



**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-2023/17

**Ledger Nano X**  
**Firmware SE 2.1.0**



## 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](mailto:certification@ssi.gouv.fr)

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

Référence du rapport de certification	<b>ANSSI-CSPN-2023/17</b>
Nom du produit	<b>Ledger Nano X</b>
Référence/version du produit	<b>Firmware SE 2.1.0</b>
Catégorie de produit	<b>Matériel et logiciel embarqué</b>
Critère d'évaluation et version	<b>CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)</b>
Commanditaire	<b>LEDGER</b> 1 rue du Mail 75002 Paris
Développeur	<b>[LEDGER]</b> 1 rue du Mail 75002 Paris
Centre d'évaluation	<b>EDSI</b> 1 rue du Mail 75002 Paris
Fonctions de sécurité évaluées	<b>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</b>
Fonctions de sécurité non évaluées	<b>None</b>
Restriction(s) d'usage	<b>No</b>

## 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.cyber.gouv.fr](http://www.cyber.gouv.fr).

## TABLE DES MATIERES

1	The product.....	6
1.1	Product presentation .....	6
1.2	Description of the product evaluated .....	6
1.2.1	Product category .....	6
1.2.2	Product Identification .....	7
1.2.3	Security Functions.....	7
1.2.4	Configuration evaluated .....	7
2	The evaluation.....	8
2.1	Evaluation requirements .....	8
2.2	Evaluation work .....	8
2.2.1	Product installation.....	8
2.2.2	Documentation analysis.....	8
2.2.3	Source code review ( optional) .....	8
2.2.4	Conformity analysis of security functions.....	8
2.2.5	Analysis of security function mechanism resistance.....	8
2.2.6	Vulnerability analysis (design, manufacture, etc.).....	9
2.2.7	Ease of use analysis.....	9
2.3	Cryptographic mechanism strenght analysis.....	9
2.4	Random number generator analysis.....	9
3	Certification .....	10
3.1	Conclusion.....	10
3.2	Recommandations et restrictions d'usage .....	10

# 1 The product

## 1.1 Product presentation

The product evaluated is the "Ledger Nano X, Firmware SE 2.1.0" developed by LEDGER.

The LEDGER Nano X 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), is responsible for managing USB and BLE (Bluetooth) communications with the host, relaying the communications to the secure microcontroller, as well as the battery management;
- 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

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

### 1.2.2 Product Identification

Product	
Product Name	Ledger Nano X
Version of the SE Firmware	Firmware SE 2.1.0
SE reference	ST33J2M0
Name of the SE Firmware	BOLOS
MCU reference	STM32WB35
Name of the MCU Firmware	SEPROXYHAL
Product Identification	0x33 00 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
- The application isolation

### 1.2.4 Configuration evaluated

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

## 2 The evaluation

### 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 of installation and any non-conformities

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 known vulnerabilities

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

### 2.2.6.2 List of vulnerabilities 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 strength 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 X, Firmware SE 2.1.0" 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 et restrictions d'usage**

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].