



**PREMIÈRE
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-2023/13

Ledger Nano S Plus **Firmware SE 1.0.4**

Paris, le 21 Juillet 2023

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

Vincent STRUBEL

[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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2023/13
Nom du produit	Ledger Nano S Plus
Référence/version du produit	Firmware SE 1.0.4
Catégorie de produit	Matériel et logiciel embarqué
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	LEDGER 1 rue du Mail 75002 Paris
Développeur	LEDGER 1 rue du Mail 75002 Paris
Centre d'évaluation	EDSI 4 rue Alfred Kastler 1400 Caen, France
Fonctions de sécurité évaluées	Génération d'aléa Mécanisme d'attestation Vérification du PIN utilisateur Canal sécurisé pour l'installation et la mise à jour des <i>firmwares</i> et d'applications
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.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	6
1.2.1	Catégorie du produit.....	6
1.2.2	Identification du produit.....	7
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée.....	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation.....	8
2.2	Travaux d'évaluation.....	8
2.2.1	Installation du produit.....	8
2.2.2	Analyse de la documentation.....	8
2.2.3	Revue du code source (facultative).....	8
2.2.4	Analyse de la conformité des fonctions de sécurité.....	8
2.2.5	Analyse de la résistance des mécanismes des fonctions de sécurité.....	8
2.2.6	Analyse des vulnérabilités (conception, construction, etc.).....	9
2.2.7	Analyse de la facilité d'emploi.....	9
2.3	Analyse de la résistance des mécanismes cryptographiques.....	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification.....	10
3.1	Conclusion.....	10
3.2	Recommandations et restrictions d'usage.....	10
ANNEXE A.	Références documentaires du produit évalué.....	11
ANNEXE B.	Références liées à la certification.....	12

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Ledger Nano S Plus, Firmware SE 1.0.4 » développé par LEDGER.

Le Nano S Plus de LEDGER est un *Personal Security Device* (PSD) dont le but est de stocker de façon sécurisée des secrets cryptographiques et de fournir des primitives cryptographiques. Le produit peut être utilisé comme portemonnaie électronique, comme second facteur d'authentification, ou encore comme coffre à mot de passes. Les ajouts de fonctionnalités se font au travers d'applications, que l'utilisateur installe sur le produit depuis un magasin applicatif, qui s'appuient sur les primitives cryptographiques offertes par le produit.

Le produit est composé de deux microcontrôleurs :

- Un microcontrôleur générique, appelé *Microcontroller Unit* (MCU), en charge de gérer les communications USB avec l'hôte et d'assurer le relai avec le microcontrôleur sécurisé ;
- un microcontrôleur sécurisé, appelé *Secure Element* (SE), en charge d'exécuter le système d'exploitation BOLOS et les applications embarquées, et de réaliser les opérations cryptographiques.

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

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

1.2.2 Identification du produit

Produit	
Nom du produit	Ledger Nano S Plus
Référence du SE	ST33K1M5C
Version du <i>firmware</i> du SE	Firmware SE 1.0.4
Nom du <i>firmware</i> du SE	BOLOS
Référence du MCU	STM32F042K6
Nom du <i>firmware</i> du MCU	SEPROXYHAL
Identifiant du produit	0x33 10 00 04

La version certifiée du produit peut être identifiée en suivant les procédures décrites au chapitre 3.5 de la [CDS].

Le manuel utilisateur, voir [GUIDES], détaille également les étapes permettant de vérifier l'authenticité du produit.

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la génération d'aléa ;
- le mécanisme d'attestation ;
- la vérification du PIN utilisateur ;
- l'utilisation d'un canal sécurisé pour l'installation et la mise à jour des *firmwares* et d'applications.

1.2.4 Configuration évaluée

La configuration évaluée correspond au produit « Ledger Nano S Plus » tel que livré pour un utilisateur final, identifiable tel que décrit au chapitre 1.2.2.

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 produit en lui-même ne nécessite pas d'installation mais il faut le configurer en suivant les étapes décrites dans le guide utilisateur, voir [GUIDES].

2.2.1.3 Notes et remarques diverses

Néant.

2.2.2 Analyse de la documentation

L'évaluateur a eu accès à des documents de conception fournis par le développeur dans le cadre de cette évaluation.

2.2.3 Revue du code source (facultative)

L'évaluateur a eu accès au code source des *firmwares* du SE et du MCU. La revue a concerné les portions de code liées aux fonctions de sécurité faisant partie de la cible de sécurité [CDS].

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 inexploitable pour le niveau d'attaquant considéré, 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 de la TOE est remise en cause.

2.2.7.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un utilisateur.

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 « Ledger Nano S Plus, Firmware SE 1.0.4 » 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 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 : <ul style="list-style-type: none">- <i>Ledger Nano S Plus Security Target</i>, version 1.2, 9 juin 2022.
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none">- Rapport Technique d'Évaluation du Nano S Plus de Ledger en vue d'une certification CSPN, référence CE-RT-22-004-RB, version 1.3, 15 juin 2023.
[GUIDES]	Guide de configuration du produit : <ul style="list-style-type: none">- En ligne : Configurer votre Ledger Nano S Plus – Assistance, dernière mise à jour le 21 avril 2023, lien actif le 6 juillet 2023.

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 5.0, 12 janvier 2023. 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.