramètres d'autorisation, droits, plage horaire, plage journalière, conditions spéciales, pour valider si le franchissement de l'accès est légitime.
L'AP8001XR transmet un ordre de déverrouillage à l'AP6003 afin de permettre le passage du porteur de badge. Dans le même temps, l'AP8001XR génère un événement de passage autorisé, horodaté, pour enregistrement par le serveur d'application AEOS.

4.3.2 - Avec confirmation par PIN Code

Sur certain accès, le lecteur dispose d'un clavier numérique intégré afin que la procédure d'accès ne soit pas basée que sur la reconnaissance d'un badge avec des droits d'accès, mais que le porteur du badge soit également confirmé.
Dans les processus d'échange et de reconnaissance, la demande de saisie du Code PIN intervient lorsque la validité des droits d'accès est confirmée à l'AP6003, par l'AP8001XR.
Si la validité est confirmée, l'AP8001XR génère une « clé PIN publique » et la transfert au lecteur Invexs en même temps que la confirmation par code PIN.
Le lecteur initialise le processus de saisi du code personnel. Lorsqu'un code PIN est saisi, il est chiffré en AES128bits avec la « clé PIN publique » et transmis via une liaison RS485 protocole HDLC à l'interface AP6003. Le code PIN (toujours chiffré) est transmis de l'AP6003 à l'AP8001XR via le réseau Technique

sous sécurisation TLS1.1. L'AP8001XR déchiffre le code PIN et vérifie que ce dernier est bien associé au porteur de badge de l'identifiant précédemment reçu.
3 essais sont autorisés pour permettre la saisie du code PIN associé au détenteur du badge.
3 refus entrainent la génération d'un événement d'accès refusé pour raison spécifique « code PIN erroné »
1 saisie correcte confirme le déverrouillage de l'accès et la génération d'un événement de passage autorisé précisant la confirmation par code PIN.

Si aucun code PIN n'est saisi, un « time out » géré par l'AP8001XR qui effectue la réinitialisation du processus. Un événement spécifique est alors généré pour signaler le « time out ».
Le système est en attente de la présentation d'un badge DESFire valide devant le lecteur.

4.4 - Hypothèses sur l'environnement du produit

4.4.1 - Hypothèses sur l'environnement physique du produit

4.4.1.1 - *Installation des serveurs*

Pour l'évaluation, il est supposé que les serveurs (station de programmation des SAM, serveur AEOS, serveur de certificat) sont installés dans un local informatique sécurisé dont l'accès est strictement limité aux personnels habilités.

4.4.1.2 - *Installation du contrôleur AP8001XR et des interfaces AP6003*

Pour l'évaluation, ils sont supposés que le contrôleur AP8001XR ainsi que ses interfaces AP6003 sont installés dans un local technique sécurisé dont l'accès est limité.

4.4.1.3 - *Installation des lecteurs*

Pour l'évaluation, il est supposé que les lecteurs sont implantés de façon à garantir une gestion périmétrique hermétique :

- Site(s)
- Zone(s)
- Local (locaux)

Aucun câble, ni aucun équipement ne sont posés/installés en zone non protégée, exception du lecteur de badge Convexs, Invexs. Le câble de raccordement des lecteurs de badge doit être traversant. Il ne doit pas courir le long de la porte en zone non protégé, même au travers d'une goulotte ou d'un tube de protection.
Le câble assurant la liaison entre les lecteurs Convexs, Invexs et les contrôleurs est supposé direct.
Le câblage de l'ensemble des équipements constituant les environnements de porte est direct, point à point.

4.4.1.4 - *Installation des accès*

Consulter la liste des équipements minimum présentés dans le chapitre 4.1.8.1.

4.4.2 - Hypothèses sur les exploitants du produit

Les personnels exploitant de la solution sont supposés appartenir à l'organisation interne de gestion de la sureté, du client, ou être mandataire de ce service sous son contrôle et autorité.
Ils sont supposés avoir suivi une formation spécifique à leurs attributions et aux tâches qui leurs sont confiées.
Ils disposent tous, d'un compte de connexion à l'application NEDAP AEOS, individuel. Basé sur une identification par Login+Mot de passe. La gestion des comptes exploitant devra s'appuyer sur les « Recommandations de sécurité relatives aux mots de passe » rédigées par l'ANSSI

4.4.3 - Hypothèses sur les porteurs de badges

Les porteurs de badge sont les utilisateurs finaux de la solution. Ils disposent de badges sans contact (RFID) DESFire EV1 et éventuellement de code PIN personnel.

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

4.4.4 - Hypothèses sur l'environnement technique du produit

4.4.4.1 - *Serveur NEDAP AEOS*

- Serveur (UTC) aux caractéristiques préconisées et déployant les logiciels énumérés dans le chapitre 4.1.4.3.
- Le système est protégé des virus et ne permet pas l'exécution de code malveillant
- Le niveau de protection du réseau Transactionnel sera équivalent ou supérieur…
- Toutes les mises à jour de sécurité, Windows 2008/2012 serveur et outils, disponibles sont installées
- 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

4.4.4.2 - *Architecture réseau*

Les réseaux transactionnel et technique sont supposés être cloisonnés. Aucune passerelle, informatique ou de transmission de données, ne doit être mise en œuvre entre ces réseaux.
Les échanges de données entre les deux réseaux (intercommunication AP8001XR) sont filtrés par un pare-feu intégré au contrôleur. La procédure de configuration du pare-feu, établi par NEDAP, devra être réalisée.

4.4.4.3 - *Contrôleur AP8001XR*

Un compte utilisateur usine, est configuré par défaut dans tous les AP8001XR neufs livrés. Il est convenu que ce compte a été désactivé et qu'un nouveau compte utilisateur a été créé et maintenu secret. Ce compte s'adresse à l'intégrateur ainsi qu'au mainteneur, mandaté par le client final.

4.4.4.4 - *Certificats électroniques*

- Dans la mise en œuvre de la sécurisation TLS, les certificats sont émis par le serveur de certificat, déployé par le client final, en se conformant aux recommandations NEDAP :

Liste des liens de communication concernés par l'usage de certificats ou de clés de session :

- Entre Serveur AEOS et poste d'exploitation (client léger) : Https
- Entre Serveur AEOS et UTL (AP8001XR) : JRMP sous TLS 1.1
- Entre Serveur AEOS et Serveur RADIUS (IEEE 802.1x) : EAP sous TLS 1.1
- Entre UTL (AP8001XR) et Serveur RADIUS (IEEE 802.1x) : EAP sous TLS 1.1
- Entre poste d'exploitation (client léger) et Serveur RADIUS (IEEE 802.1x) : EAP sous TLS 1.1
- Entre UTL (AP8001XR) et les UTC (AP6003) : protocole NEDAP sous TLS 1.1
- Entre ULT (AP8001XR) et les lecteurs INVEXS (gestion de code PIN) : clé de session générée par l'AP8001XR pour le chiffrement du Code PIN en AES128bits, pour transfert sous protocole HDLC

4.4.4.5 - *Badges technologie DESFire EV1*

Les badges doivent être livrés encodés (processus préliminaire non réalisé par NEDAP) :

- Identifiant du badge (8 caractères HEXA -4 octets)
- Clé DESFire diversifiée
- Paramètre DESFire spécifiques

4.4.4.6 - *Lecteurs de badge*

Les lecteurs de badges sont déployés en configuration « transparent » ce qui implique qu'ils n'interviennent pas dans le chiffrement ou déchiffrement de l'identifiant DESFire. Ils assurent le transite de l'identifiant déjà chiffré par le badge en AES 128bits. Les paramètres de chiffrement sont définis par le client et programmés respectivement dans la SAM, mise en œuvre dans l'UCP (AP6003), et les badges DESFire EV1.

4.5 - Description des utilisateurs typiques

Les acteurs concernés par l'utilisation et la mise en œuvre du produit sont :

4.5.1 - Exploitants

Les exploitants sont les personnels appartenant à l'organisation interne de gestion de la sureté du client, ou être mandataire de ce service sous son contrôle et autorité.
Ils ont pour fonction de configurer et adapter au quotidien les différentes fonctions du système NEDAP AEOS, qui concourent à attribuer des autorisations d'accès sur l'ensemble des portes et obstacles physique contrôlés.

Toute connexion des exploitants au système de gestion NEDAP AEOS est tracée dans l'historique des événements en distinguant le login de l'utilisateur et l'adresse IP du contrôleur

4.5.2 - Agents techniques

Les agents techniques sont les personnels intervenant dans le cadre des opérations de mise en service (déploiement) et de maintenance.
Aucun exploitant n'est amené à se connecter directement sur les contrôleurs, c'est une prérogative des agents techniques.

Toute connexion au contrôleur est tracée dans l'historique des événements en distinguant le login de l'utilisateur et l'adresse IP du contrôleur

4.5.3 - Porteurs de badge

Les porteurs de badge sont les utilisateurs finaux de la solution. Ils disposent de badges sans contact (RFID) DESFire EV1 et éventuellement de code PIN personnel. Au sein des porteurs de badge, on distingue 4 populations, Résident, Visiteur, Prestataire et véhicule, pour lesquels le système de contrôle d'accès dispose de moyens de gestion spécifiques

4.6 - Description du périmètre de l'évaluation

La cible prévoie l'évaluation des équipements suivants :

- Les contrôleurs AP8001XR
- Les interfaces AP6003

5- Description de l'environnement technique de fonctionnement

Les éléments suivants ou leur simulation sont nécessaires à l'évaluation:

5.1.1 - Dispositifs d'accès

- Gestion d'environnement d'accès disposant des équipements minimums :
  - Détecteur d'ouverture (état de la porte)
  - Bouton poussoir (commande de sortie)
  - Contact sec de confirmation de passage pour les obstacles physiques
  - Organe de serrurerie condamnant l'accès (pilotage par action sur l'alimentation de l'organe ou commande par contact sec)

5.1.2 - Postes Informatiques

- Microsoft Windows 2008 serveur, dernier correctif
- Microsoft Windows 7, dernier correctif
- Microsoft Windows SQL 2012, dernier correctif

5.1.3 - Badges

Les opérations de contrôle des accès mettent en œuvre des badges RFID technologie NXP DESFire EV1, pré encodés.

5.1.4 - JavaCard (SAM)

- JavaCard : J2A080
- JCOP : 21 version 2.4.1 ou supérieure
- Processeur : P5CC080

6- Données sensibles

6.1 - Description

Les biens sensibles protégés par la solution sont :

Biens/données sensibles	Intégrité	Confidentialité	Disponibilité
Les clés privées DESfire	Non	Oui	Non
Les certificats intervenants dans les échanges chiffrés TLS	Non	Oui	Non
Les certificats intervenants dans l'authentification 802.1x	Non	Oui	Non
Les identifiants individuels des utilisateurs	Non	Oui	Non
Les droits/autorisations d'accès des utilisateurs	Non	Oui	Non
Les codes PIN des utilisateurs de badge	Non	Oui	Non

6.2 - Répartition des données sensibles dans les équipements techniques de la solution

Voir tableau en annexe 1.

7- Description des menaces

Pour l'évaluation, les attaquants suivants sont considérés :

- Attaquant sur le réseau TCP/IP transactionnel : attaquant présent sur le réseau TCP/IP transactionnel ;
- Attaquant sur le réseau TCP/IP Technique : attaquant présent sur le réseau TCP/IP Technique ;
- Attaquant intervenant sur le contrôleur AP8001XR
- Attaquant externe sur la liaison RS485 établie entre le lecteur de badge/UCP (AP6003)

Ne sont pas pris en compte les menaces dont les points d'entrée sont les postes informatiques serveurs et postes d'exploitations, ni les badges.

En tenant compte des hypothèses d'environnement, sont considérées les menaces suivantes :

7.1 - Intrusion sur le réseau Transactionnel

Un attaquant est connecté sur le réseau Ethernet TCP/IP Transactionnel et déploie des moyens d'écoute dans le but d'identifier des données sensibles ou d'effectuer des attaques par rejeu de transaction/commandes

Ecoute des transactions échangées entre le serveur (UTC) et les contrôleurs (AP8001XR)	
Transaction	**Menaces**
Toute transaction contenant l'identifiant d'un porteur de badge	Interception du format des identifiants DESFire, dans le but de reproduire un badge ou d'en créer de nouveaux
Toute transaction contenant le code PIN d'un porteur de badge	Interception du PIN code associé à un badge (usurpation d'identité d'accès)
Modification des droits d'accès d'un porteur de badge existant	Rejeu d'une transaction (adaptée) pour réaliser des modifications des droits d'un badge existant avec des autorisations étendues
Affectation des droits d'accès d'un porteur de badge sur un accès	Rejeu d'une transaction (adaptée) pour attribuer à un badge existant des autorisations sur un accès
Modification d'une plage horaire/ d'une plage journalière	Rejeu d'une transaction pour faire modifier une plage limitée en plage étendue (8h00-18h00 => 0h00 23h59)
Affectation d'un badge temporaire	Rejeu d'une transaction (adaptée) pour transférer les droits d'accès d'une personne sur un badge utilisé par un tiers (usurpation d'identité d'accès)
Modification des droits d'accès d'un porteur de badge, désactivation du code PIN	Rejeu d'une transaction permettant de désactiver la fonction de vérification associée à une personne, puis de voler le badge pour l'utiliser en autorisation d'accès directe.

Ecoute des commandes échangées entre le serveur (UTC) et les contrôleurs (AP8001XR)	
Commande	**Menaces**
Déverrouillage ponctuel d'un accès ou de tous les accès	Rejeu d'une commande d'ouverture pour permettre le franchissement de l'accès
Déverrouillage permanent d'un accès ou de tous les accès	Rejeu d'une commande d'ouverture pour permettre le franchissement de l'accès
Déverrouillage sur plage horaire d'un accès ou de tous les accès	Rejeu d'une commande d'ouverture pour permettre le franchissement de l'accès sur une période programmée

7.2 - Intrusion sur le réseau Technique

Un attaquant est connecté sur le réseau Ethernet TCP/IP Technique et déploie des moyens d'écoute dans le but d'identifier des données sensibles, d'effectuer des attaques par rejeu de transaction/commandes, ou d'utiliser l'AP8001XR comme passerelle pour atteindre le réseau Transactionnel.

Tentative d'accès au réseau Transactionnel via le contrôleur AP8001XR	
Connexion	**Menaces**
Attaque visant à établir une connexion/liaison sur réseau transactionnel en utilisant le contrôleur AP8001XR comme passerelle entre les deux réseaux	Ecoute sur le réseau Transactionnel à partir du réseau Technique

Ecoute des transactions échangées entre un contrôleur (AP8001XR) et ses interfaces (AP6003)	
Transaction	**Menaces**
Toute transaction contenant l'identifiant d'un porteur de badge	Interception des identifiants individuels des utilisateurs, dans le but de reproduire un badge ou d'en créer de nouveaux
Toute transaction contenant le code PIN d'un porteur de badge	Interception du PIN code associé à un badge (usurpation d'identité d'accès)

Ecoute des commandes échangées entre un contrôleur (AP8001XR) et ses interfaces (AP6003)	
Commande	**Menaces**
Commande de changement d'état de l'un des relais pilotant les organes de serrurerie sous gestion du contrôleur	Rejeu d'une commande d'ouverture pour permettre le franchissement de l'accès

7.3 - Intrusion Externe

Un attaquant, situé en zone non protégée, est connecté la liaison RS485 entre le lecteur de badge et l'UCP (AP6003) pour obtenir des données sensibles de l'AP6003.

Ecoute des transactions échangées entre un lecteur de badge et son UCP (AP6003)	
Transaction	**Menaces**
Transaction d'instanciation	Initier un mode « configuration/console » avec l'AP6003 pour obtenir des données sensibles

Note : Les menaces portant sur le vol d'équipements, comme par exemple le vol du contrôleur AP8001XR ou des lecteurs de badge, ne sont pas retenues pour l'évaluation. Ces menaces impliquent des attaques de type matériel. Les menaces concernant la substitution ou l'émulation de lecteur de badge ne sont pas retenues pour les mêmes raisons.

Aucune attaque de type matériel ne sera effectuée pour la présente évaluation.

8- Description des fonctions de sécurité

1. Protection en transmission de l'identifiant personnel
   Les identifiants personnels des porteurs de badge, encodés dans les badges DESFire EV1, utilisés dans la solution, sont protégés en confidentialité lors de leur transmission par un chiffrement en AES 128bits (clé diversifiée)

2. Protection en transmission du code PIN
   Les codes PIN sont protégés en confidentialité par chiffrement AES 128bits réalisé par le lecteur de badge, via une clé publique transmise par le contrôleur AP8001XR

3. Protection des données échangées entre serveur AEOS et contrôleur AP8001XR
   Les commandes et transactions échangées entre le serveur AEOS et le contrôleur AP8001XR sont protégées en confidentialité et contre les tentatives de rejeu par la mise en œuvre du protocole de chiffrement TLS 1.1 avec clé RSA au format JKS de 2048bits.

4. Protection des données échangées entre contrôleur AP8001XR et interface AP6003
   Les commandes et transactions échangées entre le contrôleur AP8001XR et les interfaces AP6003 sont protégées en confidentialité et contre les tentatives de rejeu par la mise en œuvre du protocole de chiffrement TLS 1.1 avec clé RSA au format JKS de 2048bits.

5. Sécurisation du contrôleur AP8001XR pour qu'il ne soit pas une passerelle entre les réseaux Transactionnel et Technique
   Configuration du FIREWALL logiciel embarqué dans le contrôleur AP8001XR pour filtrer intégralement les deux réseaux, Transactionnel et Technique, sur lesquels il est implanté.

6. Sécurisation de la console de configuration AP6003
   Les interfaces AP6003 disposent d'un port de configuration dédié (USB) qui ne fait pas appel à ses liaisons de communication nécessaires à ses fonctions (réseau Technique ou liaison série vers les lecteurs de badge)

9- Argumentaire de couverture des menaces

Menaces	Fonctions de sécurité mise en œuvre pour couvrir la menace					
	(1)	(2)	(3)	(4)	(5)	(6)
Intrusion sur le réseau Transactionnel						
Interception du format des identifiants DESFire, dans le but de reproduire un badge ou d'en créer de nouveaux	■		■			
Interception du PIN code associé à un badge (usurpation d'identité d'accès)		■	■			
Rejeu d'une transaction (adaptée) pour réaliser des modifications des droits d'un badge existant avec des autorisations étendues			■			
Rejeu d'une transaction (adaptée) pour attribuer à un badge existant des autorisations sur un accès			■			
Rejeu d'une transaction pour faire modifier une plage limitée en plage étendue (8h00-18h00 => 0h00 23h59)			■			
Rejeu d'une transaction (adaptée) pour transférer les droits d'accès d'une personne sur un badge utilisé par un tiers (usurpation d'identité d'accès)			■			
Rejeu d'une transaction permettant de désactiver la fonction de vérification associée à une personne, puis de voler le badge pour l'utiliser en autorisation d'accès directe.			■			
Déverrouillage ponctuel d'un accès ou de tous les accès			■			
Déverrouillage permanent d'un accès ou de tous les accès			■			
Déverrouillage sur plage horaire d'un accès ou de tous les accès			■			
Intrusion sur le réseau Technique						
Ecoute sur le réseau Transactionnel à partir du réseau Technique			■		■	
Interception du format des identifiants DESFire, dans le but de reproduire un badge ou d'en créer de nouveaux	■			■		
Interception du PIN code associé à un badge (usurpation d'identité d'accès)		■		■		
Rejeu d'une commande d'ouverture pour permettre le franchissement de l'accès				■		
Intrusion Externe						
Interception de données sensibles via le mode de configuration de l'AP6003						■

10- Description des mécanismes cryptographiques mis en œuvre dans la solution

10.1 - Réseau transactionnel

a) Echange de données entre le serveur RADIUS (IEEE802.1x) et les équipements AEOS : UTC (Application serveur AEOS) et contrôleurs UTL (AP8001XR)
Coté serveur AEOS et AP8001XR :

- ✓ Protocole TLS 1.1 : JSSE (Java Socket Secure Extension)
- ✓ Fichier de certificat type : JKS (Java Key Storage)
- ✓ Certificat : RSA (fourniture client final)
- ✓ Certificat Authority : A définir

b) Echange de données entre le serveur d'application AEOS et les contrôleurs (UTL) AP8001XR :
Coté serveur AEOS :

- ✓ Protocole TLS 1.1 : JSSE (Java Socket Secure Extension)
- ✓ Fichier de certificat type : JKS (Java Key Storage)
- ✓ Certificat : RSA (fourniture client final)
- ✓ Certificat Authority : A définir

Coté contrôleurs (UTL) AP8001XR :

- ✓ Protocole TLS 1.1 : JSSE (Java Socket Secure Extension)
- ✓ Fichier de certificat type : JKS (Java Key Storage)
- ✓ Certificat : RSA (fourniture client final)
- ✓ Certificat Authority : A définir

10.2 - Réseau technique

Echange de données entre le contrôleur (UTL) AP8001XR et les modules déportés (UCP) AP6003 :
Coté contrôleurs (UTL) AP8001XR :

- ✓ Protocole SSL : JSSE (Java Socket Secure Extension)
- ✓ Fichier de certificat type : JKS (Java Key Storage)
- ✓ Certificat : RSA (fourniture client final)
- ✓ Certificat Authority : A définir

Coté module déporté (UCP) AP6003 :

- ✓ Protocole SSL : PolarSSL
- ✓ Fichier de certificat type : PEM/CER/DER
- ✓ Certificat : RSA (fourniture client final)
- ✓ Certificat Authority : A définir

10.3 - Badges (hors évaluation CSPN)

Les badges sont de technologie DESFire développée par NXP.
Les échanges de données entre les badges et les lecteurs se réalisent sans contact sur les principes de la RFID (Radio Frequency Identification)
La technologie DESFire propose un cadre d'utilisation standard et sécurisé. Avant leur distribution, les badges DESFire sont encodés par le client final. Cette phase d'initialisation a pour but de personnaliser électriquement un badge en y programmant une application qui va héberger l'identifiant de contrôle d'accès ainsi que les paramètres associés à sa sécurisation. Une contrainte d'unicité est appliquée aux identifiants de contrôle d'accès afin de ne permettre aucun doublon.
Les badges sont sous la responsabilité des porteurs de badges à qui ils ont été distribués, car employés pour les identifiés individuellement.

Afin de protéger en confidentialité les identifiants, ils sont chiffrés avec un algorithme AES128bits avant toute transmission.
Le badge DESFire réalise ce chiffrement en utilisant une clé diversifiée, préalablement établi à l'aide de son UID et d'autres données secrètes. L'algorithme de diversification est l'AESCMAC (NIST 800 38B) et il est implémenté et ses paramètres sécurisé dans tous les SAM (Javacard) équipant les interfaces AP6003. Les SAM des AP6003 disposent également de la clé privée DESFire employée pour calculer les clés diversifiées encodées dans les badges. Lors d'une procédure d'accès, le badge transmet l'identifiant chiffré ainsi que son UID. Ces informations sont transportées par les lecteurs, sans traitement, pour être transmis jusqu'à l'AP6003. Le SAM de l'interface AP6003 dispose de toutes les informations pour recalculer la clé diversifiée et ainsi déchiffrer la trame reçue pour en extraire l'identifiant.

10.4 - Lecteur de badge INVEXS

Pour des raisons de sûreté il peut être demandé au système de gestion des accès de s'assurer que le porteur du badge est son porteur légitime. Une des solutions est d'utiliser un numéro « secret » d'identification personnel (code PIN) qui devra être confirmé lors de la procédure d'accès. Ce code PIN est acquit sur des lecteurs de badges spécifiques (INVEXS) qui mettent à disposition un clavier numérique.
Les codes PIN ne sont pas encodés dans les badges, ils sont mémorisés par les porteurs de badge.
Ils ont été préalablement définis et renseignés via l'IHM du système de gestion des accès. Les codes PIN une fois définis, sont transférés dans les contrôleurs de terrain AP8001XR pour permettre une comparaison locale aucours d'une procédure d'accès.
La confirmation du porteur de badge par code personnel étant un paramètre activable par les exploitants du système, c'est le contrôleur AP8001XR qui informe le lecteur INVEXS que pour le badge qui vient d'être présenté une confirmation doit être réalisée.

Afin de protéger en confidentialité les codes PIN, ils sont chiffrés avec un algorithme AES128bits avant toute transmission.
A chaque transaction, lorsque le contrôleur AP8001XR signifie au lecteur INVEXS qu'une confirmation par code PIN est requise, il auto génère une paire de clés (privée et publique) pour chiffrer le code qui va être transmis. La clé publique est transmise au lecteur en même temps que l'ordre d'activer son clavier.

Lorsque le lecteur réceptionne la clé publique il génère, à partir de cette clé, deux clé AES de 16 octets chacune. L'une pour le chiffrement l'autre pour garantir l'intégrité des données (CMAC). Mode CTR.
Le résultat du chiffrement est remonté au contrôleur AP8001XR, qui décrypte les données à partir de la clé privée initialement générée pour cet échange.
Les clés générées par le contrôleur AP8001XR sont conservées en mémoire volatile (RAM) avant d'être effacées à l'issue du processus de confirmation du badge présenté.

11- Annexe 1 : Recensement des données sensibles par équipements

ANNEXE 1

Matériel	Fonction	Donnée sensible	Type	Transmission	Chiffrement	Mémorisation	Protection
AP8001XR	Contrôleur, analyse des droits et conditions d'accès	ID personnel (ID desfire déchiffré)	Chaine de caractères HEXA - 4 octets	Provenance AP6003 canal TLS	TLS 1.1	RAM	Effacement sur autoprotection et sur perte d'alimentations
		PIN Code	Chaine de caractères 4 à 10 chiffres numériques	Provenance UTC canal TLS	TLS 1.1	RAM	Effacement sur autoprotection et sur perte d'alimentations
		PIN Code	Chaine de caractères 4 à 10 chiffres numériques	Provenance AP6003 canal TLS	AES 128	RAM	Clés auto générées (privée+publique) à chaque transaction de confirmation par code PIN
		Autorisations	données	Provenance UTC canal TLS	TLS 1.1	RAM	Effacement sur autoprotection et sur perte d'alimentations
		Accès SAM (JavaCard)	Clé	Station de configuration SAM	AES 128	JavaCard AP8001XR	Clés de mise à jour du SAM (JavaCard)
		Certificat 802.1X	Certificat PKI	TLS 1.1	RSA 2048 bits	JavaCard AP8001XR	SafeSign IC Applet + application blueX intégrés dans la JavaCard
		Certificat TLS (réseau transactionnel)	Certificat PKI	TLS 1.1	RSA 2048 bits	JavaCard AP8001XR	SafeSign IC Applet + application blueX intégrés dans la JavaCard
		Certificat TLS (réseau technique)	Certificat PKI	TLS 1.1	RSA 2048 bits	JavaCard AP8001XR	SafeSign IC Applet + application blueX intégrés dans la JavaCard
AP6003	Interface assurant la communication avec le(s) lecteur(s), la gestion de l'environnement des accès et pilotage du module SAM	Accès SAM (JavaCard)	clé	Station de configuration SAM	AES 128	JavaCard AP6003	Clés de mise à jour du SAM (JavaCard)
		Paramètres DESfire	Clé privée DESfire + algorithme de diversification	Initialisation USINE	AES128	JavaCard AP6003	SafeSign IC Applet + application blueX intégrés dans la JavaCard
		ID personnel (ID Desfire déchiffré)	Chaine de caractères HEXA - 4 octets	Provenance lecteur transparent, RS485 (protocole HDLC)	AES 128	JavaCard AP6003	Opération de calcule de la clé diversifiée pour le déchiffrement réalisé, par et dans l'espace mémoire de la JavaCard
		Certificat TLS (réseau technique)	Certificat PKI	TLS 1.1	RSA 3048 bits	JavaCard AP6003	SafeSign IC Applet + application blueX intégrés dans la JavaCard
Lecteur transparent	Acquisition et transmission des informations DESfire, sans traitement local, sur présentation d'un badge	PIN Code	Chaine de caractères 4 à 10 chiffres numériques	RS485 (protocole HDLC)	AES 128	RAM (le temps d'une transaction)	Génération de 2 clés AES (chiffrement & CMAC) à partir de la clé publique transmise par l'AB8001XR
		ID personnel (ID DESfire chiffré)	Paquets chiffrés	RF communication	AES 128	Pas de mémorisation locale	Chiffrement réalisé par la puce DESfire du badge à partir d'une clé diversifiée préalablement encodée.

12- Annexe 2 : lexique contrôle d'accès (métier)

Terme/Acronyme	Définition
Antenne	L'antenne est la partie visible du système de gestion d'accès. Elle permet le dialogue avec le badge (niveau radiofréquences) et envoie le signal électrique correspondant au lecteur, qui se trouve dans la zone protégée.
Lecteur	Le lecteur est l'élément du système de contrôle d'accès qui gère une antenne ou un point de badgeage. Il convertit le signal analogique de l'antenne et en extrait les indications de numéro de badge, code site etc., qu'il transfert au contrôleur par protocole.
Lecteur transparent	Pour l'emploi de certaine technologie d'identification, des informations spécifiques (clés privées) sont chargées dans les lecteurs pour communiquer avec les badges et récupérer un identifiant. Les lecteurs transparents ne disposent d'aucune information spécifique, elles sont contenues dans le contrôleur auquel est raccordé le lecteur.
Contrôleur	Le contrôleur est la partie intelligente de la gestion de l'accès (CPU). Il gère les lecteurs de badges qui lui sont connectés et les autorisations d'accès (périodes horaires, identifiants, accès) pour ces portes.
AP8001XR	AEOS Processing Unit : terme NEDAP générique pour désigner un contrôleur
UTC	Unité de Traitement Centralisée : Terme générique désignant un ordinateur ou un automate pilotant des équipements de terrain via un réseau de communication évolué
UTL	Unité de Traitement Locale : Terme générique de la profession « contrôle d'accès » pour désigner un contrôleur en dehors de toute spécificité constructeur
UCP	Unité de Contrôle de porte : Terme générique de la profession « contrôle d'accès » pour désigner les interfaces électroniques qui se positionnent entre les contrôleurs et les lecteurs de badge et qui assurent le raccordement des équipements techniques d'un environnement d'accès (Lecteur de badge, contact de porte, bouton poussoir de sortie, commande d'ouverture, etc)
Tête de lecture	La tête de lecture est l'élément qui communique avec les badges afin de récupérer un identifiant et le transférer vers un élément de gestion au travers

	d'un protocole standard (OMRON, WIEGAND, RS232 etc.)
Identifiant	Numéro de badge, numéro d'identification biométrique, code mental, plaque d'immatriculation, etc.
UID (DESFire)	Unique Identifier number. Identifiant unique (garantie constructeur) implémenté dans toutes les puces DESFire.
Badge	Carte d'identification physique répondant à la norme ISO 7810 (format carte de crédit 85.6x54x0.76mm) embarquant une technologie permettant la transmission d'un identifiant
Technologie d'identification	Moyen technique (informatique ou électronique) assurant pour un équipement unique la transmission d'un identifiant unique (chaîne de caractères)
SAM	Secure Access Module : Puce électronique (type SIM) intégrant des fonctions de sécurisation et de chiffrement des données traitées.
JavaCard	Puce électronique de type SAM conçue et fabriqué par la société Oracle
DESFire EV1	Technologie d'identification RFID sécurisée et programmable développée par NXP.
Diversification	Principe utilisé en cryptographie pour obtenir à partir d'une clé maître (devant impérativement restée secrète) une clé dérivée par application d'un algorithme.
Accès	Ouvrant/porte/Point de passage sécurisé qui assure le filtrage physique des personnes disposant d'un identifiant avec autorisations
Environnement de porte	Terme employé pour qualifier l'ensemble des équipements électroniques et mécaniques, mis en œuvre sur un accès pour en assurer la gestion/sécurisation (Lecteurs, serrure, contact de position, bouton de sortie libre, boîtier bris de glace évacuation, ferme porte, flexible passe câble, radars, etc…)
Composants embarqués	Terme NEDAP pour décrire les fonctions déployées dans les équipements de terrain pour assurer les automatismes locaux.
Autorisation	Droits programmés à une personne, qui lui permettent, au travers des différents identifiants qui lui sont affectés, de franchir les accès sécurisé par un système de contrôle d'accès
Evènement	Enregistrement horodaté d'une action/changement d'état, sans criticité, sur un système centralisé
Alarme	Enregistrement horodaté d'une action/changement d'état, avec une criticité identifié, sur un système centralisé
Unicité de passage	Moyen (électronique/physique) qui garantit le franchissement d'un accès par une seule personne à la fois.
Zone sécurisée/non sécurisée	Zone dont tous les accès périmétriques sont sécurisés par des contrôleurs et lecteurs limitant la

	présence aux seules personnes autorisées
Porteur/utilisateur	Par Utilisateur et porteur il est entendu toute personne à qui il a été confié des identifiants et des droits (badge(s) ; plaque d'immatriculation ; caractère biométrique ; code PIN, etc), afin de franchir des accès contrôlés.
Exploitant	Par Exploitant il est entendu toute personne disposant d'un droit d'exploitation sur les applications du système de gestion des accès : Administrateur, gestionnaire, opérateur, agent, hôtesse, mainteneur, etc.
Code PIN	(Personal Identifacation Number) code numérique individuel intervenant dans une procédure d'accès, en complément de la présentation d'un badge, pour confirmer le porteur/utilisateur.