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

Certification Report ANSSI-CSPN-2019/03

Ledger Nano S
Version 1.5.1 (2c970001)

Paris, le February 14th, 2019

Courtesy Translation

SÉCURITÉ CERTIFICATION

Warning

This report is intended to provide sponsors with a document certifying the security of the product under the operating or usage conditions set out in this report, for the version evaluated. It is also intended to inform potential buyers of the conditions in which they may use or operate the product, in order to ensure that the product is used under the conditions for which it has been evaluated and certified. Consequently, this certification report must be read in conjunction with the evaluated user and administration guides and the product's security target, which contains a list of threats and a set of assumptions about the usage environment and conditions, so that users can make an informed decision as to whether the product meets their security requirements.

Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

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
France

certification@ssi.gouv.fr

Certification report reference **ANSSI-CSPN-2019/03**
Product name **Ledger Nano S**
Product reference/version **Version 1.5.1 (2c970001)**
Product category **Embedded hardware and software**
Evaluation criteria and version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Sponsor **Ledger SAS** **1 rue du Mail** **75002 Paris**
Developer **Ledger SAS** **1 rue du Mail** **75002 Paris**
Evaluation facility **THALES (TCS – CNES)** **290 allée du Lac** **31670 Labège** **France**
Security functions evaluated **True Random Number Generator** **Firmware attestation mechanism** **User PIN verification system** **Secure channel for installing/updating firmware and applications**
Security function(s) not evaluated **None**
Restriction(s) on use **No**

Preface

Certification

The security certification of information technology products and systems is governed by amended decree No. 2002-535 of 18 April 2002. This decree states that:

- L'agence nationale de la sécurité des systèmes d'information establishes certification reports. These reports specify the characteristics of the proposed security objectives. They may contain any warnings that the authors deem useful for security purposes. They may be disclosed to third parties or the general public at the sponsor's discretion (article 7).
- The certificates issued by the Prime Minister attest that the sample product or system evaluated complies with the specified security objectives. They also attest that the evaluations have been performed in accordance with current rules and standards, with the requisite competence and impartiality (article 8).

The CSPN (first level security certification) procedures are available at www.ssi.gouv.fr.

Contents

1. The product

1.1. Product presentation

The product evaluated is the "Ledger Nano S, version 1.5.1 (2c970001)" developed by *LEDGER SAS*.

The *Ledger Nano S* is a Personal Security Device (PSD) designed to securely store cryptographic secrets and provide cryptographic primitives. As it provides secure cryptographic storage, the product can also be used as a hardware wallet, a second factor of authentication or a password manager. These additional functionalities are provided by applications that the user installs from an application store, which use the cryptographic primitives offered by the product itself.

The product's architecture is key to its security. It features two microcontrollers:

- A generic microcontroller called the Microcontroller Unit (MCU), which manages inputs/outputs (screen and buttons);
- A secure microcontroller called the Secure Element (SE) ST31H320, which runs the BOLOS operating system and performs cryptographic tasks. This component is also certified [CER].

The figure below shows the architecture of the product.

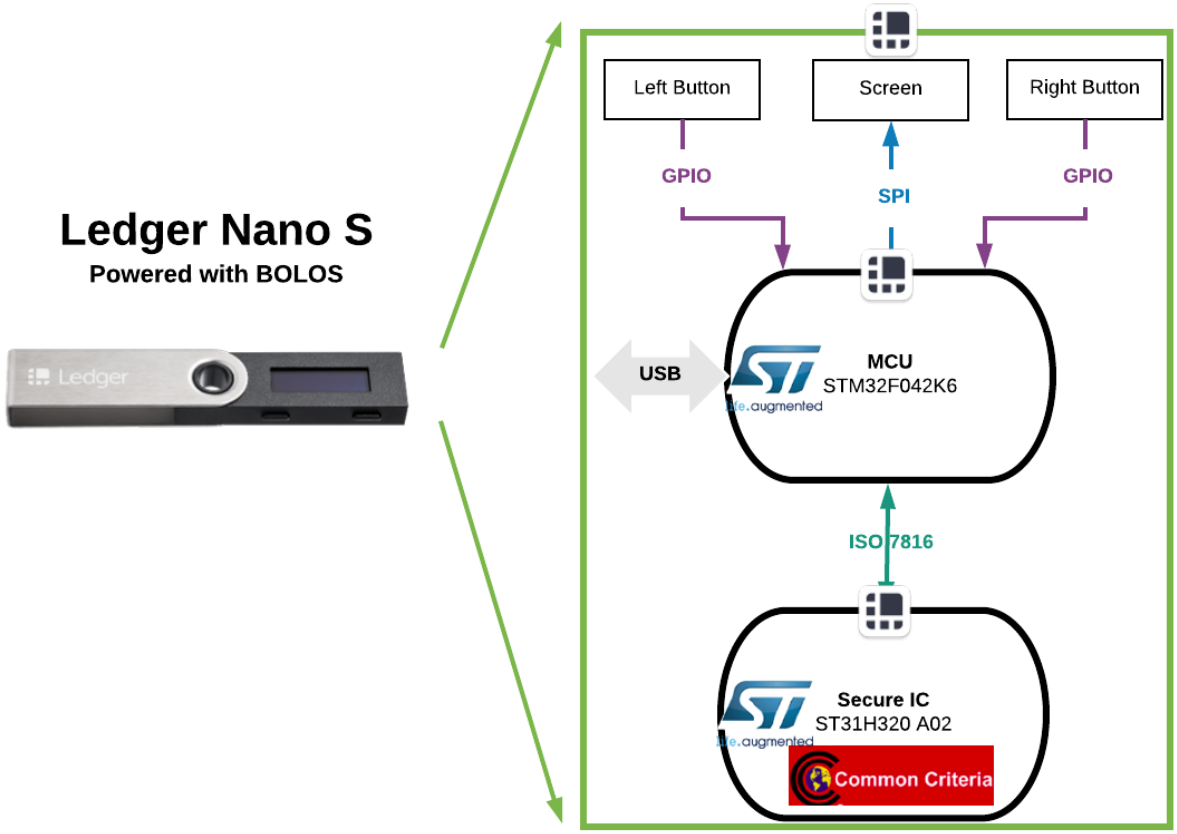

Figure 1 – Product architecture

The figure below shows the architecture of the software running on the SE.

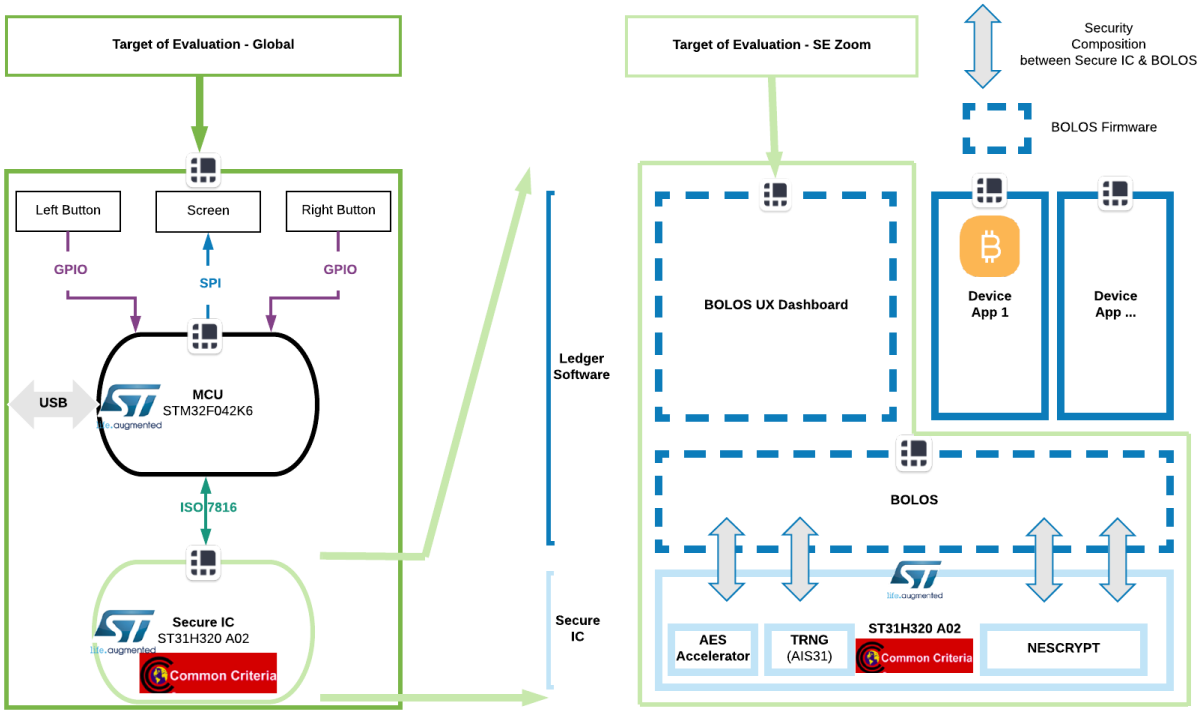

Figure 2 – Detailed diagram of the architecture

1.2. Description of the product evaluated

The security target [ST] 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 – embedded hardware and software**
☐ 13 – industrial programmable logic controller
☐ 99 – other

1.2.2. Product identification

Product name	Ledger Nano S
SE reference	ST31H320
SE operating system	BOLOS
SE firmware version	1.5.1
MCU operating system	SEPROXYHAL
MCU reference	STM32F042K6
MCU firmware version	1.6

Once authenticated, users can check the certified product version by opening the Settings menu and selecting Device and then Firmware. The SE and MCU firmware versions are displayed.

The Ledger Blue tool can also be used to identify the firmware versions, via the following command: `python -m ledgerblue.checkGenuine --targetId 0x31100004`.

The user guide [GUIDES] also explains in detail how to verify the authenticity of the product.

1.2.3. Security functions

The security functions evaluated are:

- The True Random Number Generator

- The firmware attestation mechanism
- The user PIN[1] verification system
- The secure channel for installing/updating firmware and applications.

1.2.4. Configuration evaluated

The test platform consists of a Ledger Nano S, version 1.5.1 (2c970001) for the SE and 1.6 for the MCU.

[1] Personal Identification Number

2. The evaluation

2.1. Evaluation benchmarks

The evaluation was performed in accordance with First Level Security Certification [CSPN]. The document references can be found in **Erreur ! Source du renvoi introuvable.**.

2.2. Anticipated workload and duration of the evaluation

The length of the evaluation was determined by the workload anticipated in the evaluation file.

2.3. The evaluation process

The evaluation process was conducted on the basis of the security requirements, sensitive assets, threats, users and security functions described in the security target [ST].

2.3.1. Product installation

2.3.1.1. Specific environment configuration features and installation options

The product was evaluated using the configuration specified in paragraph 1.2.4.

No installation is required. However, users must initialise the product before use, as explained in [GUIDES].

2.3.1.2. Description of the installation process and of any non-conformities

The product does not need to be installed, it is ready to use.

2.3.1.3. Installation time

Not applicable.

2.3.1.4. Notes and remarks

None.

2.3.2. Document analysis

The analysis of the documents and materials provided concluded that the product is well designed.

2.3.3. Source code review (optional)

The evaluator reviewed the source code and concluded that it is well organised and properly documented. Every interface is well commented.

The maintainability of the code is ensured by the use of clearly defined functions.

2.3.4. Security function compliance analysis

All the security functions tested complied with the security target [ST].

2.3.5. Security function strength analysis

All the security functions underwent intrusion tests and none of them displayed any exploitable vulnerability to the specified level of attack, in the product's context of use.

2.3.6. Vulnerability analysis (conception, design, etc.)

2.3.6.1. List of known vulnerabilities

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

2.3.6.2. List of vulnerabilities discovered during the evaluation and expert opinion

No intrinsic or operational vulnerabilities were discovered that might undermine the security of the product.

2.3.7. Developer access

Not applicable.

2.3.8. Ease of use analysis and recommendations

2.3.8.1. Cases where security is undermined

The evaluator did not identify any cases where the TOE's security objectives are undermined.

2.3.8.2. Recommendations for safe use of the product

The evaluator did not make any particular recommendations. The context of use specified in the security target [ST] must be adhered to and users must comply with the [GUIDES] provided, particularly the sections entitled 'Check the firmware version' and 'Check hardware integrity'.

2.3.8.3. Expert opinion on ease of use

The product is well documented on the whole, and should not present any problems for the general user.

2.3.8.4. Notes and remarks

No notes or remarks were made in the [ETR].

2.4. Cryptographic mechanism strength analysis

The product's cryptographic mechanisms were analysed as part of the CSPN evaluation. The analysis did not reveal any non-conformity with the general security reference base (RGS), or any exploitable vulnerability.

2.5. Random number generator analysis

The product's randomiser was analysed as part of the CSPN evaluation. The analysis did not reveal any non-conformity with the general security reference base [RGS], or any exploitable vulnerability.

3. Certification

3.1. Conclusion

The evaluation was performed in accordance with current rules and standards, with the competence and impartiality required of an approved evaluation facility.

This certificate attests that the product evaluated "Ledger Nano S, version 1.5.1 (2c970001)" meets the security requirements set out in its security target [ST] based on the level of evaluation expected for first level security certification.

3.2. Restrictions of use

This certificate relates to the product specified in chapter 1.2 of this certification report.
Users of the certified product must comply with the environment security requirements specified in the security target [ST], and, where relevant, must follow the recommendations set out in this report regarding the context of use of the product (see 2.3.8.2).

Annex 1. Documentary references for the product evaluated

[ST]	*Ledger Nano S Security Target* Version : 1.2 ; Date: *18 October 2018.*
[ETR]	*Rapport Technique d'Evaluation CSPN Projet: Ledger Nano S* Reference : LEDGER_CSPN_RTE version 2.0 ; Version : 2.0 ; Date: *30 January 2019.*
[ANA-CRY]	*Analyse des mécanismes cryptographiques Projet: Ledger Nano S* Reference : LEDGER_CRY ; Version : 1.0 ; Date: *20 November 2018.*
[SPEC-CRY]	*Ledger Nano S Cryptographic Mechanisms Description - Release 1.3* Version : 1.3 ; Date: *18 November 2018.*
[GUIDES]	*User Manual Ledger Nano S* Version : 1.0 ; Date: *30 July 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.*

Annex 2. Certification references

Amended decree No. 2002-535 of 18 April 2002 relating to the evaluation and certification of the security provided by information technology products and systems.	
[CSPN]	First level security certification of information technology products, version 1.1, reference ANSSI-CSPN-CER-P-01/1.1 of 7th of April 2014. Evaluation criteria for first level security certification, version 1.1, reference ANSSI-CSPN-CER-I-02/1.1 of 23rd of April 2014. Evaluation methodology for first level security certification, reference ANSSI-CSPN-NOTE-01/2 of 23rd of April 2014. Documents available at www.ssi.gouv.fr.
[RGS]	Cryptographic mechanisms – Rules and recommendations concerning the choice and dimensioning of cryptographic mechanisms, version 2.03 of 21st of February 2014, appended to the general security reference base (RGS_B1), see www.ssi.gouv.fr.