PREMIÈRE MINISTRE
Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense
et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2023/13

Ledger Nano S Plus

Firmware SE 1.0.4

WARNING

This report is intended to provide sponsors with a document enabling them to certify the level of safety offered by the product under the conditions of use or operation defined in this report for the version that has been evaluated. It is also intended to provide the potential purchaser of the product with the conditions under which he will be able to operate or use the product in such a way as to find himself in the conditions of use for which the product has been evaluated and certified; this is why this certification report must be read in conjunction with the evaluated user and administration guides as well as the product's security target, which describes the threats, the assumptions about the environment and the presupposed conditions of use, so that the user can judge whether the product meets his needs in terms of security objectives.

Certification does not in itself constitute a recommendation of the product by the Agence nationale de la sécurité des systèmes d'information (ANSSI) and does not guarantee that the certified product is totally free of exploitable vulnerabilities.

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-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	The True Random Number Generator The attestation mechanism The user PIN verification system The use of a secure channel for installing and updating firmware and applications
Fonctions de sécurité non évaluées	None
Restriction(s) d'usage	No

Table des matières

1 The product

1.1 Product presentation

The product evaluated is the “Ledger Nano S Plus, Firmware SE 1.0.4” developed by LEDGER.

The LEDGER Nano S Plus is a Personal Security Device (PSD) designed to securely store cryptographic secrets and provide cryptographic primitives. The product can be used as an electronic wallet, as a second authentication factor, or as a password safe. Functionality is added through applications that users install on the product from an application shop, based on the cryptographic primitives offered by the product.

The product is composed of two microcontrollers:

- A generic microcontroller, called the Microcontroller Unit (MCU), responsible for managing USB communications with the host and relaying the communications to the secure microcontroller;
- A secure microcontroller, called Secure Element (SE), in charge of running the BOLOS operating system and embedded applications and performing cryptographic operations.

1.2 Description of the product evaluated

The security target [CDS] describes the product evaluated, its security functionalities and its operating environment.

1.2.1 *Product category*

☐ 1	intrusion prevention
☐ 2	virus/malicious code protection
☐ 3	firewall
☐ 4	data erasure
☐ 5	security administration and supervision
☐ 6	identification, authentication and access control
☐ 7	secure communication
☐ 8	secure messaging
☐ 9	secure storage
☐ 10	secure operating environment
☐ 11	set top box (STB)
☒ 12	**hardware and embedded software**
☐ 13	industrial programmable logic controller
☐ 99	other

1.2.2 *Product Identification*

Product	
Product Name	Ledger Nano S Plus
SE reference	ST33K1M5C
Version of the SE Firmware	Firmware SE 1.0.4
Name of the SE Firmware	BOLOS
MCU reference	STM32F042K6
Name of the MCU Firmware	SEPROXYHAL
Product Identification	0x33 10 00 04

The certified version of the product can be identified by following the procedures described in chapter 3.5 of the [CDS].

The user manual, see [GUIDES], also details the steps for verifying the authenticity of the product.

1.2.3 *Security Functions*

The security functions evaluated are:

- The True Random Number Generator
- The attestation mechanism
- The user PIN verification system
  The use of a secure channel for installing and updating firmware and applications

1.2.4 *Configuration evaluated*

The configuration evaluated consists of the "Ledger Nano S Plus" as delivered to an end user, identifiable as described in chapter 1.2.2.

2 L'évaluation

2.1 Evaluation requirements

The evaluation was carried out in accordance with Certification de sécurité de premier niveau [CSPN].

2.2 Evaluation work

The evaluation work was carried out on the basis of the security requirements, sensitive assets, threats, users and security functions defined in the security target [CDS.

2.2.1 *Product installation*

2.2.1.1 Environment settings and installation options

The product has been evaluated in the configuration specified in paragraph 1.2.4.

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

The product itself does not require installation, but it must be configured by following the steps described in the user guide, see [GUIDES]

2.2.1.3 Notes and remarks

None.

2.2.2 *Documentation analysis*

The evaluator had access to design documents provided by the developer as part of this evaluation.

2.2.3 *Source code review (optional)*

The evaluator had access to the source code of the SE and MCU firmwares. The review concerned the portions of code related to the security functions included in the security target [CDS].

This analysis contributed to the compliance and resistance analysis of the product's security functions.

2.2.4 *Conformity analysis of security functions*

All the security functions tested were found to comply with the security target [CDS].

2.2.5 *Analysis of security function mechanism resistance*

All security functions have undergone penetration testing, and none has been found to present a vulnerability that could be exploited in the context in which the product is used and by the intended level of attacker.

2.2.6 *Vulnerability analysis (design, manufacture,etc.)*

2.2.6.1 List of know vulnerabilities

No known and exploitable vulnerabilities have been identified in the evaluated version of the product .

2.2.6.2 List of vuleneraibilities discovered during the evaluation and expert opinion

Potential vulnerabilities have been identified, but found to be unexploitable for the level of attacker considered, in the context defined by the security target [CDS].

2.2.7 *Ease of use analysis*

2.2.7.1 Case where security is compromised

The evaluator has not identified any situation where the TOE's security has been called into question.

2.2.7.2 Expert opinion on ease of use

Overall, the product is well documented, and its implementation does not present any difficulties for a user.

2.2.7.3 Other notes and remarks

No notes or remarks were made in the evaluation technical report [RTE].

2.3 Cryptographic mechanism strenght analysis

The cryptographic mechanisms implemented by the product's security functions (see [CDS]) have been analyzed in accordance with procedure [CRY-P-01] and the results recorded in report [RTE].

This analysis did not identify any non-compliance with the [ANSSI Crypto] standard. The independent vulnerability analysis performed by the evaluator did not reveal any exploitable vulnerability for the targeted attacker level.

2.4 Random number generator analysis

The product includes a random generator which has been analyzed in accordance with procedure [CRY-P-01].

This analysis did not identify any non-compliance with the [ANSSI Crypto] standard.

The independent vulnerability analysis performed by the evaluator did not reveal any exploitable vulnerability for the targeted attacker level.

3 Certification

3.1 Conclusion

The evaluation was conducted in accordance with the current rules and standards, with the competence and impartiality required for an accredited evaluation center.

This certificate attests that the product "Ledger Nano S Plus, Firmware SE 1.0.4" submitted for evaluation meets the security characteristics specified in its security target [CDS] for the level of evaluation expected in a first-level security certification.

3.2 Recommandations and restrictions on use

This certificate applies to the product specified in chapter 1.2 of this certification report.

The user of the certified product must ensure compliance with the environmental security objectives specified in the security target [CDS] and follow the recommendations contained in the guides provided [GUIDES].