Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2015/02

NEDAP AEOS

Version 3.0.4

Paris, le 10 avril 2015

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

Guillaume POUPARD

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2015/02**
Nom du produit **NEDAP AEOS**
Référence/version du produit **Version 3.0.4**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Commanditaire **Nedap France S.A.S** **8/10 chemin d'Andrésy** **90050 Eragny sur Oise** **France**
Centre d'évaluation **OPPIDA** **4-6 avenue du Vieil Etang - Bât B** **78180 Montigny Le Bretonneux** **France**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le système de contrôle d'accès physique « NEDAP AEOS, version 3.0.4 ». Le produit permet à des utilisateurs disposant de badges sans contact, en technologie RFID (*Radio Frequency Identification*) d'accéder à une zone sécurisée. Pour cela, 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 AEOS repose sur les équipements suivants : badge, lecteur de badge, module d'interface, contrôleur d'accès, serveur applicatif de gestion des accès AEOS, serveur de certificats, serveur RADIUS (*Remote Authentication Dial-In User Service*), station d'exploitation AEOS et station de programmation des SAM (*Secure Access Module*).
Ces équipements sont situés sur deux réseaux cloisonnés au moyen d'un pare-feu embarqué dans le contrôleur d'accès.
Les serveurs (d'applications AEOS, de certificats et d'authentification), les stations d'exploitation et les stations de programmation des SAM sont situés sur le réseau Ethernet TCP/IP dit « transactionnel ». Le réseau transactionnel, établi et administré par le client final, est installé dans une zone sécurisée dont l'accès est strictement limité aux personnes habilitées ; par conséquent, ce réseau est hors du périmètre de l'évaluation.
Les lecteurs de badges, les modules d'interface et le contrôleur d'accès sont situés sur le réseau TCP/IP dit « technique ».
Le contrôleur d'accès (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 une porte pilotée par le contrôleur.
Le module d'interface (AP6003) a pour fonction de gérer la communication avec 1 ou 2 lecteurs de badges. 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), le statut des équipements supervisés.
Les lecteurs de badge ne disposent d'aucune clé privée dans la mémoire locale, les clés privées sont sécurisées dans un SAM implanté dans le contrôleur AP8001XR. On distingue 2 types de lecteurs employés dans la solution :

- les lecteurs de type *Convexs* qui permettent l'initialisation d'échanges de données avec les badges DESFire qui leur sont présentés (RFID) ;
- les lecteurs de type *Invexs* qui permettent l'initialisation d'échanges de données avec les badges DESFire qui leur sont présentés (RFID) et proposent un clavier numérique pour vérifier que les porteurs de badge disposent du code PIN (*Personal Identification Number*) associé au badge.

Le schéma ci-dessous résume l'architecture de la solution décrite précédemment.

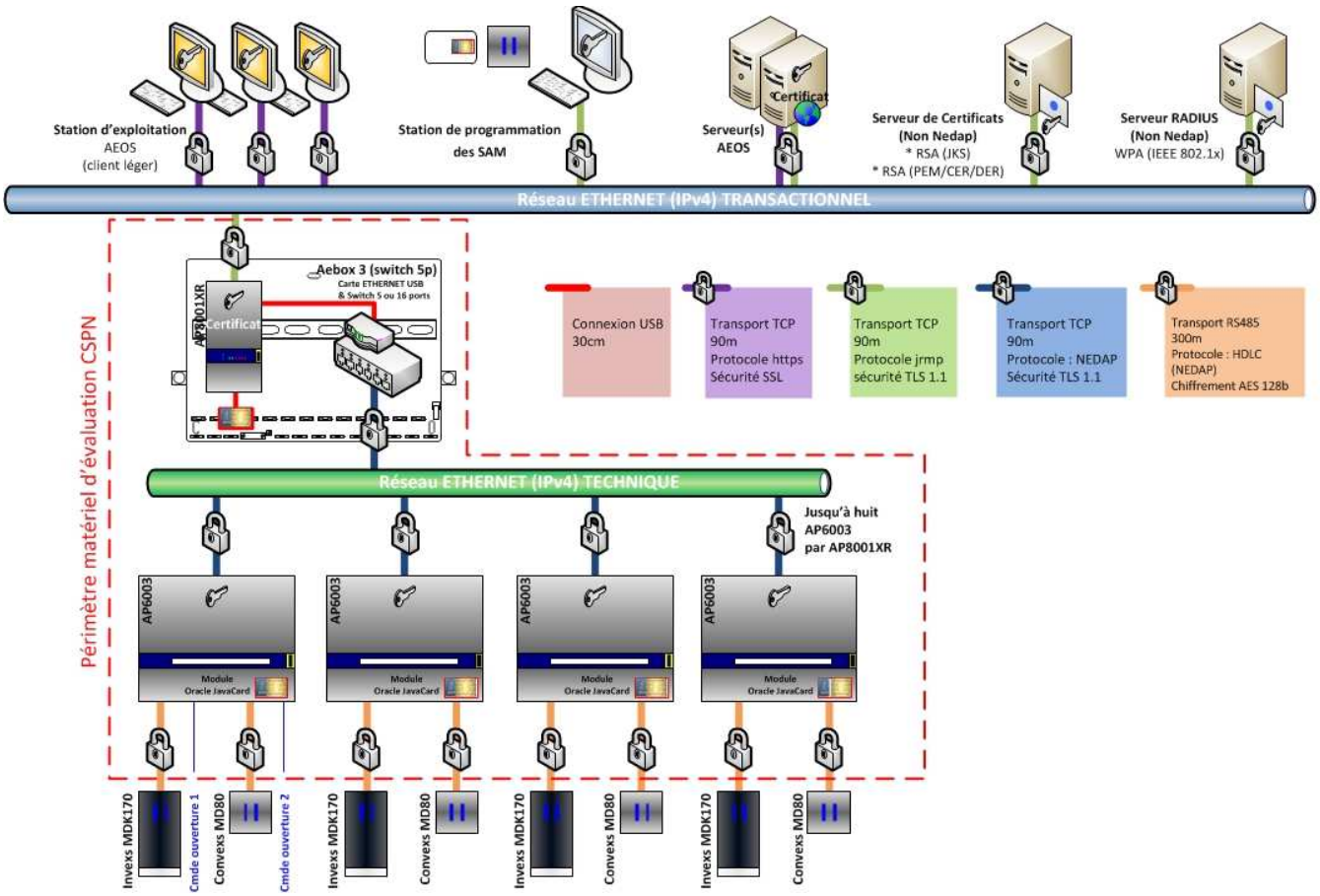

Figure 1 - Schéma de l'architecture de la solution NEDAP AEOS

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☒ **6 - identification, authentification et contrôle d'accès**
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ 99- Autres

1.2.2. Identification du produit

Les numéros de version des *firmware* installés sont identifiables grâce au logiciel AECONF via le serveur applicatif AEOS. La procédure d'utilisation d'AECONF est décrite dans [GUIDES].

1.2.3. Services de sécurité

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :

- la protection en confidentialité de l'identifiant personnel ;
- la protection en confidentialité du code PIN ;
- la protection en confidentialité et contre le rejeu des données échangées entre le serveur applicatif AEOS et le contrôleur AP8001XR ;
- la protection en confidentialité et contre le rejeu des données échangées entre le contrôleur AP8001XR et l'interface AP6003;
- le filtrage des flux réseaux entre les réseaux technique et transactionnel au travers de l'utilisation d'un pare-feu embarqué dans le contrôleur AP8001XR.

1.2.4. Configuration évaluée

Dans le cadre de l'évaluation et comme indiqué dans la cible de sécurité [CDS], le produit a été livré en version 3.04 sous la forme de machine virtuelle hébergeant l'ensemble des applications du réseau transactionnel, avec les équipements AP8001XR, AP6001 un lecteur de badge *Convexs*, un lecteur de badge *Invexs* et un badge DESFire EV1.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue par la procédure CSPN.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 4.1 « Description générale du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 6 « Données sensibles »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 7 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 8 « Description des fonctions de sécurité »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 4.5 « Description des utilisateurs typiques »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

La plateforme de test correspond à la configuration évaluée détaillée au paragraphe 1.2.4. Le produit nécessite une base de données au choix. Dans le cadre de l'évaluation le choix de la base de données s'est porté sur une base MS SQL Server.

2.3.2.2. Particularités de paramétrage de l'environnement

Le produit a été livré préconfiguré.

2.3.2.3. Options d'installation retenues pour le produit

Les options d'installation retenues sont celles fournies par le développeur.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

Sans objet.

2.3.2.5. Durée de l'installation

Sans objet.

2.3.2.6. Notes et remarques diverses

L'installation du produit et sa configuration initiale sont bien documentées.

2.3.3. Analyse de la documentation

Dans son ensemble, la documentation est claire et compréhensible, permettant ainsi une prise en main rapide du produit évalué.

2.3.4. Revue du code source (facultative)

Le code semble clairement écrit et respecter les bonnes pratiques de programmation.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Protection en confidentialité de l'identifiant personnel	**Réussite**
Protection en confidentialité du code PIN	**Réussite**
Protection des données échangées entre serveur AEOS et contrôleur AP8001XR	**Réussite**
Protection des données échangées entre contrôleur AP8001XR et interface AP6003	**Réussite**
Filtrage des flux réseaux entre le réseau technique et transactionnel au travers de l'utilisation d'un pare-feu embarqué dans le contrôleur AP8001XR	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Sans objet.

2.3.8. Avis d'expert sur le produit

Le fonctionnement du produit est conforme à ses spécifications fonctionnelles.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Les fonctions listées au 2.3.5 ont été évaluées.

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Le produit dans sa version évaluée offre des mécanismes globalement robustes et à l'état de l'art.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Il n'a pas été identifié de vulnérabilités sur ce produit particulier.

2.3.11. Accès aux développeurs

Sans objet.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

L'utilisation et l'administration du produit doivent se faire par des utilisateurs formés et de confiance conformément à ce qui est décrit dans le guide utilisateur. Par ailleurs les utilisateurs devront s'assurer que les mécanismes cryptographiques mis en œuvre sur le réseau technique sont conformes aux recommandations de l'ANSSI [REF-CRY]. En particulier, l'utilisation du protocole TLSv1.1 ou TLSv1.2 doit être privilégié. De plus, il convient de créer des utilisateurs non privilégiés sur le contrôleur AP8001XR afin de donner des privilèges minimaux au travers de règles *sudoers*.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste de référence des mécanismes cryptographiques est celle fournie par la cible de sécurité [CDS]. La résistance de ces mécanismes a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [RTE] et concluent que, si les recommandations présentes dans [GUIDES] sont appliquées, les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de l'ANSSI (voir [REF-CRY]).

2.5. Analyse du générateur d'aléas

Les moyens mis en œuvre pour la génération et le retraitement des nombres aléatoires utilisés par la solution NEDAP AEOS permettent d'atteindre le niveau de résistances aux attaques visé par la CSPN.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « NEDAP AEOS**,** version 3.0.4 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN - NEDAP lecteur transparent - R11.pdf* Version : *R11* ; Date : *26 février 2013.*
[RTE]	*Rapport Technique d'Evaluation CSPN NEDAP* Référence : *OPPIDA/CESTI/CSPN_NEDAP/RTE/2.1*; Version : 2.1 ; Date : *05 mars 2015.*
[GUIDES]	Guide d'installation : AEMON AECONF_UserMan_E.pdf AEOS_InstallMan_Advanced_E.pdf AEOS_InstallMan_E.pdf AEOS_LiquibaseTool_E.pdf AEOS_WebService_E.pdf

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur http://www.ssi.gouv.fr/
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur http://www.ssi.gouv.fr/