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

Maintenance Report
ANSSI-CSPN-2019/03-M01

Ledger Nano S
Version 1.5.5 (2c970001)

Reference Certificate : ANSSI-CSPN-2019/03

Paris, August 7th, 2019

COURTESY TRANSLATION

SÉCURITÉ CERTIFICATION

1. References

[CER]	Rapport de certification ANSSI-CSPN-2019/03 Ledger Nano S Version 1.5.1 (2c970001), February 14th, 2019, ANSSI.
[MAI]	Assurance continuity procedure ANSSI-CC-MAI-P-01.
[IAR]	Security Impact Analysis from Ledger Nano S v1.5.1 to v1.5.5 Report, Release 1.0, March 13th, 2019, *LEDGER*.

2. Identification of the maintained product

The product "Ledger Nano S, version 1.5.1 (2c970001)" has been initially certified under the reference ANSSI-CSPN -2019/03 (reference [CER]).

The product object of this maintenance, is the "Ledger Nano S, version 1.5.5" developed by *LEDGER*.

The maintained revision of the product is identifiable, after user authentication, by opening the *Settings* menu and selecting *Device* and then *Firmware*. Version 1.5.5 of the SE firmware is then displayed.

3. Description of changes

The security impact analysis report (reference [IAR]) mentioned that the following modifications have been done:

- Addition of the Shnorr signature scheme to ensure compatibility with *ZILLIQA*,
- Modification of the Blake2 implementation, which can generate output sizes other than 224, 256, 384 or 512 bits,
- Enhanced user experience,
- Functional bugs correction,
- Size optimisation of the cryptographic library code.

4. Conclusions

The changes listed above, which apply to functionalities outside the TOE, are considered as having a minor impact on the previously evaluated TOE.
The level of confidence in this new version of the product is therefore identical to that of the certified version, under the conditions described in the report [CER].

5. Warning

The resistance level of a certified product declines as time goes by. The vulnerability analysis of this product revision versus the new attacks that would have appeared since the certificate release has not been conducted in the frame of this current maintenance. Only a re-evaluation or a "surveillance" of the new product revision would allow maintaining the assurance level in a timely and efficient manner.