PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2022/05

Nedap AEOS

Version 2021.2

Paris, le 8 avril 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]

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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2022/05**
Nom du produit **Nedap AEOS**
Référence/version du produit **Version 2021.2**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **NEDAP FRANCE SAS** 8 chemin d'Andrésy 95610 Eragny sur Oise
Développeur **NEDAP NV** Parallel Weg 2 7141DC Groenlo Pays Bas
Centre d'évaluation **OPPIDA** 6 avenue du Vieil Etang Bâtiment B 78180 Montigny le Bretonneux
Fonctions de sécurité évaluées Protection de la transmission de l'identifiant personnel Protection de la transmission du code PIN Protection des échanges entre serveur AEOS et contrôleur AP7803 Protection de l'accès à la clé de lecture DESFire Protection physique des lecteurs claviers Emission d'une alarme en cas de déconnexion du matériel.
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit évalué 6
1.2.1 Catégorie du produit 7
1.2.2 Identification du produit 7
1.2.3 Fonctions de sécurité 8
1.2.4 Configuration évaluée 8
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Travaux d'évaluation 9
2.2.1 Installation du produit 9
2.2.2 Analyse de la documentation 9
2.2.3 Revue du code source (facultative) 9
2.2.4 Analyse de la conformité des fonctions de sécurité 9
2.2.5 Analyse de la résistance des mécanismes des fonctions de sécurité 9
2.2.6 Analyse des vulnérabilités (conception, construction, etc.) 10
2.2.7 Analyse de la facilité d'emploi 10
2.3 Analyse de la résistance des mécanismes cryptographiques 10
2.4 Analyse du générateur d'aléa 10
3 La certification 11
3.1 Conclusion 11
3.2 Recommandations et restrictions d'usage 11
ANNEXE A. Références documentaires du produit évalué 12
ANNEXE B. Références liées à la certification 13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Nedap AEOS, Version 2021.2 » développé par NEDAP NV.

Ce produit est une solution 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 dûment autorisée à le faire.

Le tableau ci-dessous synthétise le périmètre de l'évaluation :

Composant du système		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE) et supposé de confiance
GAC	Système d'exploitation		Microsoft Windows 2016/2019 Server
	Applicatifs	**Nedap AEOS 2021.2 : AEOS Application Server et AOES Lookup Server**	
	Fonctions cryptographiques	**OpenJDK Azul Zulu 11.39.0.15.**	
	Bases de données et annuaires		Microsoft SQL Server 2016/2017/2019
UTL : contrôleurs AP7803m	Système d'exploitation	**Linux 5.4.15**	
	Applicatifs	**Nedap AEOS 2021.2**	
	Fonctions cryptographiques	**MbedTLS 2.26**	
	SAM		SAM NXP AV2
Lecteurs	Lecteurs simples	**Nedap Convexs MD80C, MD80G, MD80FC, MD80FG** **Nedap Invexs : MD170B, MD170W, MD190**	
	Lecteurs-clavier	**Nedap Invexs : MDK170B, MDK170W, MDKS170B, MDKS170W, MDK190**	
Badges			NXP DESFire EV1/EV2 avec clés fixes ou clés dérivées

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*

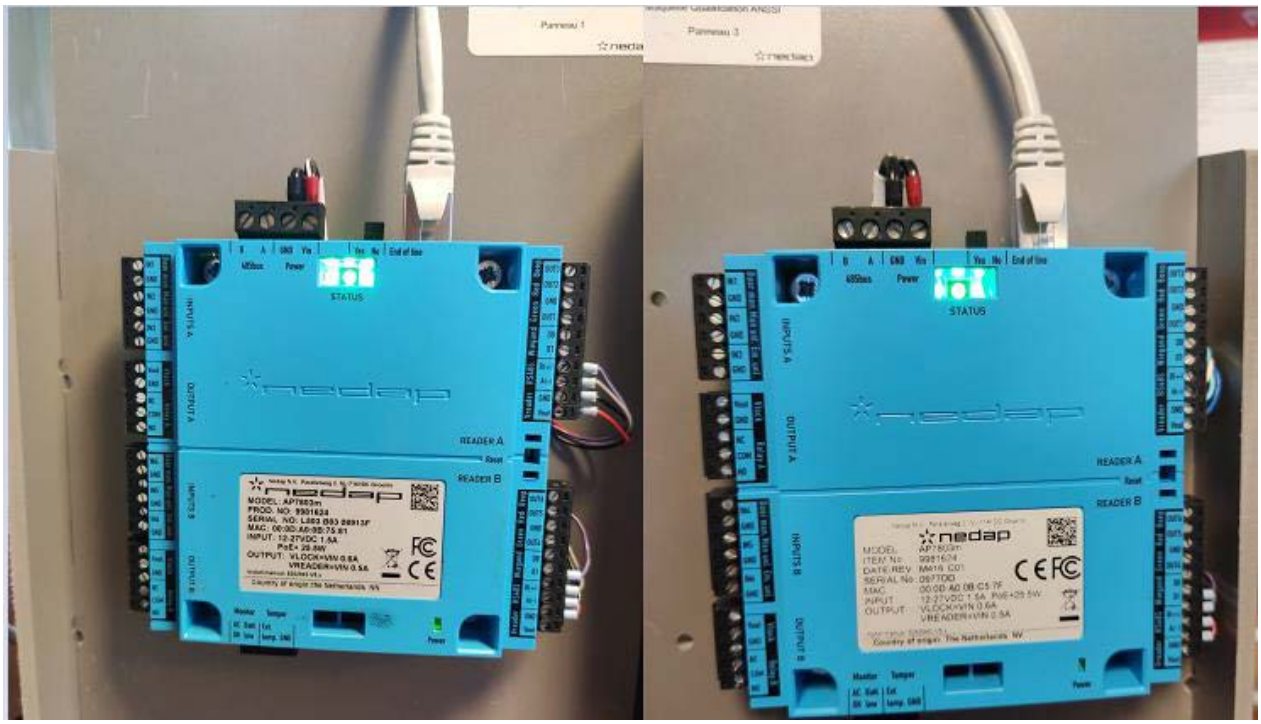
☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☒	**6**	**identification, authentification et contrôle d'accès**
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	Nedap AEOS
Numéro de la version évaluée	Version 2021.2

La version certifiée du produit est la version 2021.2, et peut être identifiée dans le menu « Informations » de l'interface *web* d'administration :

Les contrôleurs de modèle AP7803m, ainsi que les différents modèles de lecteurs, sont identifiables par la mention MODEL appliquée sur le boîtier :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la protection de la transmission de l'identifiant personnel ;
- la protection de la transmission du code PIN ;
- la protection des échanges entre serveur AEOS et contrôleur AP7803 ;
- la protection de l'accès à la clé de lecture DESFire ;
- la protection physique des lecteurs claviers ;
- l'émission d'une alarme en cas de déconnexion du matériel.

1.2.4 *Configuration évaluée*

La configuration évaluée est une maquette constituée de :

- deux contrôleurs AP7803 ;
- quatre lecteurs de badges (trois lecteurs Invexs et un lecteur Convexs) ;
- un poste d'administration hébergeant le logiciel d'administration ;
- un routeur KMETech (hors périmètre).

La fixation des lecteurs de badges sur la maquette est représentative de la situation en environnement de production. En effet, les lecteurs sont vissés directement sur leur support.

Les contrôleurs ne sont en revanche pas placés dans un coffret, comme cela serait le cas en production.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-07].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'évaluateur n'a pas procédé à l'installation du produit. Le commanditaire a fourni une maquette préinstallée et prête à l'emploi, et a procédé à la mise en route du produit aux côtés de l'évaluateur. En particulier, le commanditaire a procédé au paramétrage des protections.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES]dans le cadre de cette évaluation.

Les guides du produit permettent d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 2021.2 » 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 Recommandations et 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 spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- l'administrateur doit impérativement se conformer aux sections 6.3.1 à 6.3.4 du document [PARAM] décrivant les valeurs à utiliser de « *key usage*» des certificats électroniques ;
- l'administrateur doit impérativement configurer le compte privilégié disponible par défaut en se conformant à la section 10.3.1 du document [PARAM], afin de :
    - modifier le hash du mot de passe stocké en base en données ;
    - marquer le compte comme « verrouillé » dans la base de données ;
- l'administrateur doit impérativement se conformer à la section 10.2 du document [PARAM], afin de paramétrer un nombre maximal d'essais de connexion.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité Nedap AEOS 2021, version 1.4, 22 mars 2022.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation CSPN REMBRANDT – Nedap AEOS, référence OPPIDA/CESTI/REMBRANDT/RTE, version 2.2, 15 mars 2022.
[GUIDES]	Guides d'utilisation : - *AEOS Device Integration Protocol*, version 12, 7 juillet 2020 ; - *AEOS Advanced Installation*, version 2020.1, 13 mai 2020 ; - *AEOS transparent reader scripting*, version 5, 12 juillet 2019 ; - *AP 7x03(m) Installation sheet*, version 5, 22 juin 2016 ; - *Convexs 80 Installation sheet*, version 12, 8 novembre 2017 ; - *Invexs 170 Installation sheet*, version 12, 27 mai 2019 ; - *Invexs 190 Installation sheet*, version 8, 21 mars 2017 ; - [PARAM] AEOS End-2-End - Paramétrage de la solution ANSSI - AEOS 2021.2, version 6, 11 mars 2022.

ANNEXE B. Références liées 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 des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 3.0, 12 avril 2021. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-07]	Note d'application - Méthodologie pour l'évaluation de systèmes de contrôle d'accès physique en vue d'une CSPN, référence ANSSI-CSPN-NOTE-07, version 1.0, 7 juillet 2020.