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-2019/03

Ledger Nano S
Version 1.5.1 (2c970001)

Paris, le 14 février 2019

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2019/03**
Nom du produit **Ledger Nano S**
Référence/version du produit **Version 1.5.1 (2c970001)**
Catégorie de produit **Matériel et logiciel embarqué**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Ledger SAS** **1 rue du Mail** **75002 Paris**
Développeur **Ledger SAS** **1 rue du Mail** **75002 Paris**
Centre d'évaluation **THALES (TCS – CNES)** **290 allée du Lac** **31670 Labège** **France**
Fonctions de sécurité évaluées **Générateur d'aléa** **Mécanisme d'attestation du firmware** **Vérification du PIN utilisateur** **Canal sécurisé pour l'installation / la mise à jour de firmwares et d'applications**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

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 CSPN 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 « Ledger Nano S, version 1.5.1 (2c970001) » développé par *LEDGER SAS*.

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

L'architecture participe à la sécurité du produit. Il est composé de deux microcontrôleurs :

- un générique, appelé *Microcontroller Unit* (MCU), en charge de gérer les entrées/sorties (affichage et boutons physiques) ;
- un sécurisé, le *Secure Element* (SE) ST31H320, en charge d'exécuter le système d'exploitation BOLOS et de réaliser les opérations cryptographiques. Ce composant est par ailleurs certifié [CER].

La figure ci-dessous explicite l'architecture du produit.

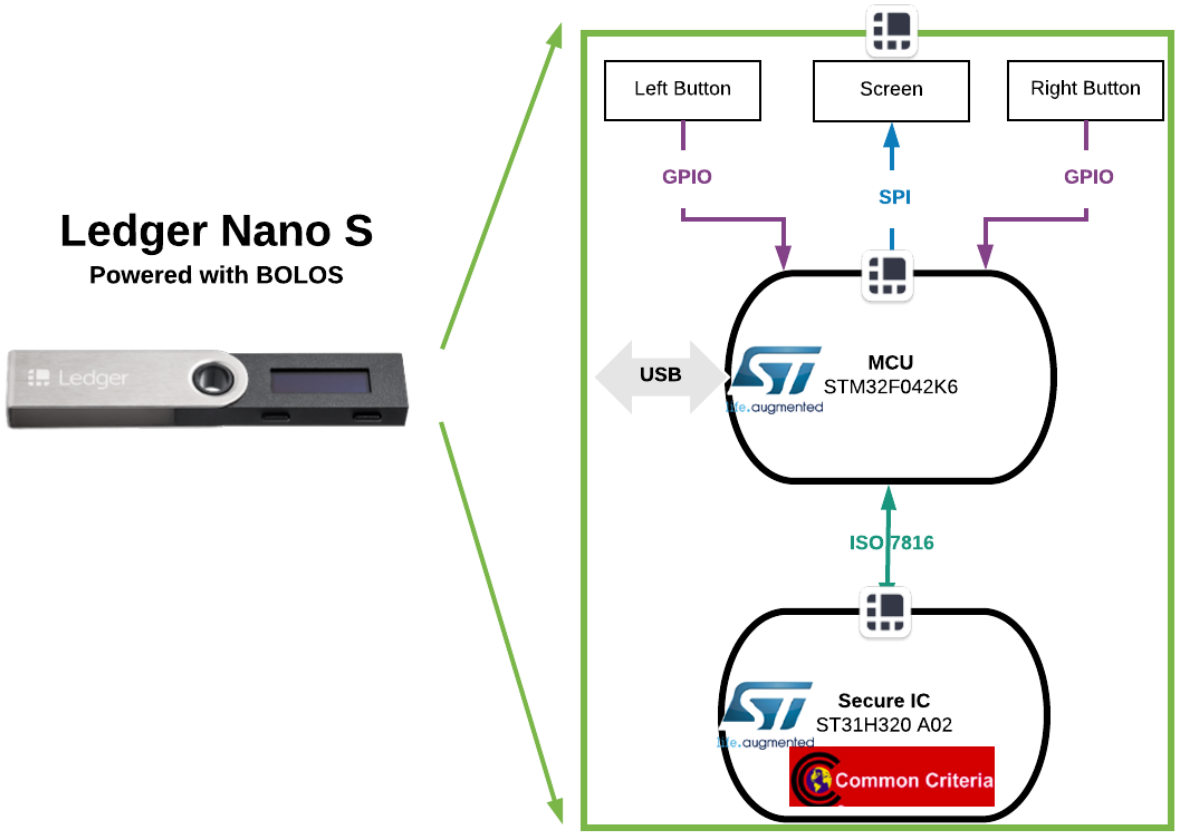

Figure 1 - Architecture produit

La figure ci-dessous détaille l'architecture logicielle exécutée par le SE.

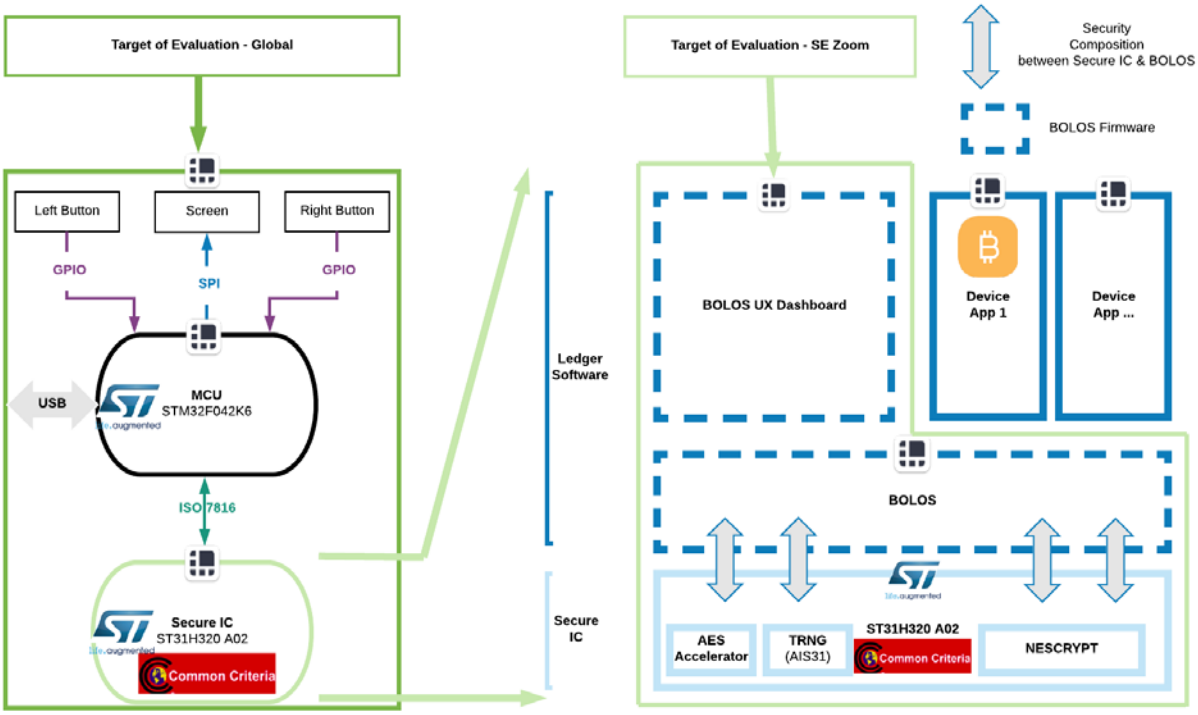

Figure 2 – Détail de l'architecture

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

Nom du produit	Ledger Nano S
Référence du SE	ST31H320
Nom du système d'exploitation du SE	BOLOS
Version du firmware du SE	1.5.1
Nom du système d'exploitation du MCU	SEPROXYHAL
Référence du MCU	STM32F042K6
Version du firmware du MCU	1.6

La version certifiée du produit peut être identifiée, après authentification de l'utilisateur, en sélectionnant le menu *Settings*, puis *Device* et enfin *Firmware* l'affichage expose les versions des *firmwares* du SE et MCU.

L'outil *ledgerblue* permet également d'interroger le produit afin de récupérer les versions des *firmwares* avec la commande suivante : `python -m ledgerblue.checkGenuine --targetId 0x31100004`.

Le guide utilisateur [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 :
- le générateur d'aléa ;
- le mécanisme d'attestation du *firmware* ;

- la vérification du PIN[1] utilisateur ;
- l'utilisation d'un canal sécurisé pour l'installation / la mise à jour de *firmwares* et d'applications.

1.2.4. Configuration évaluée

La plateforme de test est constituée d'un Ledger Nano S en version 1.5.1 (2c970001) pour le SE et 1.6 pour le MCU.

[1] *Personal Identification Number*

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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 est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. 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].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

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

Il n'y a pas d'installation, mais l'utilisateur doit initialiser le produit avant de pouvoir s'en servir, comme indiqué dans [GUIDES].

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

Le produit n'a pas besoin d'installation, il est prêt à l'emploi.

2.3.1.3. Durée de l'installation

Sans objet.

2.3.1.4. Notes et remarques diverses

Néant.

2.3.2. Analyse de la documentation

L'analyse des documents et fournitures a permis de conclure à une bonne conception du produit.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code est clairement organisé et correctement documenté. Chaque interface est bien commentée.

La maintenabilité du code est assurée par l'utilisation de fonctions clairement définies.

2.3.4. Analyse de la conformité des fonctions de sécurité

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

2.3.5. 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.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

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

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. 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.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Aucune recommandation particulière n'est formulée par l'évaluateur. Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis, en particulier les sections *Check the firmware version* et *Check hardware integrity*.

2.3.8.3. 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 grand public.

2.3.8.4. Notes et remarques diverses

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

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé au titre de cette évaluation CSPN. L'analyse n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

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, version 1.5.1 (2c970001) » 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 spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Ledger Nano S Security Target* Version : 1.2 ; Date : *18 octobre 2018.*
[RTE]	*Rapport Technique d'Evaluation CSPN Projet: Ledger Nano S* Référence : LEDGER_CSPN_RTE version 2.0 ; Version : 2.0 ; Date : *30 janvier 2019.*
[ANA-CRY]	*Analyse des mécanismes cryptographiques Projet: Ledger Nano S* Référence : LEDGER_CRY ; Version : 1.0 ; Date : *20 novembre 2018.*
[SPEC-CRY]	*Ledger Nano S Cryptographic Mechanisms Description - Release 1.3* Version : 1.3 ; Date : *18 novembre 2018.*
[GUIDES]	*User Manual Ledger Nano S* Version : 1.0 ; Date : *30 juillet 2018.*
[CER]	*Rapport de maintenance ANSSI-CC-2015/59-M01, ST31H320 A02 including optional cryptographic library NESLIB. Certifié par l'ANSSI le 20 avril 2016 sous la référence ANSSI-CC-2017/59-M01.*

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 des produits des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.