PRIME MINISTER

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CSPN-2019/12

Ledger Nano X

FW SE: Version 1.2.5-1 (2C970004)

FW MCU: Version 2.8

Paris, 27 September 2019

Courtesy Translation

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, in itself, constitute a recommendation of the product by the National Cybersecurity Agency (ANSSI), and does not guarantee that the certified product is totally free of exploitable vulnerabilities.

All correspondence regarding this report should 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

certification@ssi.gouv.fr

Certification report reference **ANSSI-CSPN-2019/12**
Product name **Ledger Nano X**
Product reference/version **FW SE: Version 1.2.5-1 (2C970004)** **FW MCU: Version 2.8**
Product category **Hardware and embedded software**
Evaluation criteria and version **FIRST LEVEL SECURITY CERTIFICATION (CSPN)**
Sponsor **Ledger SAS** **1 rue du Mail** **75002 Paris, France**
Developer **Ledger SAS** **1 rue du Mail** **75002 Paris, France**
Evaluation centre **CEA - LETI** **17 avenue des Martyrs** **38054 Grenoble Cedex 9** **France**
Security functions evaluated **True Random Number Generator** **Firmware attestation mechanism** **User PIN verification** **Secure channel for installing/updating firmware and applications**
Security function(s) not evaluated **None**
Restriction(s) on use **None**

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:

- The National Cybersecurity Agency 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 X, FW SE version 1.2.5-1 (2C970004), FW MCU: version 2.8" developed by *LEDGER SAS.*

The *LEDGER* Nano X is a Personal Security Device (PSD) designed to securely store cryptographic secrets and provide cryptographic primitives. This product may be used as an electronic wallet, a second factor of authentication, or a password manager by installing appropriate additional applications. The installation of additional applications, which the user downloads from an app store, relies on the product's cryptographic primitives.

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

- a generic microcontroller or Microcontroller Unit (MCU) STM32WB55CG;
- a secure microcontroller or Secure Element (SE) ST33J2M0, which performs all sensitive operations. This component is certified

The figure below shows the architecture of the product.

Figure 1 - Product architecture

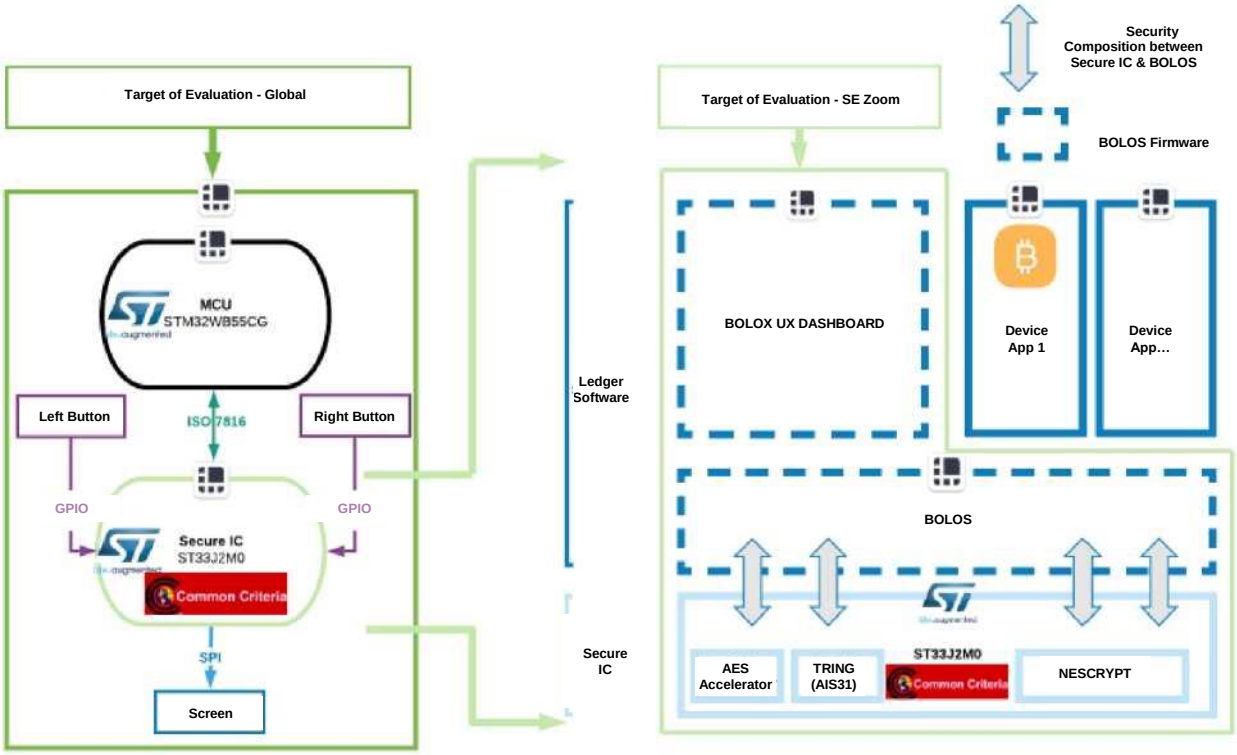

Figure 2 – Detailed diagram of the architecture

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 name	Ledger Nano X
SE reference	ST33J2M0
SE operating system	BOLOS
SE firmware version	1.2.5-1 (2C970004)
MCU reference	STM32WB55CG
MCU operating system	SEPROXYHAL
MCU firmware version	2.8

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

The Ledger Blue tool can also be used to identify the firmware versions, via the following command: `python -m ledgerblue.checkGenuine --targetId 0x33000004`.

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 X, version 1.2.5-1 (2C970004) for the SE and 2.8 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 procedures [CSPN]. The document references can be found in Appendix 2.

2.2. Anticipated workload and evaluation time

The evaluation time 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 [CDS].

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 0.

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

N/A.

2.3.1.4 Notes and remarks

None.

2.3.2. Documentation 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 [CDS].

2.3.5. Security function strength analysis

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

2.3.6. Vulnerability analysis (design, manufacture, 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. Meetings with developers

N/A.

2.3.8. Ease of use analysis

2.3.8.1. Cases where security is undermined

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

The evaluator did not make any particular recommendations. The conditions of use set out in the security target [CDS] must be met and users must comply with the [GUIDES] provided.

2.3.8.2. Expert opinion on ease of use

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

2.3.8.3 Notes and remarks

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

2.4. Cryptographic mechanism strength analysis

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

2.5. Randomiser analysis

The product's randomiser was analysed as part of the CSPN evaluation. The analysis did not reveal any non-conformities with the RGS, or any exploitable vulnerabilities.

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 centre.
This certificate attests that the evaluated product - "Ledger Nano X, FW SE: Version 1.2.5-1 (2C970004), FW MCU: Version 2.8" - meets the security requirements set out in its security target [CDS], based on the level of evaluation expected for first level security certification.

3.2. Recommendations and restrictions on use

This certificate relates to the product specified in chapter 1.2 of this certification report. Users of the certified product must comply with security objectives relating to the environment and conditions of use, as specified in the safety target [CDS]. Users must also comply with [GUIDES]

Appendix 1. Documentary references for the product evaluated

[CDS]	*Ledger Nano X Security Target* Version: *1.2*; Date: *10 June 2019.*
[RTE]	*CSPN Evaluation Technical Report - IncompreX* Reference: LETI.CESTI.INX.ETR.001; Version: 1.1; Date: *9 September 2019.* *Rating of cryptographic mechanisms - IncompreX* Reference: LETI.CESTI.INX.RT.001; Version: 1.1; Date: *9 September 2019.*
[GUIDES]	*Ledger Nano X Bluetooth-enabled hardware wallet User Manual* Reference: LedgerNanoX_UserManual_v1.3; Version: 1.3; Date: *6 June 2019.*
[CER]	*"ST33J2M0 A02", certified by ANSSI on 21 August 2017 under reference ANSSI-CC-2017/50, Monitoring report under reference ANSSI-CC-2017/50-S01, 18 April 2019.*

Appendix 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, reference ANSSI-CSPN-CER-P-01/2.0 of 6 September 2018. Evaluation criteria for first level security certification, reference ANSSI-CSPN-CER-P-02/3.0 of 18 March 2019. Evaluation methodology for first level security certification, reference ANSSI-CSPN-NOTE-01/3 of 6 September 2018. 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 21 February 2014, appended to the general security reference base (RGS B1), see www.ssi.gouv.fr.