Cible de sécurité Nedap AEOS 2021

Nedap France SAS
8-10 chemin d'Andrésy
BP 90050 – Eragny/Oise
95611 Cergy Pontoise Cedex

01 61 03 03 00
www.nedap.fr

Table des matières

1.Statut du document.

1. Version

Date	Rédacteur	Version	
19/05/2020	Ludwig FULGORI	v1.0	Version initiale
22/06/2021	Ludwig FULGORI	v1.1	Corrections suite retour ANSSI
13/07/2021	Ludwig FULGORI	v1.2	Version validée pour envoi à l'ANSSI
14/03/2022	Ludwig FULGORI	v1.3	Modifications suite aux retours de l'ANSSI
22/03/2022	Ludwig FULGORI	v1.4	Précisions sur les éléments incluent dans la TOE

2. Diffusion

Nom	Prénom	Société
FIGUEIREDO	Emmanuel	Nedap France SAS
FULGORI	Ludwig	Nedap France SAS
LY	Léonard	Nedap France SAS

2.Introduction

1. Identification de la cible de sécurité

Cette cible de sécurité a été élaborée en vue d'une qualification élémentaire.

2. Identification du produit

Catégorie	Identification, authentification et contrôle d'accès
Nom commercial du produit	Nedap AEOS
Version évaluée	2021.2
Editeur des logiciels	Nedap NV – Security Management
Type de produit	Solution assurant la reconnaissance et l'autorisation de passage, individuel, sur des accès physiques sécurisés

3.Description générale du produit

1. Présentation de la solution

AEOS est une solution complète de contrôle d'accès physique, constituée d'une application web et de matériel électronique (contrôleurs et lecteurs de badges). AEOS a pour principale fonctionnalité de contrôler les autorisations d'accès d'un porteur de carte RFID et de ne déclencher l'ouverture du passage que si la personne est dument autorisée à le faire.

AEOS propose une gamme complète de fonctionnalité pour s'adapter à toutes les configurations possibles en garantissant l'application de la politique de sureté de l'exploitant.

2. Liste des éléments constituant la solution

Le produit proposé est constitué des logiciels suivants :

- Un ou plusieurs serveurs de base de données. AEOS est compatible avec Microsoft Windows 2016, Microsoft SQL Server 2016 et supérieur, Oracle 18c et supérieur ou PostgreSQL 9.4 ou supérieur.
- Le ou les logiciels AEOS Application Server, dont le rôle consiste à gérer les besoins métiers (génération de l'interface Web, connexion avec la base de données, communication avec les équipements terrains, fonctionnel logiciel).
- Le ou les logiciels AEOS Lookup Server, dont le rôle consiste à générer un annuaire des éléments présents sur le système (serveurs d'applications, contrôleurs, poste clients, postes de paramétrages AEMon…)
- Le ou les logiciels de programmation des contrôleurs AEMon
- Le ou les postes clients légers d'exploitation AEOS
- Le ou les postes de programmation des SAM NXP AV2

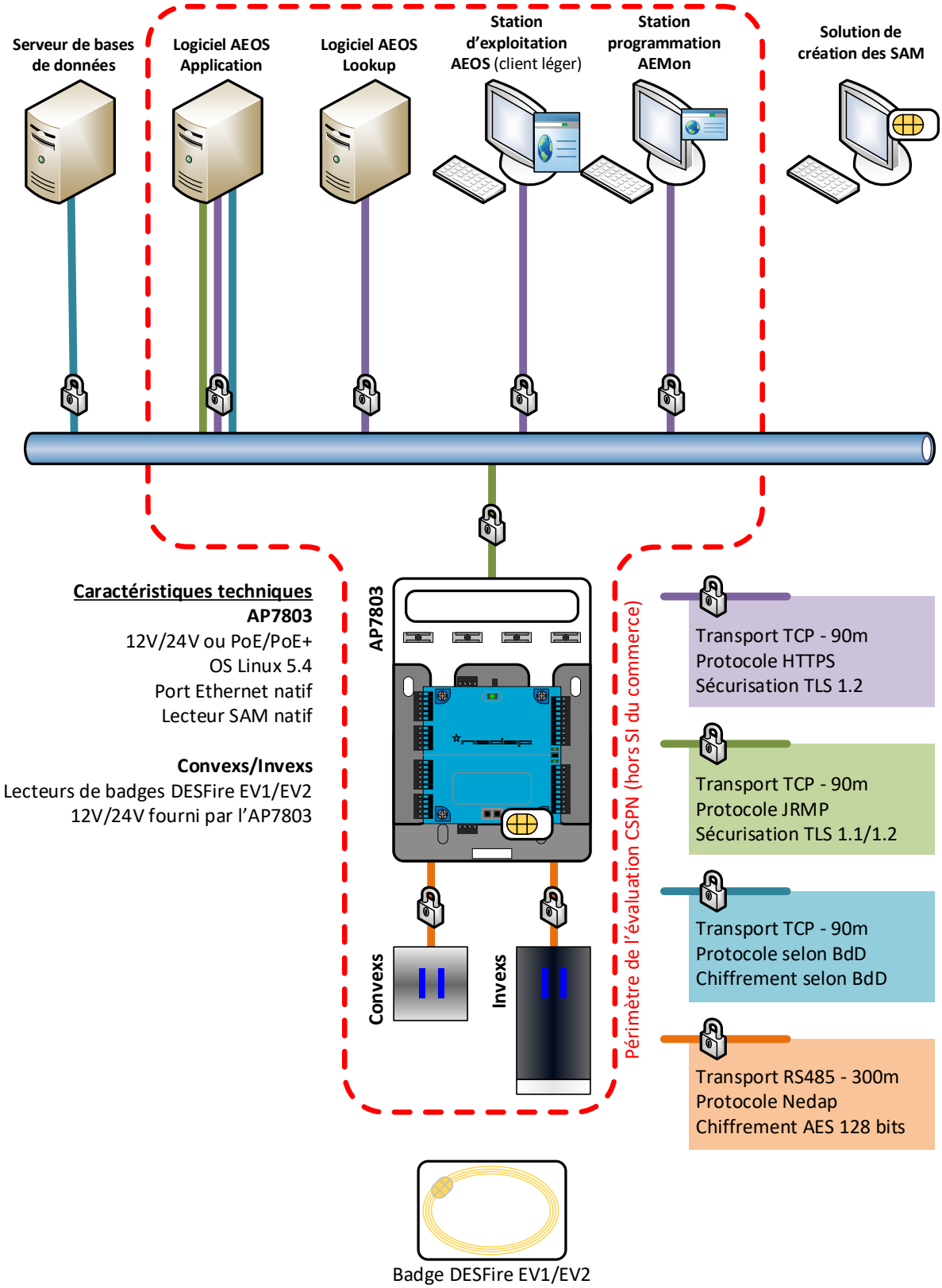
Ces différents éléments peuvent être installés sur un ou plusieurs serveurs/postes clients, selon les besoins et les règles métiers en vigueur.

Le produit est également constitué d'équipements matériels :

- Le ou les contrôleurs AP7803
- Le ou les lecteurs de badges Convexs et Invexs
- Les badges DESFire EV1 ou EV2
- Les SAM NXP AV2
- Les logiciels AEOS Application Server et AEOS Lookup Server, ainsi que la version OpenJDK fournie avec le logiciel.

La cible de sécurité porte sur les deux logiciels AEOS Application Server et AOES Lookup Server, le contrôleur AP7803 ainsi que les lecteurs Convexs et Invexs. Les autres éléments nommés ne font pas partie du périmètre de la cible de sécurité.

3. Schéma général d'architecture



4. Descriptif fonctionnel

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 sécurisée.

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, contrôleur d'accès et serveur d'application.

Ces équipements sont connectés sur un même réseau TCP/IP. L'ensemble des échanges entre les éléments Nedap constituant la solution sera chiffrée grâce à des certificats RSA 2048. Le réseau, les applications serveurs et les matériels informatiques ne font pas partis du périmètre de la cible de sécurité.

La solution est également constituée d'une solution de programmation des SAM NXP AV2, connectée ou non sur le réseau TCP/IP. Les SAM programmées seront ensuite insérés directement dans le lecteur intégré du module AP7803. La solution de programmation des SAM NXP AV2 ne fait pas partie du périmètre de la cible de sécurité.

5. Eléments constitutifs de la solution

1. Serveur applicatif AEOS

Le serveur applicatif AEOS assure la gestion globale de la solution de sécurisation des accès. Développé par NEDAP en Java, l'application AEOS est constituée d'un poste informatique sous environnement Microsoft Windows Server et emploie une base de données professionnelle (Microsoft SQL Server, Oracle ou MySQL)

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, les populations, les droits d'accès et les événements/alarmes horodatés dans une base de données.

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

Nom du fournisseur	Nom du produit	Spécifications
Microsoft	Windows Server	Version 2016 ou supérieure
Microsoft	SQL Server	Version 2016 ou supérieure
Oracle	Oracle Database	Version 18c ou supérieure
Logiciel libre	PostgreSQL	Version 9.4 ou supérieure
Logiciel libre	Open JDK	Version Azul Zulu 11.39.0.15 fournie avec le logiciel

Le déploiement des systèmes d'exploitation et des logiciels de bases de données devra se faire conformément aux recommandations de l'ANSSI. Le système d'information accueillant le système de contrôle d'accès sera cloisonné physiquement ou, à défaut, logiquement, conformément aux recommandations de l'ANSSI. Le cloisonnement physique empêche l'utilisation de certaines fonctionnalités de sécurité complémentaires du logiciel (authentification via LDAPS par exemple) ou complique légèrement certaines taches (déploiement des certificats directement depuis une autorité vers les contrôleurs) sans pour autant empêcher son utilisation nominale.

2. Poste d'exploitation du logiciel AEOS

Les postes clients permettent l'exploitation du logiciel AEOS. Il se connecte au serveur au travers d'une interface HTTPS.

3. SAM NXP AV2

Les SAM utilisés sont de type NXP AV2. Toute solution du commerce permettant de se connecter et de programmer des SAM NXP AV2 peut être utilisée. La SAM contiendra la clé DESFire qui sera utilisée pour la lecture du badge. La programmation de la SAM dépendra de l'utilisation ou non de clés diversifiées et sera détaillée dans une annexe.

Le module SAM est supposé fonctionner conformément aux spécifications du fabricant.

4. Contrôleur AP7803

Le contrôleur AP7803 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 de la connectique nécessaire à la connexion de deux lecteurs de badges et environnements de portes, permettant de gérer un ou deux accès simultanément, selon la configuration qui est faites.

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, le contrôleur est conçu pour assurer intégralement sa fonction sans dégrader le niveau de sécurité des accès contrôlés.

La perte du réseau 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 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. Une demande de présence est faite régulièrement pour s'assurer néanmoins du bon fonctionnement de l'équipement.

Par défaut, le contrôleur AP7803 ne dispose pas du firmware permettant le mode transparent, mais d'un firmware plus générique ainsi que d'un Kernel permettant son démarrage. Afin de pouvoir charger le firmware permettant le mode transparent, il faut s'assurer que le contrôleur AP7803 dispose à minima du Kernel v1.07

Après mise à jour, le contrôleur sera équipé d'un firmware spécifique au fonctionnement en mode transparent. Le Kernel sera également remplacé par un Kernel spécifique, intégré dans le Firmware permettant le mode transparent.

Dans ce mode de programmation, le contrôleur utilise un langage de script pour les échanges avec la carte DESFire. Le script sera fait pour que le module SAM soit utilisé. Les échanges ont lieu directement entre le module SAM NXP AV2 et la carte DESFire EV1 ou EV2. Le résultat des échanges, à savoir le numéro encodé dans le badge, est retourné au contrôleur pour traitement des autorisations.

Contrôleur AP7803	Version Kernel (avant mise à jour)	2.06
	Version Firmware	1.12

Les contrôleurs sont équipés de contact d'autoprotection optique, s'activant lorsque l'on ouvre le boitier, ains que de la connectique nécessaire pour le raccordement d'un mécanisme d'autoprotection externe. Les contacts d'autoprotection devront être programmés pour générer une alarme.

Lecteur de badges Convexs ou Invexs

Les lecteurs de badges sont les modèles Convexs et Invexs de la gamme NEDAP AEOS. Le qualificatif « transparent » signifie que le lecteur ne dispose d'aucune clé DESFire privée dans sa mémoire locale, les clés privées sont sécurisées dans un SAM hardware implanté dans le contrôleur AP7803, qui les sollicite lors des procédures d'autorisation d'accès.

On distingue trois 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 en option (lettre « K » dans la nomenclature) un clavier numérique pour confirmer les porteurs de badge par code PIN (badge + code personnel).
- Les lecteurs de type Invexs qui permettent l'initialisation d'échange de données avec les badges DESFire qui leur sont présentés (RFID) et propose en option (lettre « K » dans la nomenclature) un clavier numérique pour confirmer les porteurs de badge par code PIN (badge + code personnel) ainsi qu'un écran (lettre « S » dans la nomenclature).

Par défaut, les lecteurs Convexs et Invexs ne disposent pas du firmware permettant le mode transparent, mais d'un firmware plus générique ainsi que d'un Kernel permettant leur démarrage. Afin de pouvoir charger le firmware permettant le mode transparent, il faut s'assurer que les lecteurs Convexs dispose à minima du Kernel v2.06 et les lecteurs Invexs du Kernel v2.06 également.

Après mise à jour, le contrôleur sera équipé d'un firmware spécifique au fonctionnement en mode transparent. Le Kernel sera également remplacé par un Kernel spécifique, intégré dans le Firmware permettant le mode transparent.

Le lecteur sera équipé d'un firmware spécifique au fonctionnement en mode transparent. Dans ce mode de programmation, le lecteur ne dispose d'aucune information liée à la sécurité du badge.

Lecteur Convexs MD80	Version Kernel (avant mise à jour)	2.06
	Version Firmware	2.11
Lecteur Invexs MD170 ou MDK170	Version Kernel (avant mise à jour)	2.06
	Version Firmware	2.09
Lecteur Invexs MDKS170	Version Kernel (avant mise à jour)	2.06
	Version Firmware	2.09
Lecteur Invexs MD190 ou MDK190	Version Kernel (avant mise à jour)	2.06
	Version Firmware	2.09

Les lecteurs Convexs sont équipés de contact d'autoprotection optique, s'activant lorsque l'on ouvre le boitier ou lorsque l'on le désolidarise de son support. De par la nature du lecteur de badges Convexs (lecteur transparent sans code PIN), l'ouverture du lecteur ne génère aucun risque particulier

Les lecteurs Invexs sont équipés d'un contact d'autoprotection de type accéléromètre, s'activant lorsque l'on ouvre le boitier ou lorsque l'on le désolidarise de son support.

Les contacts d'autoprotection devront être programmés pour générer une alarme. De même, une alarme devra être programmée dans le logiciel en cas de déconnexion du lecteur du bus RS485 sur lequel il est connecté.

5. Badges DESFire EV1 ou EV2

Les identifiants RFID utilisés seront les badges DESFire EV1 ou EV2 de la société NXP. L'utilisation du numéro de série de la puce sera proscrite même si elle reste techniquement possible. Les badges seront encodés par un outil tiers. Toutes les fonctionnalités de la cartes DESFire (numéro de série aléatoire, clés diversifiées, choix de l'application, du fichier et de la clé, …) sont supportées par la solution Nedap. Dans le cadre de la diversification, les algorithmes supportés seront ceux de la carte SAM NXP AV2. D'autres algorithmes pourront être implémentées en utilisant le langage de script fournit en annexe.

La puce DESFire EV1 est certifié Critères Communs EAL4+

La puce DESFire EV2 est certifié Critères Communs EAL5

6. Configuration

La configuration se fait par script chargé dans le logiciel embarqué dans le contrôleur. Le script défini l'authentification sur la SAM, les échanges entre le module SAM et la carte DESFire, ainsi que le retour du numéro traité vers le contrôleur.

Le langage de script et des exemples sont détaillés dans le document « aeos_transparent_reader_scripting_icm_v6_en.pdf » fournit en annexe.

Dans ce script, il faut spécifier les informations de connexions à la SAM (numéro et version de KeyEntry et clé d'authentification). La clé d'authentification devra être chiffré via le certificat présent dans la mémoire du contrôleur, selon la procédure décrite dans le document fournit en annexe.

Le tableau suivant synthétise la configuration présentée en évaluation.

Composant du système		**Inclus dans la cible de l'évaluation** (TOE)	**Non évalué** (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
GAC	**Système d'exploitation**		Microsoft Windows 2016/2019 Server	
	Applicatifs	Nedap AEOS 2021 : AEOS Application Server et AEOS Lookup Server		
	Fonctions cryptographiques	OpenJDK Azul Zulu 11.39.0.15		
	Bases de données et annuaires		Microsoft SQL Server 2016/2017/2019	
UTL	**Système d'exploitation**	Linux 5.4.15		
	Applicatifs	Nedap AEOS 2021		
	Fonctions cryptographiques	mbedTLS 2.26		
	SAM		SAM NXP AV2	
Lecteurs	**Lecteurs simples**	Nedap Convexs - MD80C - MD80G - MD80FC - MD80FG Nedap Invexs - MD170 - MD190		
	Lecteurs avec clavier à codes	Nedap Invexs - MD170K - MD190K		
Badges			NXP DESFire EV1/EV2 avec clés fixes ou clés dérivées	

4.Description de l'environnement d'utilisation du produit

1. Utilisation usuelle

A l'heure actuelle dans les opérations de contrôle des accès, mettant en œuvre des badges RFID de technologie NXP DESFire EV1 ou EV2 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 :

- Communication avec le contrôleur par utilisation de protocoles standards non chiffrés (volonté des clients de disposer d'une liaison non-propriétaire pour faciliter tout changement de produit/fournisseur, au détriment de la sécurité)
- Information sensible (clés privées) enregistrées dans le lecteur

Ce mode de fonctionnement correspond à celui décrit dans le document de l'ANSSI intitulé « Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf » au chapitre « 4.3.3 Architecture n°3, déconseillée ». Le matériel Nedap proposé dans cette cible peut être configuré dans ce mode de fonctionnement, en utilisant les firmware adaptés, mais ce mode est exclu de la présente cible de sécurité.

Le matériel Nedap peut également être configuré dans le mode de fonctionnement décrit au chapitre « 4.3.2 Architecture n°2, acceptable » du même document, par changement de firmware et configuration, mais ce mode est également exclu de la présente cible de sécurité.

2. Utilisation cible du produit NEDAP AEOS

La solution NEDAP met en œuvre différentes fonctions afin de pallier 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.

Ce mode de fonctionnement correspond à celui décrit dans le document de l'ANSSI intitulé « Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf » au chapitre « Architecture n°1, hautement recommandée ». Le matériel Nedap proposé dans cette cible peut être configuré dans ce mode de fonctionnement, en utilisant les firmware adaptés et configurations adaptées.

Conscient du risque engendré par le déport des clés de chiffrement dans l'UTL plutôt que dans le lecteur, Nedap a fait le choix de recourir à un module SAM NXP AV2 amovible, programmable depuis toute application compatible, indépendamment de Nedap ou de ses partenaires, afin que l'utilisateur final reste maitre de la gestion de ses clés. Le module SAM à deux utilités :

- Stocker la ou les clés de lecture DESFire EV1 ou EV2 de l'utilisateur dans un espace mémoire sécurisé
- Gérer l'authentification avec la carte DESFire EV1 ou EV2 directement, le contrôleur ne servant que de relai pour le dialogue. Le module SAM gère l'utilisation de clés symétriques fixes ou diversifiées selon les algorithmes qu'il implémente, et retourne au contrôleur l'information lue dans la carte DESFire EV1 ou EV2.

Dans ce mode de fonctionnement, le contrôleur n'est pas partie prenante dans l'échange entre le module SAM et la carte DESFire EV1ou EV2. Le contrôleur comme le lecteur peuvent ainsi être qualifié de « transparent ».

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 ou EV2 et l'encodage consiste en la création d'une « application » dédiée au contrôle d'accès, dont l'AID est connu du contrôleur, et qui comporte un fichier de données et dont l'accès est protégé par une clé dite de lecture de 128 bits, conformément aux spécifications techniques de la carte DESFire EV1 ou EV2.

1. Utilisation d'une clé non diversifiée, sans code PIN

Un badge DESFire EV1 ou EV2 valide est présenté par son détenteur devant un lecteur Convexs. Le contrôleur contient un script qui cherche si le ou les numéros AID d'applications attendus sont présents dans la carte. Si tel est le cas, le contrôleur va mettre en relation le badge DESFire EV1 ou EV2 et la carte SAM NXP AV2, qui vont s'authentifier mutuellement grâce à l'algorithme AES128, puis le badge va transmettre au module SAM les données attendues, données qui seront ensuite retransmise au contrôleur.

Le contrôleur AP7803 traite le numéro ainsi reçu et contrôle les droits d'accès de la carte par rapport aux données qu'il stocke dans sa base de données embarquée. Si toutes les conditions d'accès sont réunies (droits d'accès, plage horaire, plage journalière, conditions spéciales), alors le contrôleur AP7803 génère un ordre de passage qui se matérialise par le pilotage d'un relais de la carte électronique, qui actionne l'ouverture de l'accès protégé. En parallèle, le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de passage.

Si le badge présenté n'est pas autorisé à passer, l'accès reste verrouiller et le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de tentative d'accès non autorisé.

1. Utilisation d'une clé non diversifiée, avec code PIN

Un badge DESFire EV1 ou EV2 valide est présenté par son détenteur devant un lecteur Convexs. Le contrôleur contient un script qui cherche si le ou les numéros AID d'applications attendus sont présents dans la carte. Si tel est le cas, le contrôleur va mettre en relation le badge DESFire EV1 ou EV2 et la carte SAM NXP AV2, qui vont s'authentifier mutuellement grâce à l'algorithme AES128, puis le badge va transmettre au module SAM les données attendues, données qui seront ensuite retransmise au contrôleur.

Le contrôleur AP7803 traite le numéro ainsi reçu et contrôle les droits d'accès de la carte par rapport aux données qu'il stocke dans sa base de données embarquée. Si toutes les conditions d'accès sont réunies (droits d'accès, plage horaire, plage journalière, conditions spéciales), alors le contrôleur AP7803 active le clavier à code intégré au lecteur, pour que le porteur du badge puisse saisir son code personnel. Si le code personnel saisi correspond à celui attendu, le contrôleur génère un ordre de passage qui se matérialise par le pilotage d'un relais de la carte électronique, qui actionne l'ouverture de l'accès protégé. En parallèle, le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de passage.

Si le badge présenté n'est pas autorisé à passer, ou si le code saisi ne correspond pas à celui attendu après le nombre d'essais autorisé, l'accès reste verrouiller et le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de tentative d'accès non autorisé.

A noter que la longueur du code, le nombre d'essais avant refus ou une liste de code interdits peuvent être paramétré dans l'application AEOS.

De plus, un mécanisme de code dit « sous contrainte » est implémenté et peut être activé. Dans ce mode de fonctionnement, une erreur volontaire de saisie par la personne qui se présente devant l'accès, comme par exemple une erreur sur le dernier chiffre, est une information de tentative de fraude du système par un tiers qui force une personne autorisée à lui ouvrir un accès. Le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de passage doublé d'un second évènement de tentative d'accès sous contrainte.

2. Utilisation d'une clé diversifiée, sans code PIN

Un badge DESFire EV1 ou EV2 valide est présenté par son détenteur devant un lecteur Convexs. Le contrôleur contient un script qui cherche si le ou les numéros AID d'applications attendus sont présents dans la carte. Si tel est le cas, le contrôleur va mettre en relation le badge DESFire EV1 ou EV2 et la carte SAM NXP AV2. Le module SAM va alors calculer la clé diversifiée en fonction de l'algorithme choisi, de la clé mère stockée et de divers éléments de diversification (numéro de série de la carte, numéro de l'application…) en fonction de l'algorithme retenu. Dès lors, la carte DESFire EV1 ou EV2 et le module SAM NXP AV2 vont s'authentifier mutuellement grâce à l'algorithme AES128, puis le badge va transmettre au module SAM les données attendues, données qui seront ensuite retransmise au contrôleur.

Le contrôleur AP7803 traite le numéro ainsi reçu et contrôle les droits d'accès de la carte par rapport aux données qu'il stocke dans sa base de données embarquée. Si toutes les conditions d'accès sont réunies (droits d'accès, plage horaire, plage journalière, conditions spéciales), alors le contrôleur AP7803 génère un ordre de passage qui se matérialise par le pilotage d'un relais de la carte électronique, qui actionne l'ouverture de l'accès protégé. En parallèle, le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de passage.

Si le badge présenté n'est pas autorisé à passer, l'accès reste verrouiller et le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de tentative d'accès non autorisé.

3. Utilisation d'une clé non diversifiée, avec code PIN

Un badge DESFire EV1 ou EV2 valide est présenté par son détenteur devant un lecteur Convexs. Le contrôleur contient un script qui cherche si le ou les numéros AID d'applications attendus sont présents dans la carte. Si tel est le cas, le contrôleur va mettre en relation le badge DESFire EV1 ou EV2 et la carte SAM NXP AV2. Le module SAM va alors calculer la clé diversifiée en fonction de l'algorithme choisi, de la clé mère stockée et de divers éléments de diversification (numéro de série de la carte, numéro de l'application…) en fonction de l'algorithme retenu. Dès lors, la carte DESFire EV1 ou EV2 et le module SAM NXP AV2 vont s'authentifier mutuellement grâce à l'algorithme AES128, puis le badge va transmettre au module SAM les données attendues, données qui seront ensuite retransmise au contrôleur.

Le contrôleur AP7803 traite le numéro ainsi reçu et contrôle les droits d'accès de la carte par rapport aux données qu'il stocke dans sa base de données embarquée. Si toutes les conditions d'accès sont réunies (droits d'accès, plage horaire, plage journalière, conditions spéciales), alors le contrôleur AP7803 active le clavier à code intégré au lecteur, pour que le porteur du badge puisse saisir son code personnel. Si le code personnel saisi correspond à celui attendu, le contrôleur génère un ordre de passage qui se matérialise par le pilotage d'un relais de la carte électronique, qui actionne l'ouverture de l'accès protégé. En parallèle, le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de passage.

Si le badge présenté n'est pas autorisé à passer, ou si le code saisi ne correspond pas à celui attendu après le nombre d'essais autorisé, l'accès reste verrouiller et le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de tentative d'accès non autorisé.

A noter que la longueur du code, le nombre d'essais avant refus ou une liste de code interdits peuvent être paramétré dans l'application AEOS.

De plus, un mécanisme de code dit « sous contrainte » est implémenté et peut être activé. Dans ce mode de fonctionnement, une erreur volontaire de saisie par la personne qui se présente devant l'accès, comme par exemple une erreur sur le dernier chiffre, est une information de tentative de fraude du système par un tiers qui force une personne autorisée à lui ouvrir un accès. Le contrôleur AP7803 génère et transfert au serveur un évènement horodaté de passage doublé d'un second évènement de tentative d'accès sous contrainte.

4. Hypothèse sur l'environnement du produit

1. Installation des serveurs

Pour l'évaluation, il est supposé que le serveur d'application AEOS est installé dans un local informatique sécurisé dont l'accès est strictement limité aux personnels habilités. Il est également supposé que le serveur soit déployé avec toutes les mises à jour possibles, est maintenu à jour et respecte les bonnes pratiques de sécurité informatique.

Pour l'évaluation, il est également supposé que l'application tierce de création des SAM soit soit isolée de tout accès réseau, soit connecté à un réseau de manière sécurisée, afin d'empêcher toute connexion qui entrainerait une possible divulgation des secrets à inscrire dans le module SAM.

Le bon fonctionnement du module SAM est également supposé vrai par hypothèse

2. Installation des équipements techniques AP7803

Pour l'évaluation, il est supposé que les contrôleurs AP7803 sont installés dans un local technique sécurisé dont l'accès est strictement limité aux personnels habilités.

3. Installation des lecteurs

Pour l'évaluation, il est supposé que les lecteurs soient déployés afin de garantir une gestion périmétrique hermétique et concentrique :

- 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 ou 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.

4. Installation des accès

Pour l'évaluation, les accès protégés disposeront à minima d'un mécanisme de verrouillage de l'accès et d'un mécanisme de surveillance de l'état de la porte (ouverte ou fermée). Le câblage de l'ensemble des équipements constituant les environnements de porte est direct, point à point, du côté protégé de l'accès.

5. Description des utilisateurs typiques

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 incombent.

Ils disposent tous, d'un compte de connexion à l'application Nedap AEOS, individuel, basé sur nom d'utilisateur et un 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.

6. Description du périmètre de l'évaluation

Les porteurs de badge sont les utilisateurs finaux de la solution. Ils disposent de badges sans contact (RFID) DESFire EV1 ou EV2 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.

5. Hypothèses sur l'environnement technique du produit

1. Serveur NEDAP AEOS

Le serveur répond aux caractéristiques techniques préconisées par Nedap. Il dispose d'un logiciel de protection contre les virus et ne permet pas l'exécution de code malveillant. Il dispose également d'un pare feu paramétré pour ne laisser passer que le trafic strictement nécessaire. Toutes les mises à jour de sécurité disponibles sont installées. Seule le JDK fourni avec AEOS doit rester dans la version d'installation.

Il dispose d'un compte administrateur, doté de tous les privilèges de configuration et exploitation, et d'un compte exploitant, doté de privilèges restreints, et réservé à l'utilisation courante du système.

A l'installation, l'application Nedap AEOS utilise des certificats auto signés qui seront utilisés pour la communication entre les différents éléments logiciels et matériels de la solution. Ces certificats devront être remplacés par des certificats propres à l'environnement de l'utilisateur.

Plus généralement, il suit les recommandations de l'ANSSI pour le déploiement d'un système informatique dans un environnement numérique.

Le serveur est cloisonné et considéré comme faisant partie structurellement de la zone névralgique de l'infrastructure technique de l'utilisateur. Il n'expose pas vers d'autres réseaux d'interfaces permettant son utilisation ou un vecteur d'attaque.

2. Architecture réseau

L'architecture réseau déployée pour connecter le serveur d'applications AEOS et les contrôleurs AP7803 doit être sécurisée pour prévenir de tout risque d'intrusion. L'accès aux équipements constituant la solution de contrôle d'accès doit être réservée uniquement aux postes et équipement en ayant un besoin impératif. Le réseau sera réputé cloisonner des autres systèmes d'informations de l'entreprise, logiquement ou physiquement. Dans tous les cas, le système ne sera pas connecté directement à Internet.

3. Contrôleur AP7803

Un compte utilisateur usine est configuré par défaut dans tous les contrôleurs AP7803. Ce compte devra être désactivé et un ou plusieurs nouveaux comptes utilisateur devront être créés et maintenus secret. Ces comptes s'adressent à l'intégrateur ainsi qu'au mainteneur, mandaté par le client final.

Lors de sa fabrication, un certificat auto signé qui sera utilisé pour la communication avec le serveur de la solution est installé dans le contrôleur. Ce certificat devra être remplacé par un certificat propre à l'environnement de l'utilisateur.

Avant installation, le contrôleur devra être intégralement réinitialiser conformément aux préconisations de Nedap afin de s'assurer que le contrôleur ne soit pas préchargé de données potentiellement dangereuses. Le contrôleur sera ensuite mis à jour avec la version cible du logiciel dont on aura au préalable vérifier l'intégrité.

4. Certificats électroniques

La solution Nedap AEOS fait usage de certificats numériques pour garantir l'intégrité des messages échangés entre les différents éléments qui la compose. Par défaut, des certificats auto signés, identiques sur tous les systèmes, sont utilisés. Ces certificats devront être tous remplacés par des certificats propres à l'environnement de l'utilisateur. Les noms d'alias des certificats sont cependant imposés par la solution.

ca : autorité de certification signant la clé aeosinternal.

aeosinternal : certificat utilisé pour les échanges entre les différents éléments constituant la solution, à savoir le serveur d'application, le serveur lookup, le logiciel de paramétrage AEmon et les contrôleurs AP7803. Chaque élément possède la clé privée et la clé publique, afin de pouvoir chiffrer les éléments qu'il transfère et déchiffrer les éléments qu'il reçoit.

vault : certificat utilisé sur le serveur pour chiffrer le mot de passe de la connexion à la base de données ainsi que le mot de passe du keystore contenant le certificat web.

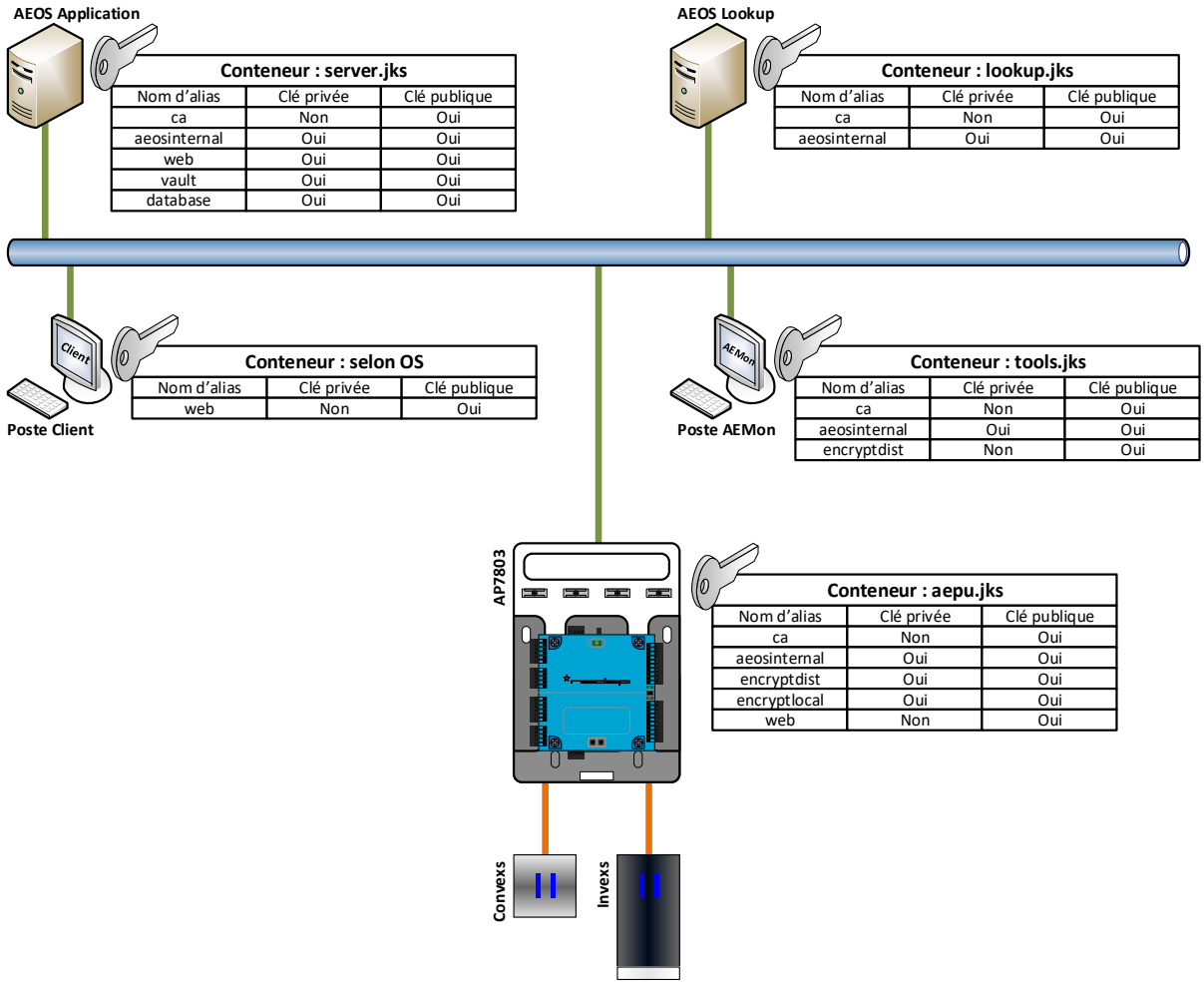
web : certificat utilisé pour le client web qui se connecte au serveur d'application, ainsi que au client web qui se connecte aux contrôleurs AP7803 pour des opérations de monitoring.

encryptdist : certificat utilisé pour le chiffrement de la clé AES de la SAM dans les scripts utilisés pour la lecture des badges DESFire.

encryptlocal : certificat utilisé pour le chiffrement de données dans le contrôleur.

database (optionnel) : certificat utilisé pour chiffrer les échanges entre le serveur et la base de données.

Les clés sont stockées dans des conteneurs différents, selon les applications, selon le schéma ci-après.



Chacun de ces certificats est généré selon un mécanisme propre au client. Il peut s'agir de certificats autosignés ou au contraire de certificat généré depuis une autorité de certification propre au client. La durée de vie des certificats est également librement paramétrable.

5. Badges technologie DESFire EV1 ou EV2

Les badges doivent être encodés, selon le processus propre à la carte DESFire, indépendamment de Nedap.

Un identifiant unique doit être encodé dans une application, et les informations nécessaires à la lecture de cet identifiant doivent être transmis à Nedap (AID de l'application, numéro de la clé de lecture, numéro de l'application, méthode d'encodage du numéro unique…).

Seule exception, la clé de lecture ne sera pas transmise à Nedap, mais inscrite dans un module SAM NXP AV2 en respectant le bon paramétrage de celle-ci. L'accès à ce module est protégé par une clé AES 128 qui devra être transmise à Nedap. Cette clé ne permet pas de retrouver la clé stockée.

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 transit 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 le contrôleur AP7803 et les badges DESFire EV1 ou EV2.

La configuration du lecteur est, dans tous les cas, supposée avoir été déployée en activant la fonctionnalité empêchant les attaques de type « attaque relais ».

Les lecteurs disposant d'un clavier à code sont également supposés déployés avec l'activation d'une alarme lors de l'ouverture du lecteur.

6. Description des utilisateurs typiques

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

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.

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.

Les agents techniques sont réputés de confiance.

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

3. Porteurs de badge

Les porteurs de badge sont les utilisateurs finaux de la solution. Ils disposent de badges sans contact (RFID) DESFire EV1 ou EV2 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.

5. Description de l'environnement technique de fonctionnement

1. Description du périmètre de l'évaluation

La cible prévoie l'évaluation des équipements suivants :

- Les lecteurs de badges Convexs MD80C, MD80G, MD80FC et MD80FG
  - La dernière lettre correspond à la couleur du lecteur, G pour Gray, C pour Charcoal.
  - La présence de la lettre F (pour Flush) indique qu'il s'agit d'un lecteur encastré tandis que son absence indique qu'il s'agit d'un lecteur à poser en applique.
  - Seule la forme et la couleur du boitier changent, les lecteurs étant strictement identique d'un point de vue électronique et logiciel.
- Les lecteurs de badges Invexs MD170B, MD170W, MDK170B, MDK170W, MDKS170B et MDKS170W
  - La dernière lettre correspond à la couleur du lecteur, B pour Black, W pour White
  - La présence de la lettre K (pour Keyboard) dans la dénomination indique la présence d'un clavier à codes sur le lecteur.
  - Seule la couleur du boitier et la présence d'un clavier à codes changent, les lecteurs étant strictement identique d'un point de vue électronique et logiciel.
- Les lecteurs de badges MD190 et MDK190
  - La présence de la lettre K (pour Keyboard) dans la dénomination indique la présence d'un clavier à codes sur le lecteur.
  - Seule la présence d'un clavier à codes change, les lecteurs étant strictement identique d'un point de vue électronique et logiciel.
- Le contrôleur AP7803

2. Dispositifs d'accès

L'environnement de l'accès disposera à minima des équipements suivants :

- 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)

3. Postes Informatiques

Le serveur informatique sera installé sous Windows 2016 Server, les derniers correctifs de Windows à date du test seront déployés. Le serveur disposera également de SQL Server 2016, avec les derniers correctifs à date déployés. Le logiciel AEOS sera installé sur ce serveur. La version du JDK fournie avec AEOS ne devra pas être modifiée.

Le poste client sera installé sous Windows 10, les derniers correctifs à date du test seront déployés. Une machine virtuelle Java à jour sera installée sur le poste client. Les tests seront faits à partir du navigateur Internet Explorer 11. Le poste client disposera également d'une solution de gestion des SAM NXP AV2, au travers du logiciel SAM Manager, de la société Islog.

4. Badges

Un premier jeu de badges DESFire sera encodé avec une clé fixe pour toutes les cartes et les informations nécessaires à leur lecture seront paramétrées dans la configuration de test.

Un second jeu de badges DESFire sera encodé avec une clé diversifiée pour toutes les cartes et les informations nécessaires à leur lecture seront paramétrées dans la configuration de test.

5. SAM

Un module SAM AV2 de la société NXP (référence P5DF081) contiendra une première clé commune à tous les badges pour le premier jeu de badges sans diversification, et une seconde clé mère nécessaire à la diversification du second jeu de badges avec diversification.

6.Description des menaces

1. Données sensibles protégées par la solution

BIENS ET DONNEES SENSIBLES	INTEGRITE	CONFIDENTIALITE	DISPONIBILITE
Les clés DESFire	Oui	Oui	Non
Les certificats intervenants dans les échanges chiffrés TLS	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

Les clés DESFire sont stockés dans le module SAM inséré dans le lecteur. Après authentification sur le module, le contrôleur AP7803 ordonne au SAM de dialoguer avec le badge DESFire selon les modalités définies dans un script. La clé d'authentification sur le SAM est inscrite de manière chiffrée dans le script. Le module SAM assure nativement la protection en intégrité des clés stockées.

Les certificats intervenants dans les échanges TLS sont stockés dans le système de fichier du contrôleur, dans un conteneur de type Java Cryptography Extension Key Store (jks). Le conteneur s'appelle aepu.jks et se trouve dans le répertoire « /var/opt/aeos/certs »

Les identifiants individuels des utilisateurs, les droits/autorisations d'accès des utilisateurs et les codes PIN des utilisateurs de badges sont stockés dans le système de fichier du contrôleur, dans de multiples fichiers se trouvant dans le répertoire « /var/opt/aeos » et ses sous répertoires. Les codes PIN sont chiffrés via un algorithme 3DES et une clé unique générée par chaque contrôleur. Cette clé est ensuite elle-même stockée dans un conteneur chiffré en RSA, en s'appuyant sur le certificat « encrytplocal » stockée dans le conteneur JCEKS du contrôleur. La clé RSA devra avoir été paramétrée avec une longueur d'au moins 2048 bits.

Le contrôleur est protégé par des mesures organisationnelles (installation dans des locaux protégés) ainsi que par une méthode d'authentification (nom d'utilisateur et mot de passe) propre à son système d'exploitation

2. Intrusion sur le réseau TCP/IP

Un attaquant est connecté sur le réseau Ethernet TCP/IP et déploie des moyens d'écoute dans le but d'identifier des données sensibles sur le contrôleur AP7803 ou d'effectuer des attaques par rejeu de transaction/commandes.

ECOUTE DES TRANSACTIONS ECHANGEES ENTRE LE SERVEUR ET LES CONTROLEURS AP7803	
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 ECHANGEES ENTRE LE SERVEUR ET LES CONTROLEURS AP7803	
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

3. Intrusion sur la connexion RS485

Un attaquant, situé en zone non protégée, est connecté la liaison RS485 entre le lecteur de badge et le contrôleur AP7803 pour obtenir des données sensibles de l'AP7803.

ECOUTE DES TRANSACTIONS ECHANGEES ENTRE LE CONTROLEUR AP7803 ET LE LECTEUR DE BADGES	
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 l'identifiant d'un porteur de badge	Rejeu d'une transaction (adaptée) pour usurper l'identité d'un autre utilisateur
Toute transaction contenant le code PIN d'un porteur de badge	Interception du PIN code associé à un badge (usurpation d'identité d'accès)
Toute transaction contenant le code PIN d'un porteur de badge	Rejeu d'une transaction (adaptée) pour usurper l'identité d'un autre utilisateur
Transaction d'initialisation	Rejeu d'une transaction (adaptée) pour usurper l'identité du lecteur de badges

7.Surface d'attaque

Localisation de l'attaquant		Attaques matérielles	Attaques logiques
Sur site	Zone névralgique		Attaque via les fonctions de gestion du système ou via la connexion au réseau d'entreprise
	Zone protégée	Attaque matérielle des UTL	Attaque au réseau de gestion des accès
	Zone publique	Attaque matérielle des badges ou lecteurs	Attaque du réseau de gestion des accès
Hors site		Attaque matérielle de tout composant du système avant ou après installation	Attaque via Internet

1. Attaques depuis la zone névralgique

Le système de contrôle d'accès est réputé cloisonné des autres systèmes d'informations, réduisant d'autant la surface d'attaque via le réseau d'entreprise. Sur ce réseau, le système de contrôle d'accès Nedap AEOS peut néanmoins exposer différents services, parmi lesquels l'interface graphique du logiciel, selon les ouvertures souhaitées en termes d'exploitation. En tout état de cause, les interfaces possibles seront les mêmes que celles pouvant être exposées sur le réseau de gestion des accès.

2. Attaque depuis la zone protégée

1. Attaque matérielle

La matériel AP7803 dispose d'un port JTAG pouvant être un vecteur d'attaque. Ce port n'est pas accessible lorsque le contrôleur est installé dans son environnement nominal de fonctionnement et l'accès à ce port nécessite l'ouverture complète du boitier. En pratique, l'accès à ce port devra déclencher une alarme d'autoprotection, soit en utilisant le capteur optique prévu à cet effet sur la carte, soit en utilisant un capteur d'ouverture complémentaire et recommandé.

Le contrôleur dispose également de deux ports RS485 utilisés pour la communication avec les lecteurs. Dans l'hypothèse ou l'un des deux ports seraient disponibles, il deviendrait également un vecteur d'attaque, avec en théorie la possibilité d'envoyer au contrôleur des commandes non prévues via ce connecteur. En pratique, les ports séries sont vus coté Linux comme des périphériques USB, avec un driver adéquat pour les piloter, et ne permettent donc pas de s'authentifier sur le shell du contrôleur.

Le contrôleur dispose d'un connecteur RJ45, raccordé au réseau TCP/IP. Toute tentative d'attaque via ce port nécessite de déconnecter la carte du réseau et génèrera une alarme coté serveur grâce à un polling régulier.

Un tiers peut également envisager de voler/remplacer le module SAM amovible présent dans le contrôleur afin soit de tenter d'en extraire le secret, soit de le remplacer par un autre dont il connait les clés pour ensuite autoriser des badges non accrédités légitimement. Le retrait du module SAM génère une alarme en temps réel. Dans l'hypothèse ou l'action est faite contrôle déconnecté du réseau, l'alarme est stockée jusqu'à la prochaine reconnexion, mais une alarme de déconnexion du contrôleur est déjà remontée. Le vol du module SAM pour en extraire les données est couvert par le fait que, à l'heure actuelle, la sécurité du module n'a jamais été mise à mal. Le remplacement du module nécessite un accès logique au contrôleur afin de paramétrer les clés d'authentification sur le module SAM.

2. Attaque logicielle.

Le contrôleur, le serveur d'application AEOS et le serveur Lookup disposent tous de certificats signés par la même autorité, afin de chiffrer l'ensemble des échanges entre ces ensembles. Il ne sera donc pas possible pour un contrôleur non pourvu du certificat adéquat de se connecter au reste de la solution.

L'attaque directe sur le contrôleur nécessite de disposer un compte autorisé pour l'authentification sur le contrôleur, la robustesse de la solution dépend dès lors de l'utilisation de comptes robuste sur le contrôleur.

L'attaque sur le logicielle peut se faire soit via l'interface de gestion du matériel, soit via l'interface web de l'utilisateur. Dans le premier des cas, comme précédemment pour le matériel, l'ensemble des échanges sont authentifiés et chiffrés via un certificat dont la possession est nécessaire pour envisager toute action.

Dans le cas de l'interface web, l'authentification est basée sur un jeton applicatif, avec des informations de comptes stockées en base de données. S'authentifier sur l'application est un préalable nécessaire à toutes les actions sur le logiciel.

3. Zone publique

1. Attaque matérielle.

Seuls les lecteurs de badges sont accessibles en zone publique. Le lecteur n'entrant pas en ligne de compte dans le chiffrement des échanges entre le badge et le module SAM, il n'est pas un vecteur d'attaque direct du système. Le lecteur devra être paramétré néanmoins pour empêcher toute tentative d'attaque relais.

Tous les lecteurs disposent d'un certificat utilisé pour le chiffrement et codé en dur dans le firmware. Ce firmware est lui-même stocké de manière chiffrée, avec une clé propre au lecteur, généré au démarrage, et copier dans la RAM du lecteur durant la phase opérationnelle. Toute tentative de vol du lecteur entrainera l'effacement de la mémoire et par conséquent une difficulté accrue pour déchiffrer le firmware et donc le certificat. Ce firmware sert aux échanges entre le lecteur et le contrôleur (canal de communication pour les mises à jour à distance, pour la gestion des LED ou du buzzer, de l'autoprotection…) ainsi que pour le chiffrement du code PIN lorsque le lecteur est équipé d'un clavier.

2. Attaque logicielle

En zone publique, il n'y a pas de connexion disponible pour une attaque logique qui soit directement accessible. Le seul risque vient d'une éventuelle connexion sur le bus RS485 du lecteur - ce qui entrainerait une alarme immédiatement. Ce lien permet d'accéder à la connexion RS485 du contrôleur qui, comme on l'a vu précédemment, ne permet pas de rebondir sur le shell du contrôleur.

4. Hors site

1. Attaque matérielle.

Tout contrôleur neuf devra être intégralement réinitialisé avant installation pour éviter le risque d'intrusion liée à la présence de données frauduleuse dans le contrôleur neuf. Le contrôleur sera ensuite mis à jour vers la version cible, qui inclut la dernière mise à jour du système d'exploitation embarqué et des librairies afférentes, avant d'être connecté au réseau du système de gestion des accès.

En cas de défaillance du matériel, la procédure de réinitialisation devra être exécutée avant tout renvoi pour réparation. Cette procédure devra être effectuée en dehors du réseau de gestion des accès. Si la défaillance du matériel ne permet plus d'effectuer la procédure de restauration, la destruction du matériel devra être envisagé. Il faudra également veiller à retirer le module SAM du contrôleur et à le stocker de manière sécurisée.

2. Attaque logicielle

Le système n'étant pas connecté directement à Internet, le risque d'attaque directe vers le système n'est pas possible sans rebond par un équipement ou un système tiers. Dans ce cas, et en plus des mesures structurelles propres à la solution, la sécurité de l'ensemble repose également sur l'ensemble des autres équipements constitutifs du réseau, dont nous ne pouvons au préalable pas prévoir les faiblesses.

8.Mécanismes de sécurité

1. Protection en transmission de l'identifiant personnel

Les identifiants personnels des porteurs de badge, encodés dans les badges DESFire, utilisés dans la solution, sont protégés en confidentialité lors de leur transmission par un chiffrement en AES 128bits. La clé peut être soit identique dans tous les badges, soit diversifiée, selon le choix fait par l'utilisateur.

2. Protection en transmission du code PIN

Les codes PIN sont protégés en confidentialité et contre les tentatives de rejeu par la mise en œuvre du protocole de chiffrement TLS 1.2 avec clé RSA de 2048bits, stockée dans un certificat installé en usine, non modifiable.

3. Protection des données échangées entre serveur AEOS et contrôleur AP7803

Les commandes et transactions échangées entre le serveur AEOS et le contrôleur AP7803 sont protégées en confidentialité et contre les tentatives de rejeu par la mise en œuvre du protocole de chiffrement TLS 1.2 avec clé RSA de 2048bits, stockée dans un certificat au format JKS des deux côtés.

4. Protection de la clé de lecture DESFire

La clé de lecture DESFire est stockée dans le module SAM NXP AV2 et est sécurisée par le fonctionnement propre de ce module.

5. Protection physique du lecteur

Dans le cadre de l'utilisation des lecteurs Nedap, seule la gamme de lecteurs Invexs disposant d'un « K » dans sa nomenclature se doit d'être protégée efficacement contre les tentatives d'ouvertures, car un mécanisme de chiffrement est intégré au lecteur pour la gestion des codes PIN.

Pour les lecteurs de la gamme Convexs ainsi que pour les lecteurs de la gamme Invexs ne disposant pas de clavier à codes, le besoin en protection physique n'existe pas puisque l'ouverture du lecteur ne permet en aucun cas d'accéder à des données, le numéro de badges transitant de manière chiffrée dans le lecteur, et le lecteur ne prenant pas part au chiffrement.

La gamme des lecteurs Convexs est équipée d'un capteur optique d'ouverture, fournissant une alarme en cas d'ouverture. Le paramétrage de ce capteur reste facultatif, n'apportant aucune plus-value dans la chaine de sécurité.

La gamme des lecteurs Invexs est équipée d'un capteur de type accéléromètre, fournissant une alarme en cas d'ouverture. Le paramétrage de ce capteur est impératif dans le cadre de l'utilisation de codes PIN, sinon il reste facultatif.

6. Protection logique du lecteur

L'interface de communication du lecteur, sur support RS485, dispose d'un mécanisme d'alarme en cas de déconnexion du matériel.

9.Informations complémentaires

1. Mise à jour du logiciel AEOS

La version du logiciel AEOS est indiquée par un numéro de version à 2 ou 3 indices. Les mises à jour portent aussi bien sur le logiciel serveur, sur les logiciels de paramétrages que sur les logiciels embarqués dans le matériel.

Nedap propose de manière annuelle une mise à jour majeure de l'application. Cette mise à jour est indiquée par une évolution des deux premiers ou uniquement du second chiffre de l'indice. Une version majeure apporte principalement de nouvelles fonctionnalités au logiciel comme au matériel.

Plusieurs fois par ans, une version mineure peut être proposée. L'évolution est indiquée par un changement du troisième indice du numéro de version, et les apports portent principalement sur des évolutions de fonctionnalités existantes.

Enfin, Nedap propose régulièrement des mises à jour portant sur un point précis, principalement à des fins de corrections. Le dernier indice du numéro de version augmente.

Dans une installation fonctionnelle, matériel et logiciel doivent avoir à minima les deux premiers indices de version identique, sous peine de non-fonctionnement. Le dernier indice du numéro de version correspond au dernier patch déployé. Selon si le patch a un impact ou pas sur le matériel, par rapport à la version précédente, il est nécessaire ou non de le déployé sur le matériel en même temps que sur le logiciel.

1. Exemple de numérotation des indices

La version présentée dans cette cible de sécurité est la version 2021.2. Il s'agit, comme son nom l'indique, d'une version sortie en 2021 (premier indice) et cette version est la seconde de l'année (deuxième indice).

Si des versions correctives devaient sortir pour cette version majeure, un troisième indice serait ajouté, correspondant au numéro de correctif (2021.2.1, 2021.2.2, …)

La prochaine version majeure portera le numéro 2021.3, la suivant 2021.4, et ainsi de suite. Toutes les versions majeures qui sortiront en 2022 verront le premier indice passé à 2022, et ainsi de suite pour les années suivantes.