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-2022/06

Winkeo FIDO2

Version 1.4.9

Paris, le 26 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-2022/06**
Nom du produit **Winkeo FIDO2**
Référence/version du produit **Version 1.4.9**
Catégorie de produit **Matériel et logiciel embarqué**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **NEOWAVE** 1480 avenue d'Arménie 13120 Gardanne, France
Développeur **NEOWAVE** 1480 avenue d'Arménie 13120 Gardanne, France
Centre d'évaluation **CEA - LETI** 17 avenue des martyrs 38054 Grenoble Cedex 9, France
Fonctions de sécurité évaluées Intégrité basée sur une signature AES Confidentialité basée sur un chiffrement AES Génération des clés symétriques Confidentialité de la mémoire flash Confidentialité de la mémoire RAM Confidentialité, intégrité et authenticité des nombres aléatoires générés Génération des clés asymétriques Résistance aux attaques physiques Intégrité et authenticité des processus FIDO (U2F et FIDO2) Vérification de la présence d'un utilisateur Suppression du *bootloader* du *secure element*
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Non

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

1.1 Présentation du produit

Le produit évalué est « Winkeo FIDO2, Version 1.4.9 » développé par NEOWAVE.

Ce produit est un *token* d'authentification électronique. Il se présente sous la forme d'une clé USB qui est conforme aux spécifications FIDO U2F et FIDO2. Le *token* est nommé « *authenticator* » dans le langage FIDO.

Ce produit existe en deux modèles :

- Winkeo FIDO2 : avec un connecteur USB de type A ;
- Winkeo-C FIDO2 : avec un connecteur USB de type C.

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.

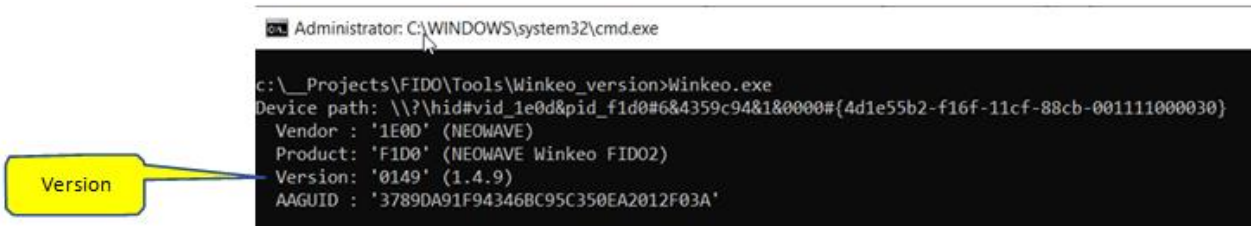
1.2.1 *Catégorie du produit*

☐	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	Winkeo FIDO2
Numéro de la version évaluée	Version 1.4.9

La version certifiée du produit peut être identifiée avec le logiciel fourni par le développeur sur demande. Cet exécutable indique la version « Version: '0149' (1.4.9) » comme illustré par la figure suivante :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'intégrité basée sur une signature AES ;
- la confidentialité basée sur un chiffrement AES ;
- la génération des clés symétriques de confiance ;
- la confidentialité de la mémoire *flash* ;
- la confidentialité de la mémoire RAM ;
- la confidentialité, intégrité et authenticité des nombres aléatoires générés ;
- la génération des clés asymétriques de confiance ;
- la résistance aux attaques physiques ;
- l'intégrité et authenticité des processus FIDO (U2F et FIDO2) ;
- la vérification de la présence d'un utilisateur ;
- la suppression du *bootloader* du *secure element*.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond au mode d'utilisation en tant que service d'authentification électronique forte pour :

- services en ligne équipés de serveurs FIDO ;
- émission de certificat grâce à une solution de serveur de signature ;
- fournisseur d'identité numérique.

Le mode de fonctionnement « hors-ligne » n'est pas évalué.

Les deux modèles de clé de sécurité Winkeo FIDO2 avec un connecteur USB type A et type C ont été évalués.

Le produit Winkeo FIDO2 est constitué :

- d'une partie physique (boitier, bouton, LED RGB et connecteur USB) ;
- d'une partie électronique (carte électronique reliant les éléments, dont le principal : le composant de sécurité MS6003 rev C, certifié Critères Communs sous la référence ANSSI-CC-2020/20) ;
- d'une partie logicielle (embarquée sur le composant de sécurité).

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

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

Le branchement de la clé de sécurité sur un port USB de l'ordinateur est suffisant pour utiliser le produit.

La gestion de la configuration (code PIN, remise à zéro en état de sortie d'usine) de la clé est possible en utilisant des services externes (système d'exploitation ou navigateur).

L'environnement mis en place pour l'évaluation est composé de :
- un ordinateur sous Windows 10, équipé de Chrome et Mozilla Firefox ;
- une station sous Linux.

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], [SPEC_CRY] et [WISEKEY] dans le cadre de cette évaluation.

Les guides du produit permettent d'installer et 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'intégralité du produit et a vérifié le respect des guides de sécurité du composant de sécurité MS6003 rev C [WISEKEY].

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

L'évaluateur a effectué une revue du code source et estime que :
- le code comporte de nombreux commentaires et est intelligible ;
- le code est modulaire : il est découpé en modules ayant leur fonctionnalité propre ;
- les constantes sont déclarées par des instructions de pré-traitement, et elles utilisent des valeurs spécifiques/complexes pour augmenter la sécurité du code.

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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

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

L'évaluateur n'a pas identifié de cas où la sécurité du produit évalué est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Les utilisateurs du produit peuvent être tout un chacun. Le produit est très simple d'utilisation, de type "branchez et utilisez", notamment sur le système d'exploitation Windows.

Le guide d'utilisation [GUIDES] note un usage un peu moins aisé sous Linux, certaines configurations nécessitent d'éditer un fichier pour ajouter une action liée aux produits de sécurité. Une fois cette règle ajoutée, le produit est aussi facile à utiliser que sous Windows.

2.2.7.3 Notes et remarques diverses

L'utilisation de la partie FIDO2 du produit conjointement avec le système *Azure Active Directory* de Windows 10 nécessite quelques réglages de la part de l'administration du Système d'Information. Il est à noter que cette utilisation "hors-ligne" du produit n'est pas couverte par la cible de sécurité [CDS].

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 [ANA_CRY].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

Les mécanismes cryptographiques du produit Winkeo FIDO2 s'appuient sur le composant de sécurité MS6003 rev C.

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.

L'utilisation du générateur physique du composant de sécurité MS6003 rev C respecte les recommandations détaillées dans les documents [WISEKEY].

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 « Winkeo FIDO2, Version 1.4.9 » 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].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de sécurité CSPN Winkeo FIDO2, version 1.5, 11 mars 2022.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN WINKEO FIDO2-2022, référence LETI.CESTI.WIN.RTE.001, version 2.1, 11 mars 2022 .
[ANA_CRY]	Analyse cryptographique : - Cotation des mécanismes cryptographiques WINKEO, référence LETI.CESTI.WIN.RTE.002, version 1.0, 27 avril 2021.
[GUIDES]	Guide d'utilisation du produit : - Winkeo FIDO2 Guide d'utilisation, version 1.2, 11 mars 2022. Guide d'administration du produit : - Winkeo FIDO2 Guide d'administration, version 1.1, 11 mars 2022.
[SPEC_CRY]	Spécifications cryptographiques : - NEOWAVE Winkeo FIDO2 - Security Design, version 1.0, 30 novembre 2020.
[WISEKEY]	Guides du composant de sécurité MS6003 rev C : - *Securing Tbx 06.04.01.xx on MS6xxx 90nm Products*, réference TPR712LX, rev. L, 10 mars 2020; - *Generating Random numbers on MS6xxx products (90nm)*, réference TPR709EX, rev. E, 06 mars 2020 ; - *Security recommendations for MS6xxx 90nm products*, référence TPR706DX, rev. D 10 mars 2020 ; - *Secure hardware AES on MSxxxx 90nm products*, reference TPR0708DX, rev. D 29 août 2017. Rapport technique pour la composition : - Evaluation Technical Report (ETR for composition) - SIROCCO-C, référence LETI.CESTI.SIR.COMPO.001, version 1.0, 16 mars 2020.

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 4.0, 3 mars 2022. 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, 26 janvier 2021.
[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.