Ledger Nano S Plus Security Target

Release 1.2

LEDGER

Table of contents

1 Document Identification

1.1 Security Target Identification

Identification	`Ledger Nano S Plus` Security Target
Release	1.2
Date	2022-06-09
Diffusion	Public

1.2 Security Target History

Release	Date	Author	Role	Comments
1.0	2022-01-27	Alain DESTRÉS	Security Certification Lead	Initial Release
1.1	2022-03-01	Alain DESTRÉS	Security Certification Lead	Updates
1.2	2022-06-09	Alain DESTRÉS	Security Certification Lead	Updates following EDSI pre-evalaution

1.3 Security Target Approbation

Release	Date	Reviewer	Role
1.2	2022-06-23	Benoît LUCET	Product Owner, Hardware wallets
1.2	2022-06-23	Matt JOHNSON	Chief Information Security Officer

2 Introduction

2.1 Document Context

This document constitutes the security target of the `Ledger Nano S Plus` in the context of a CSPN evaluation.

2.2 Documentation Identification

2.2.1 ANSSI related documents

The following tables identify the documents regarding the CSPN evaluation.

Reference	Title	Version	Date
[CER-P-01]	Certification de sécurité de premier niveau des produits des technologies de l'information	3.0	2021-04-12
[CRY-P01]	Modalités pour la realisation des analyses cryptographiques et des evaluations des générateurs de nombres aléatoires	4.1	2020-01-26

Reference	Title	Version	Date
[PG-83]	Guide des mécanismes cryptographiques: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques	2.04	2020-01-01
[RGS_B2]	Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques	2.0	2012-06-08
[RGS_B3]	Règles et recommandations concernant les mécanismes d'authentification	1.0	2010-01-13

2.2.2 Bitcoin Improvement Proposal

Reference	Title	Date
[BIP32]	Hierarchical Deterministic wallets	2012-02-11
[BIP39]	Mnemonic code for generating deterministic keys	2013-09-10
[BIP44]	Multi-Account Hierarchy for deterministic Wallets	2014-04-24

2.2.3 Ledger

Reference	Title
[CMD]	Cryptographic Mechanisms Description, version 1.1
[CTM]	Cryptography Testing Methodology, version 1.0
[CTP]	Cryptographic Test Plan, version 1.0
[UM]	User Manual - `Ledger Nano S Plus`
[Ledger Live]	Ledger Live
[CheckHardwareIntegrity]	Check hardware integrity
[Python Loader Installation]	Python Loader Installation
[Python Loader Exploitation]	Python Loader Exploitation
[LEDGERCtl]	A Python library to control Ledger devices
[Get Started]	Set up your `Ledger Nano S Plus`

2.2.4 Certicom Research

Reference	Title	Version	Date
[SEC_2]	Certicom Research Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters	2.0	2010-01-27

2.2.5 Federal Office for Information Security (BSI)

Reference	Title	Version	Date
[AIS31]	Functionality classes and evaluation methodology for physical random number generators	1.0	2001-09-25

2.2.6 STMicroelectronics Main Hardware

Reference	Type	Role
[ST33K1M5C]	Secure IC	Main Hardware offering an EAL 6+ security level as stated in [ST33_CC]
[STM32F042K6]	MCU	Supporting Hardware
[ST33_CC]	Certification	ST33K1M5C Evaluation Assurance Level 6+ Certification report CC-21-0252712

3 TOE description

The `Ledger Nano S Plus` 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 through Device Apps the user can download and install on his device.

To install such Device App, Ledger developed the Ledger Live application, which can be run on a desktop, tablet or a mobile device. Such equipment running Ledger Live is hereafter denoted Host. Once the device is connected to the Host executing Ledger Live, the user is able to setup and install Device Apps to his device.

3.1 Operational Environment

Ledger offers a full ecosystem to interface with the dedicated web services, offering a smooth User Experience:

- The Ledger's secure servers (based on HSM technology) ensure that the `Ledger Nano S Plus` is genuine, therefore proving that the current `Ledger Nano S Plus` is indeed issued by Ledger.
- The Ledger Live application, optional according to the use case, shares the account details, connects to the corresponding blockchain network and allows Device App installation on the `Ledger Nano S Plus`.
- The `Ledger Nano S Plus` device is leveraged to perform sensitive operations (i.e., generating the seed, signing transactions, submitting passwords).

The diagram below illustrates the main interactions between elements when the Ledger Live is required:

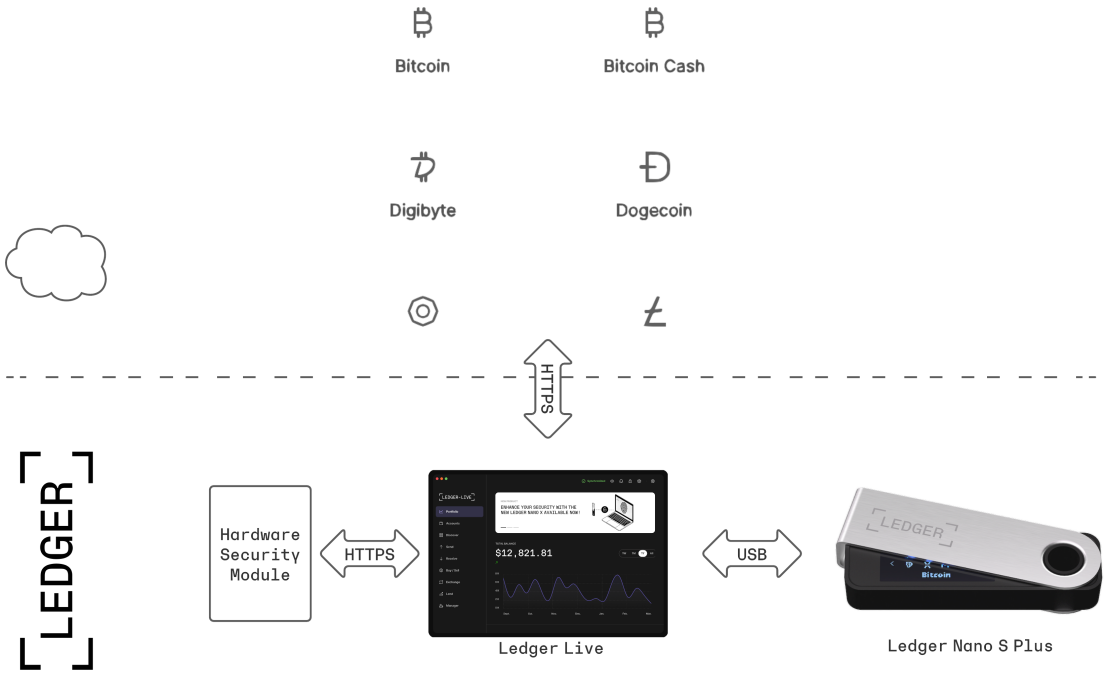

Figure 1: Environment with Ledger Live

The following diagram illustrates the main interactions between elements when the Ledger Live is not required:

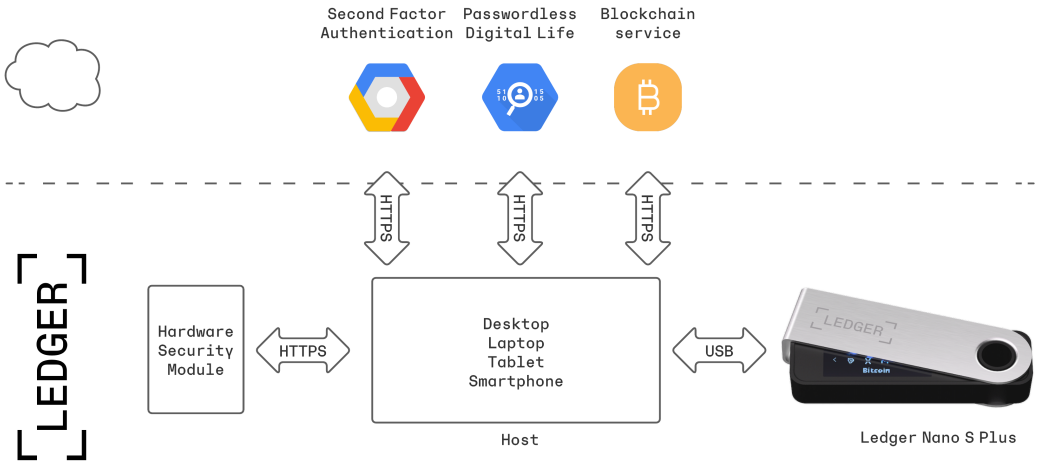

Figure 2: Environment without Ledger Live

Thus, according to the use case, the End-User interacts with:

- `Ledger Nano S Plus`
- Third-party wallet
- Ledger Live, if required

3.2 Features

The `Ledger Nano S Plus` supports the following features:

- Multi-services: Hardware Wallet, Cryptographic Platform, Password Manager, Second Factor authenticator (FIDO)
- Comply with several cryptocurrencies: Bitcoin, Bitcoin Cash, Bitcoin Gold, Ethereum, Ethereum Classic, Ethereum tokens...
- USB connectivity
- Open Source Device App: all Device Apps developed by Ledger can be reviewed and verified by End-Users (e.g. Bitcoin, Ethereum)
- Developer friendly: develop a Device App and then install it on the `Ledger Nano S Plus`
- Comply with the main BIP standards: [BIP32], [BIP39] and [BIP44]
- Multi-platform: Windows (8.1+), macOS (10.14+), Linux (64 bits desktop computers excluding ARM), Android (8.1+) and iOS (13+)
- **OLED screen**: to verify the transaction data (amount, address)
- **Buttons**: used to get the End-User's consent relative to sensitive operations like unlocking the device or processing a transaction
- **PIN**: to unlock the `Ledger Nano S Plus`
- **Plausible deniability**: an additional PIN linked to a passphrase can be defined to create an hidden account
- **Genuine PSD**: cryptographic attestation mechanisms ensuring that the `Ledger Nano S Plus` is a genuine one
- **Post-issuance capability**: all piece of software (MCU Firmware, SE Firmware, Device Apps) can be securely updated

Bold features are included in the security scope and addressed by dedicated security functions. The Ledger's security model is based on the Secure Element technology and the embedded software developed by Ledger. In other words, the compromise of the connectivity (USB) or the Host application does not compromise the PSD.

3.3 Services

Services are not included in the security scope. These services are not addressed in the scope because they are all protected by the End-User's PIN. Indeed, the `Ledger Nano S Plus` requires the End-User's PIN to unlock all services listed in the following sections. Thus, even if the services are out of scope, the secret data belonging to services are properly protected through the PIN.

3.3.1 Hardware Wallet Service

The wallet is the main service.

It is the combination of the following two elements that creates an operational wallet:

- Ledger Live executed on the Host or a crypto wallet logic from a third-party app
- `Ledger Nano S Plus` with the dedicated crypto asset application installed and currently selected. The `Ledger Nano S Plus` acts as a secure gateway to the blockchain technology.

This wallet service managing crypto assets is in charge of:

- Managing the balance (through Ledger Live)
- Handling one or several accounts (through Ledger Live)
- Supporting one or several crypto assets: Bitcoin, Bitcoin Cash, Bitcoin Gold, Ethereum, Ethereum Classic... (through Ledger Live & `Ledger Nano S Plus`)
- Processing transactions: receive & perform payments (through Ledger Live & `Ledger Nano S Plus`)

If one of these elements is removed, no transaction can be processed. The Host performs no security operations. All sensitive operations (for instance signing a transaction, confirming the transaction amount, confirming the recipient's address) are directly performed within the `Ledger Nano S Plus` based on the Secure Element technology. The security model designed by Ledger relies on the `Ledger Nano S Plus` including not only a certified secure IC [ST33_CC] but also a secure software developed by Ledger.

3.3.2 Cryptographic Platform Service

The `Ledger Nano S Plus`, considered as a cryptographic embedded platform, supports several cryptographic primitives as listed below (not limited to):

- Symmetric cryptography: DES/3DES, AES
- Asymmetric cryptography: RSA (key size: 1024, 2048, 3072, 4096 bits), EC (brainpool, SECP and ANSSI)
- Secure Hash: SHA224, SHA256, SHA384, SHA512, SHA3, Blake, Grøstl

3.3.3 Password Manager Service

A Device App manages all your passwords making the connection step easier for the End-User.

3.3.4 FIDO Service

The FIDO U2F Device App is a two-factor authentication method specified by the FIDO Alliance. It is compliant with several web services, like Facebook, Dashlane, Gmail, Dropbox, GitHub, etc.

For each of these web services, the End-User needs to set up the security parameters of the account to register the `Ledger Nano S Plus` as a second factor security key to authenticate on it. This second factor of verification will improve the security of your login processes, as the End-User will first be required to input his credentials (login/password) followed by the second factor via the `Ledger Nano S Plus`.

3.3.5 Additional Innovative Services

As the Ledger's ecosystem is developer-friendly, a third-party can develop a Device App to build an innovative and useful service. This flexible approach is possible thanks to BOLOS acting as an Open Platform.

3.4 Dual-Chip Architecture

The `Ledger Nano S Plus` is based on an architecture leveraging two hardwares:

- A generic MCU: [STM32F042K6]
- A Secure IC: [ST33K1M5C]

The [STM32F042K6], considered as a supporting hardware, is in charge of:

- Communicating with the Host via USB

- Communicating with the SE

The [ST33K1M5C] belongs to the Secure Element Technology and is Common Criteria certified (refer to [ST33_CC] to get further details). The Secure Element technology is leveraged in various sensitive applications such as: banking card, passport, driving licence, etc. The `Ledger Nano S Plus` relies on this Secure Element technology to properly protect the End-User's assets and for the handling of all sensitive operations and is in charge of (but not limited to):

- Generating the seed
- Deriving the corresponding Key Pair
- Signing transactions
- Communicating with the MCU
- Driving the screen
- Receiving the notifications from the buttons

The `Ledger Nano S Plus` is a secure hardware wallet thanks to the proper usage of the Secure Element technology. It can be used for instance in relation with Ledger Live running on top of the Host as illustrated by the following diagram:

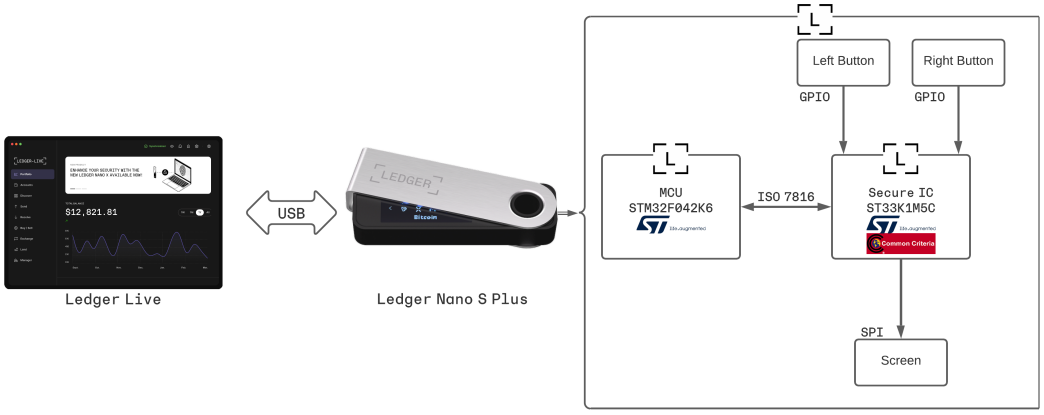

Figure 3: Zoom on the Ledger Nano S Plus

One of the main advantages of the dual-chip architecture is the fact that the environment interacting with the `Ledger Nano S Plus` can be hacked without compromising the overall security. For instance, if the Host is compromised, it cannot introduce a security breach in the `Ledger Nano S Plus`. The security model defined by Ledger is that only the `Ledger Nano S Plus` can be trusted. Thus, this solution is resistant against threats like malware.

Additionally, the End-User actively participates in the security: all sensitive operations must get the End-User's consent (PIN validation, transaction confirmation) achieved via the screen and buttons.

3.5 Identification

The following table identifies the `Ledger Nano S Plus` according to the CSPN process:

Product Name	`Ledger Nano S Plus`
Product category	Hardware and embedded software
Developer	Ledger, 1 rue du Mail, 75002 Paris
Website	www.ledger.com
SE Firmware Evaluated Version (BOLOS)	1.0.4
Product reference	TargetID: `0x33 0x10 0x00 0x04`

The product identification can be directly processed by the End-User on the `Ledger Nano S Plus`. The following steps must be performed, as mentionned on the [UM] :

1. Power on the `Ledger Nano S Plus`
2. Enter and validate the PIN
3. Access to the **Control Center** menu by holding both buttons during 3 seconds
4. Select **Settings** and press both buttons
5. Select **General** and press both buttons
6. Select **Firmware version** and press both buttons
7. Retrieve SE Firmware version
8. Verify that SE Firmware version displayed on the screen is identical to the one identified in the previous table

To verify the TargetID number the [CheckHardwareIntegrity] is used:

1. Power on the `Ledger Nano S Plus`
2. Run the `checkGenuine` command with the correct TargetID for the `Ledger Nano S Plus`: `0x33100004`
   - `python -m ledgerblue.checkGenuine --targetId 0x33100004`
3. Script outputs “Product is genuine” or a warning in case of ungenuine product

3.6 Target of Evaluation

The Personal Security Device is an embedded platform processing securely sensitive services. The PSD includes a set of core security mechanisms (TRNG, End-User verification via the enrolled PIN, attestation mechanism, post-issuance capability). These security mechanisms combined with a simplified User Experience make the PSD usage secure and simple.

The security model created by Ledger is based on the Secure Element technology. This Secure Element embeds a set of hardware security countermeasures (for instance active shield, monitoring of environmental parameters, [AIS-31] True Random Number Generator compliant).

Nevertheless, in order to get a product resistant against high attack potential, Ledger has also implemented a set of software security countermeasures. It is the composition of hardware security mechanisms (provided by the Secure IC) and the software security mechanisms (provided by Ledger) which make the `Ledger Nano S Plus` resistant against sophisticated attacks.

The Target of Evaluation, focused on the `Ledger Nano S Plus`, is identified in the following diagram:

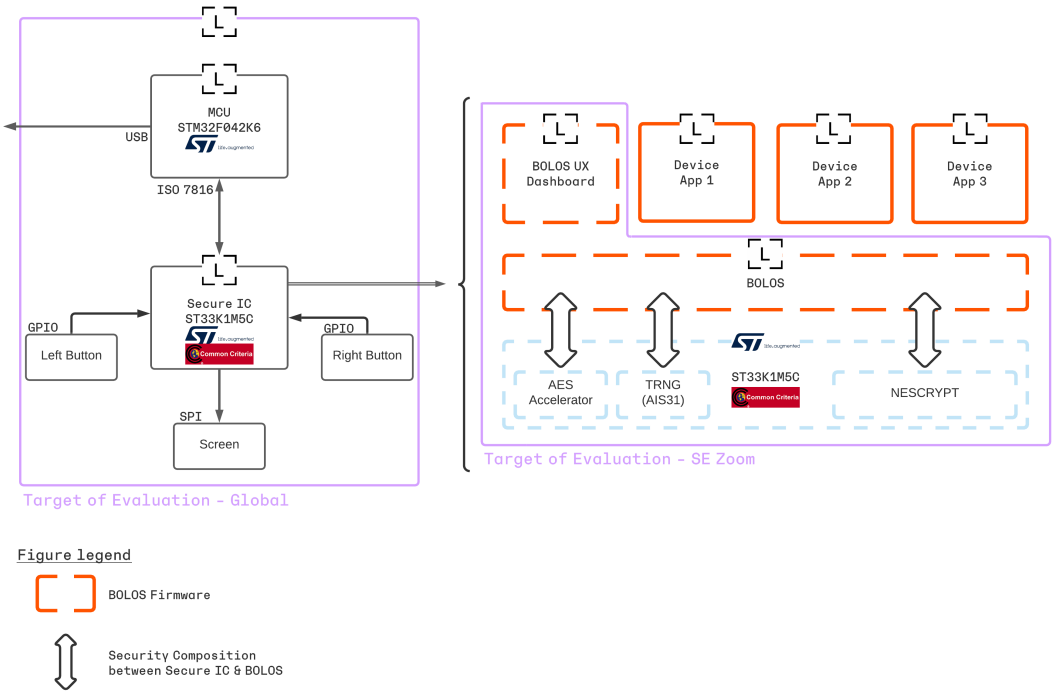

Figure 4: Target of Evaluation including a zoom on the SE

The ToE includes:

- Physical elements
  - Two buttons
  - One screen
  - One USB port
- Hardware (provided by STMicroelectronics)
  - MCU: [STM32F042K6]
  - Secure IC: [ST33K1M5C] (Common Criteria certified, [ST33_CC])
- Software (developed and secured by Ledger)
  - SEPROXYHAL firmware running on top of [STM32F042K6]
  - BOLOS firmware running on top of [ST33K1M5C] contains:
    * an OS labelled BOLOS
    * a Device App labelled BOLOS UX Dashboard

BOLOS is in charge of:

- Communicating with the outside world
- Managing peripherals (both buttons & screen)
- Performing cryptographic computation
- Storing secret data (seed, PIN)
- Offering a set of API (communication, cryptographic primitives, seed) accessible to all Device Apps

The BOLOS UX Dashboard Device App, default Device App active as soon as the PIN is

successfully verified, is:

- The entry point to select another Device App
- In charge of the onboarding phase: seed generation and PIN enrolment
- Involved in the other Device App management (installation and deletion)

The BOLOS UX Dashboard Device App ensures a UX consistency whatever the running Device App is. This Device App manages for instance buttons and the screen. Thus, this Device App also supports a third-party developer to create his own Device App.

All Device Apps (developed by Ledger or a third-party), except the BOLOS UX Dashboard Device App, are excluded from the ToE.

4 Security problem definition

4.1 Assumptions

Below is the list of assumptions:

1. The `Ledger Nano S Plus` is acquired from an official Ledger reseller (Ledger, Amazon stores)
2. The HSM is properly operated by Ledger
3. The Ledger engineering team working on firmware or HSM are competent, trained and non-hostile
4. The End-User has verified that the `Ledger Nano S Plus` has not been tampered ([Check-HardwareIntegrity])
5. The End-User only installs non-malicious Device Apps
6. The `Ledger Nano S Plus` is either powered off or locked (i.e. an End-User verification is required) when the PSD is either stolen or found
7. All techniques consisting in spying the End-User's interactions with the PSD are out of the scope. This covers for example a CCTV focused on the `Ledger Nano S Plus` and any other more sophisticated attack.

4.2 Environment Measures

Even if the `Ledger Nano S Plus` can be used within a strict environment (for instance storing the device inside a vault, signing a transaction inside a secure building), the security design developed by Ledger allows the End-User to experience the PSD in a public area. The device is architectured to provide an high assurance level to the End-User whatever the environment.

Nevertheless, with the `Ledger Nano S Plus` security model, the security is shared between the `Ledger Nano S Plus` device and the End-User. The following security rules must be fulfilled:

- The End-User **must** maintain the PIN secret
- The End-User **must** keep the recovery sheet secret
- The End-User **must** ensure that no one has access to the recovery sheet
- The End-User **must** verify transactions' details and address displayed on the screen are valid

4.3 End-User

One of Ledger's ambitions is to ensure the blockchain technology can be appropriated by all. While the solution is sophisticated, the `Ledger Nano S Plus` offers a simple and natural User

Experience. The `Ledger Nano S Plus` being designed to be a mainstream technology, it is user-friendly and can be easily manipulated by End-Users with no technical background.

4.4 Assets

As the PSD processes sensitive operations (i.e., sign transactions, manage passwords, achieve U2F authentication, ...) and stores confidential data, the following assets must be secured:

1. Random number - data
2. Secret seed - data
3. Secret Data (protected by the PIN) - data
4. PSD Access Control - operation
5. SE Firmware - data

All the assets listed above is worth of interest to an adversary and are subject to a set of threats as mentioned in *Threats*.

4.5 Threats

4.5.1 Threat Agent

The `Ledger Nano S Plus` can be considered as a sensitive device: for instance, it can be used to process some sensitive operations related to the management of the corresponding crypto assets belonging to the End-User.

One of the `Ledger Nano S Plus` features is to sign digital transactions. This signature operation, used to unlock the cryptocurrency funds located on the blockchain, involves the manipulation of the private key. The owner of this private key (the End-User) is the owner of the corresponding cryptocurrency funds.

Additionally, the `Ledger Nano S Plus` is not only an hardware wallet but also provides a set of added-value services. The Password Manager and FIDO are typical Device Apps making the digital End-User life frictionless and more secured.

Several threats are applicable to the `Ledger Nano S Plus` and can be divided into two classes:

1. Physical threats: the threat agent has a physical access to the `Ledger Nano S Plus`. This occurs when the `Ledger Nano S Plus` has been either stolen or found. The PSD's state is either powered off or locked when the PSD is either stolen or found. This PSD's state requires the PIN to get access to the sensitive services.
2. Remote threats: the threat agent has no physical access. This remote threats class is considered when the End-User's Host has been compromised. It is through this infected machine (desktop/laptop/smartphone/tablet) that an adversary will launch his attacks (i.e., signing a transaction, getting passwords).

The following section describes the main threats linked to the `Ledger Nano S Plus` related to the two threat classes.

4.5.2 Threat #1: Generating a biased or a deterministic random number

Context:

The Random Number Generator included in the `Ledger Nano S Plus` is used to:

1. Generate a Random Number exploited as a seed

2. Participate in establishing a secure channel between the `Ledger Nano S Plus` and Ledger's HSM

The `Ledger Nano S Plus`, compliant with [BIP32], is a deterministic hardware wallet. This feature indicates that a seed is generated by the device during the initialization. From this seed, the End-User has the capability to derive all Key Pairs required to manage the crypto assets accounts.

Note that this feature allows to recover the crypto assets funds if the `Ledger Nano S Plus` is lost, stolen or destroyed as long as the seed is correctly backed up (via the Recovery Sheet, see Restore mode).

The `Ledger Nano S Plus` uses the Random Number Generator not only for generating the seed but also for creating a Secure Channel between the Ledger's Secure Server and the `Ledger Nano S Plus` avoiding replay attacks.

Threat:

The entropy is the key element regarding a Random Number feature. The entropy must be ensured by a true random number. The main threat is to reduce the entropy so that it reduces dramatically the seed space. This seed's space size is 2^{256}.

Another threat is to generate a number under the control of an adversary. This number is leveraged to set-up the End-User's account by creating the crypto address. Then, the End-User's account can be provisioned.

If the sensitive number generation operation is controlled by the adversary, it is then possible to recreate the End-User's account and perform a crypto asset transfer from the End-User's account to the adversary's account.

4.5.3 Threat #2: Using an ungenuine `Ledger Nano S Plus`

Context:

Ledger is the unique manufacturer of the `Ledger Nano S Plus` device. The authenticity proves the `Ledger Nano S Plus` is only issued by Ledger avoiding some security holes related for instance to supply chain attacks. Besides, as the `Ledger Nano S Plus` is a sensitive device, it must only work as specified by Ledger. For instance, the Ledger embedded software, including not only BOLOS but also a set of Device Apps, must be executed as expected.

In other words, both authenticity and integrity of the `Ledger Nano S Plus` must be ensured.

Threat:

The main threats are:

1. Manufacturing a fake `Ledger Nano S Plus`: as an adversary manufactures a fake `Ledger Nano S Plus`, it has the full control on the device and can create malicious `Ledger Nano S Plus`.
2. Modifying the `Ledger Nano S Plus` produced by Ledger: an adversary adds malicious software or hardware to dump out sensitive data.

4.5.4 Threat #3: Bypassing the Access Control to Sensitive Services

Context:

The Ledger Nano S Plus embeds a set of sensitive services. One of them is related to the management of crypto assets. For instance, an End-User can create through his Ledger Nano S Plus a set of accounts (i.e., a professional account, an individual account, a family account) linked to several cryptocurrencies (i.e., Bitcoin, Ethereum, Ripple). The Device Apps installed on the Ledger Nano S Plus can sign transactions to unlock the funds.

Note that the Ledger Nano S Plus offers several sensitive services (FIDO, Password Manager) interesting for an adversary as well.

Threat:

The main threat is related to a stolen Ledger Nano S Plus. As soon as the Ledger Nano S Plus is stolen, a physical access to the hardware wallet is available.

This threat is also applicable remotely when the End-User's Host has been previously compromised.

4.5.5 Threat #4: Compromising the Post-Issuance Capability

Context:

The Ledger Nano S Plus includes a post-issuance capability making possible to update not only Device Apps but also firmwares (both BOLOS and SEPROXYHAL). This feature, giving Ledger an incredible flexibility, can be exploited to:

1. Add new services
2. Fix some functional and protocol issues
3. Reinforce the security of the Ledger Nano S Plus

Threat:

The main threat is to inject a malicious firmware (either SE or MCU) so that an adversary can take the full control of the Ledger Nano S Plus.

4.6 Security Functions

As raised in the previous section, the Ledger Nano S Plus can be targeted with four main threats. These threats are critical because they can compromise the Ledger Nano S Plus: deterministic random number, access to the device without End-User verification, fake or malicious Ledger Nano S Plus.

Ledger has developed appropriate security functions explained in this section to properly block each threat. It is worth highlighting that the implementation of these security functions relies on a set of security mechanisms. This security methodology of adding several security layers (defence-in-depth concept) counteracts not only straightforward but also sophisticated attacks.

4.6.1 Security Function #1: True Random Number Generator

Description:

This security function #1, labelled True Random Number Generator, aims at counteracting threat #1.

This security function is based on the TRNG embedded in [ST33K1M5C]. This TRNG, evaluated according to [AIS-31] methodology, has been successfully certified Class PTG.2.

To reinforce the entropy of the generated Random Number, Ledger has also implemented an additional software post-processing countermeasure.

Assets:

The assets related to security function #1 are:

1. Random Number - entropy - (data)
2. Secret Seed (data)

4.6.2 Security Function #2: Attestation Mechanism

Description:

This security function #2, labelled Attestation Mechanism, aims at blocking threat #2.

Ledger has implemented a solution to ensure that the `Ledger Nano S Plus` belonging to the End-User is a genuine one. To comply with this requirement, a Public Key Infrastructure (based on secp256k1 elliptic curve) has been set up: Ledger is the Certification Authority. This dedicated infrastructure, based on Hardware Security Module, is not only administrated but also operated by Ledger.

During the manufacturing process, each `Ledger Nano S Plus` initializes itself with:

1. an individual key pair generation
2. the corresponding certificate (provided by the Ledger's HSM)

Then, when the `Ledger Nano S Plus` is connected to the Host and under some circumstances (for instance a Device App, SE firmware download or MCU firmware installation), a mutual authentication between the Ledger's HSM and the `Ledger Nano S Plus` is performed.

This security function #2 relies on the following commands:

1. VALIDATE_TARGET_ID
2. INITIALIZE_AUTHENTICATION
3. VALIDATE_CERTIFICATE_LAST
4. GET_CERTITICATE_LAST

The VALIDATE_TARGET_ID and INITIALIZE_AUTHENTICATION commands initiate the mutual authentication. The VALIDATE_CERTIFICATE_LAST command is used by the PSD to authenticate the HSM while the GET_CERTIFICATE_LAST command is used by the HSM to authenticate the PSD.

At the end of this command/response sequence, a mutual authentication is achieved. Besides, both HSM and PSD have generated ephemeral keys leveraged during an ECDH to share a common secret between the HSM and the PSD.

This attestation mechanism is performed through a set of ECDSA operations as illustrated in the following diagram:

Assets:

The assets related to security function #2 are:

1. Random Number (Data)
2. PSD Genuineness (Data)
3. PSD.PublicKey (Data)
4. PSD.Ephemeral.PrivateKey (Data)
5. PSD.PrivateKey (Data)

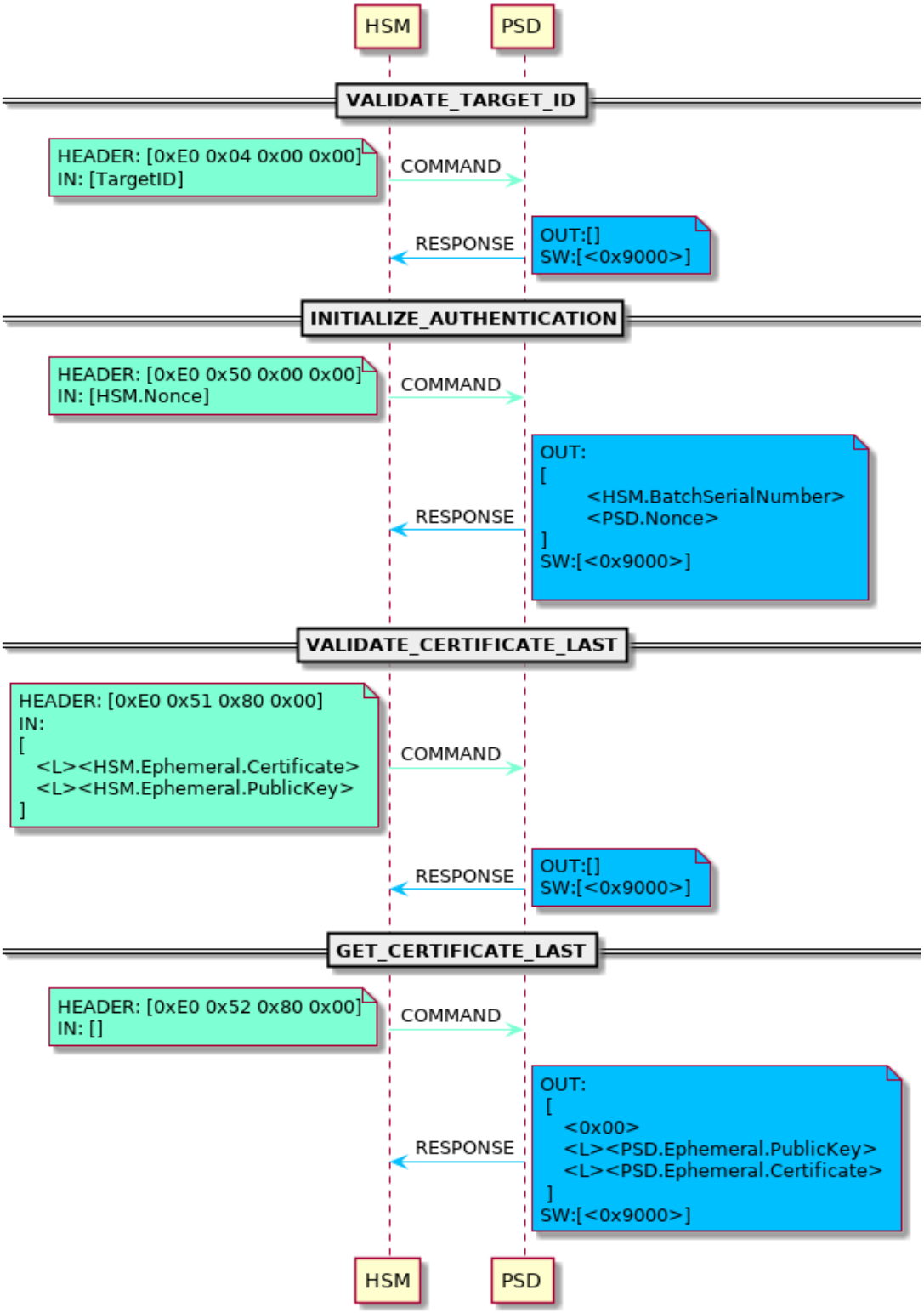

Figure 5: Security Function #2 - Attestation Mechanism

6. HSM.Ephemeral.PublicKey (Data)
7. HSM.Ephemeral.Certificate verification (Operation)
8. HSM.PublicKey (Data)

4.6.3 Security Function #3: End-User Verification

Description:

This security function #3, labelled End-User Verification, aims at counteracting threat #3.

As soon as the `Ledger Nano S Plus` is connected to a Host, the End-User must prove that he is the owner of this `Ledger Nano S Plus`. This security function #3 is the first interaction between the End-User and the `Ledger Nano S Plus`. This security function is critical because it gives access to all services supported by the `Ledger Nano S Plus`.

The End-User verification is performed through a PIN verification. As a reminder, this PIN is defined by the End-User during the onboarding stage. Also while defining the PIN he defines its length, which has to be in the following range: minimum 4 digits, maximum 8 digits.

The End-User directly enters the PIN value using the 2 buttons. This candidate PIN is then compared to the Reference PIN stored in the SE. A correct verification allows the End-User to use all services provided by the `Ledger Nano S Plus`. For instance, all cryptocurrency Device Apps are then available meaning cryptocurrency transfer is available. Note that all other Device Apps (for instance Password Manager, FIDO) are also only available as soon as the PIN verification is successfully performed.

The PIN Try Counter (PTC), whose default value is set to 3, counteracts brute-force attacks revealing the value of the PIN. As soon as the PTC exceeds its limit, the `Ledger Nano S Plus` wipes the following sensitive assets:

1. PIN
2. Seed
3. Secret Data protected by the PIN

Thanks to this security action of wiping, the `Ledger Nano S Plus` cannot be used because the current state is not operational anymore. An initialization (either "Initialize as new device or Restore a configuration") is then required (see onboarding stage).

A correct End-User verification unlocks all the `Ledger Nano S Plus` services and resets the PTC to 3.

Assets:

Several sensitive assets are used to ensure the End-User verification:

1. PSD Access Control (Data)
2. Secret data protected by the PIN (Data)
3. Reference PIN (Data)
4. PIN Try Counter (Data)
5. PIN verification (Operation)
6. PIN Try Limit (Data)
7. PIN Result (Data)

4.6.4 Security Function #4: Post-Issuance Capability over a Secure Channel

Description:

This security function #4, labelled Post-Issuance Capability over a Secure Channel, aims at counteracting threat #4.

This security function use security assets generated during security function #2 execution (mutual authentication between the HSM and the PSD).

The Post-Issuance Capability over a Secure Channel is illustrated in the following diagram:

The first commands (VALIDATE_TARGET_ID, INITIALIZE_AUTHENTICATION, VALIDATE_CERTIFICATE_LAST, GET_CERTIFICATE_LAST) performs a mutual authentication (security function #2) to ensure the HSM and PSD are genuine. Note that during the execution of the previous commands, both HSM and PSD have generated ephemeral EC key pairs. These ephemeral key pairs are leveraged to process an ECDH so that both HSM and PSD share a common secret labelled ECDH.Secret.

This ECDH.Secret is then derived to get 2 session keys:

- ENC.Session.Key
- MAC.Session.Key

These 2 session keys ensure the confidentiality and the integrity of messages (command/response) over the secure channel.

There is an additional key, labelled NENC, used to only encrypt the SE firmware. In this case, the SE firmware is encrypted twice: the first encryption is achieved through NENC while the second encryption is processed with ENC.Session.Key. NENC (an AES symmetric key initially stored during the manufacturing phase) is provisioned to the PSD during the previous SE firmware update.

After the successful processing of the MUTUAL_AUTHENTICATE command, all following commands (secured in confidentiality and integrity) are managed inside the Secure Channel.

The secure channel is designed to block typical attacks. For instance, the secure channel does not accept the same set of commands twice making replay attacks not operational anymore. Additionally, thanks to the NENC's use, the software installation is always an upgrade. It is not possible to downgrade the software version already installed on the `Ledger Nano S Plus`. This anti-rollback security protection discards all attack vectors related to install a previous software version containing a set of vulnerabilities already identified.

Assets:

1. SE Firmware (Data)
2. ECDH.Secret (Data)
3. ENC.Session.Key (Data)
4. MAC.Session.Key (Data)
5. NENC (Data)

4.7 Summary: Threats - Assets - Security Functions

4.7.1 Mapping Between Assets and Security Functions

#	Asset Name	SF#1	SF#2	SF#3	SF#4
1	Random Number	-	-		
2	Secret Seed	**I** & **C**			
3	PSD Genuineness		**AU**		
4	PSD.PublicKey		**I** & **C**		

#	Asset Name	SF#1	SF#2	SF#3	SF#4
5	PSD.Ephemeral.PrivateKey		**C**		
6	PSD.PrivateKey		**I** & **C**		
7	HSM.Ephemeral.PublicKey		**C**		
8	HSM.Ephemeral.Certificate Verification		**I**		
9	HSM.PublicKey		**I** & **C**		
10	PSD Access Control			**AU**	
11	Secret Data protected by the PIN			**I** & **C**	
12	Reference PIN			**I** & **C**	
13	PIN Try Counter			**I**	
14	PIN Verification			**I**	
15	PIN Try Limit			**I**	
16	PIN Result			**I**	
17	SE Firmware				**I**
18	ECDH.Secret				**I** & **C**
19	ENC.Session.key				**C**
20	MAC.Session.key				**C**
21	NENC				**C**

I = **I**ntegrity - **C** = **C**onfidentiality - **AU** = **AU**thenticity

4.7.2 Mapping Between Security Functions and Threats

The following table gives the full relationship between the security functions and the threats.

Security Functions	Threat #1	Threat #2	Threat #3	Threat #4
#1 True Random Number Generator	X			
#2 Attestation Mechanism	X	X		
#3 End-User Verification (PIN)			X	
#4 Post-Issuance Capability over a Secure Channel		X		X

Threat #1 is also applicable to security function #2 because a nonce is required during the attestation mechanism. Besides, as security function #4 is based on security function #2, Threat #2 is also applicable to security function #4.

5 Appendix

5.1 Use Cases

5.1.1 Onboarding

The onboarding use case is leveraged to properly initialize the `Ledger Nano S Plus`. As soon as the `Ledger Nano S Plus` is received by the End-User, this onboarding is:

1. A mandatory step: the onboarding is required to perform transactions, and
2. The first step which must be completely performed before using the `Ledger Nano S Plus`

To initialize the device, the End-User has to select one of the following modes:

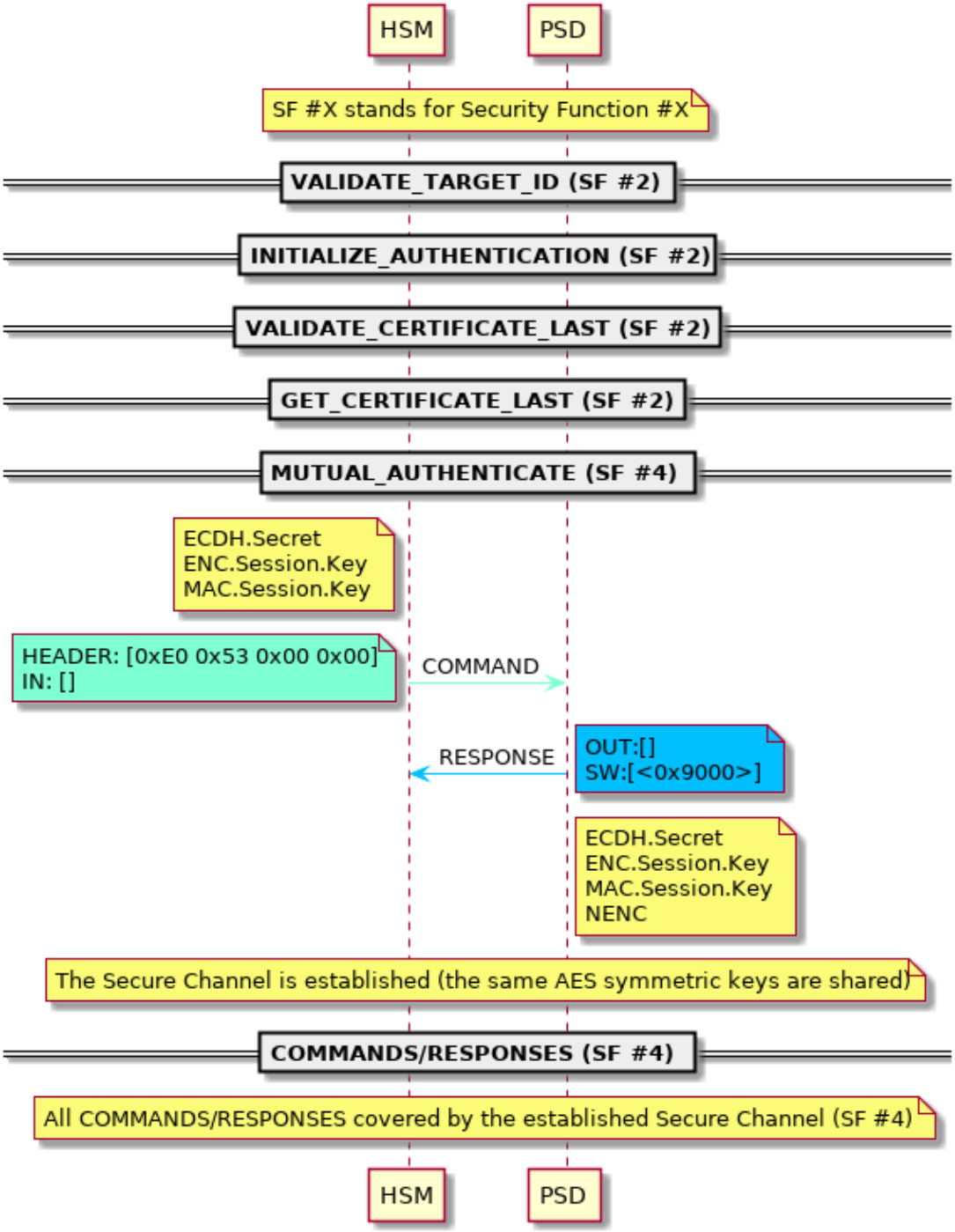

Figure 6: Security Function #4 - Secure Channel

- Set up new device mode ("Initialize as new device"), used when the End-User wants to create a seed.
- Restore mode ("Restore a configuration"), when the End-User has already a wallet and wants to restore his `Ledger Nano S Plus` (compliant with [BIP32]) to get access of his assets again.

Whatever the selected mode, the End-User has to choose a PIN code (from 4 to 8 digits long). Within the Set up new device mode, the 24-word recovery phrase is displayed word by word and must be written down on the recovery sheet. With the Restore mode, the End-User must enter the 12/18/24-word recovery phrase saved during the initialization phase. Note that during the onboarding phase, the `Ledger Nano S Plus` only generates a recovery phrase composed of 24 words.

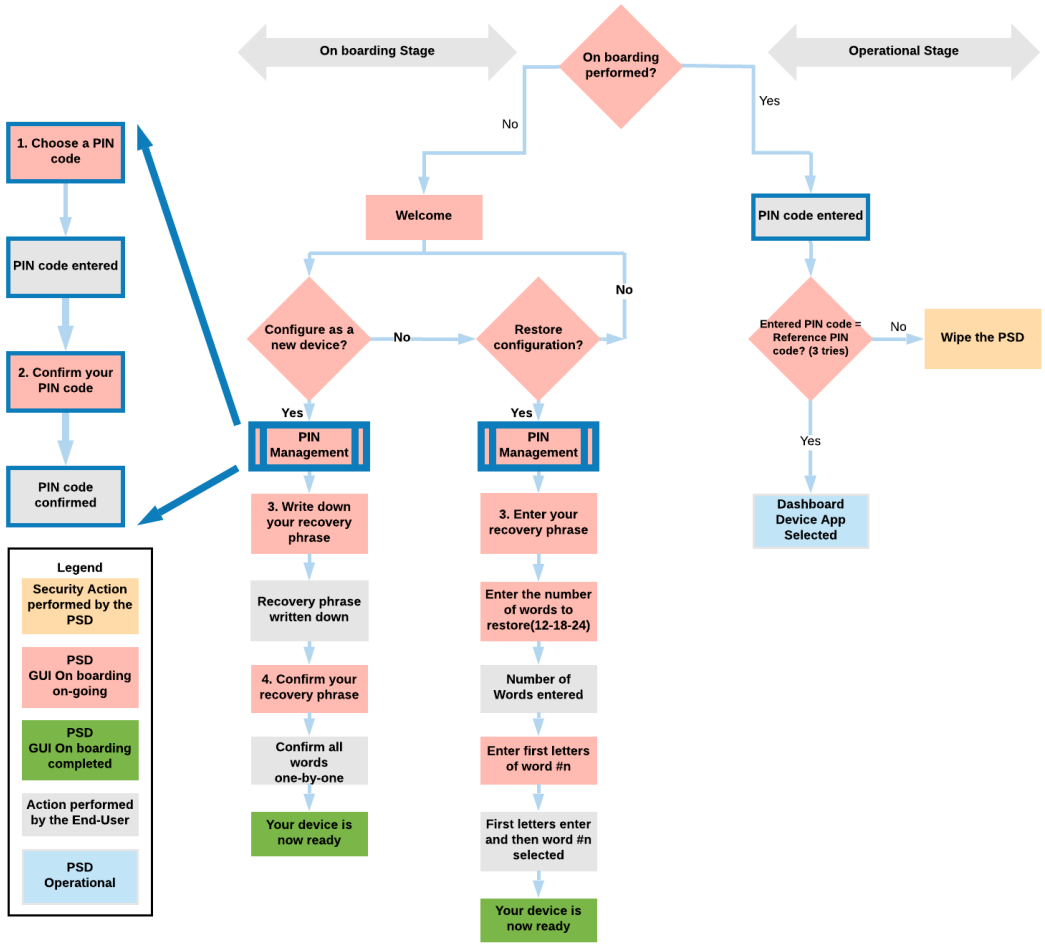

Figure 7: Onboarding Flow

As soon as the initialization is completed by the End-User, the `Ledger Nano S Plus` switches to the operational state.

5.1.2 Typical scenarios

As the `Ledger Nano S Plus` is a generic personal secure device offering a comprehensive set of security features, there are multiple use cases. For instance, The `Ledger Nano S Plus` can be used within the following scenarios (but not limited to):

1. Install the official Bitcoin Device App (in other words, signed by Ledger)
2. Perform a Bitcoin transaction
3. Perform a FIDO transaction
4. Install the latest SE firmware
5. Install a third-party Device App

All these typical scenarios are sensitive because they are manipulating sensitive assets. The `Ledger Nano S Plus` embeds 4 security functions implemented to secure the `Ledger Nano S Plus` assets.

The following table maps some scenarios with the corresponding security functions. Note that the security functions are listed in a chronological order meaning that Security Function #3 (End-User verification) is the first step, Security Function #1 is the second step and so on for the remaining security functions.

Typical Scenario	SF#3	SF#1	SF#2	SF#4
Install the official Bitcoin Device App	X	X	X	X
Perform a Bitcoin transaction	X			
Perform a FIDO transaction	X			
Install the latest SE firmware	X	X	X	X
Install a third-party Device App	X			

As illustrated by the table above, Security Function #3 (End-User verification) is always performed whatever the scenario. It is even the first security action that the End-User's must process before using the `Ledger Nano S Plus`.

As this Security Function #3 is crucial to the `Ledger Nano S Plus`, all data are wiped (including PIN, Seed and all other Secret Data) as soon as the PTC exceeds its limit. Note that the End-User has then the possibility to restore the `Ledger Nano S Plus` through the set of words written down the recovery sheet.

Depending on the use case, other Security Functions (#1, #2 and #4) may be invoked.

5.1.3 BOLOS Python Loader

Ledger has developed a dedicated tool, called BOLOS Python Loader, to communicate with the `Ledger Nano S Plus`. This tool allows to perform a set of functions. Some of them are:

1. `checkGenuine`
   This script achieves a mutual authentication between the Ledger HSM and the PSD. Firstly, the PSD ensures that the HSM is genuine, then the HSM ensures that the PSD is genuine.
2. `genCAPair`
   This script generates a Certification Authority key pair (elliptic curve secp256k1) that will be used to perform a mutual authentication.
3. `deleteApp` / `listApps` / `signApp`
   As Ledger offers the opportunity to develop some Device Apps, these scripts aim at

managing the Apps developed by a third-party.

All the functions and further details regarding the BOLOS Python Loader can be found:

- [Python Loader Installation]
- [Python Loader Exploitation]

Note Ledger has also developed another tool, labelled [LEDGERCtl], addressing the same set of features.

5.2 Acronyms

Acronym	Definition
AES	**A**dvanced **E**ncryption **S**tandard
API	**A**pplication **P**rogramming **I**nterface
ANSSI	**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation
BIP	**B**itcoin **I**mprovement **P**roposal
BOLOS	**B**lockchain **O**pen **L**edger **O**perating **S**ystem
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
CC	**C**ommon **C**riteria
DES	**D**ata **E**ncryption **S**tandard
EC	**E**lliptic **C**urve
ECDSA	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm
ECDH	**E**lliptic-**C**urve **D**iffie-**H**ellman
FIDO	**F**ast **ID**entity **O**nline
GPIO	**G**eneral **P**urpose **I**nput **O**utput
GUI	**G**raphical **U**ser **I**nterface
HSM	**H**ardware **S**ecurity **M**odule
HTTPS	**H**yper**T**ext **T**ransfert **P**rotocol **S**ecure
IC	**I**ntegrated **C**ircuit
MCU	**M**icro **C**ontroller **U**nit
Nonce	**N**umber used **once**
OLED	**O**rganic **L**ight **E**mitting **D**iode
PIN	**P**ersonnal **I**dentification **N**umber
PKI	**P**ublic **K**ey **I**nfrastructure
PSD	**P**ersonnal **S**ecurity **D**evice (synonym for the `Ledger Nano S Plus`)
PTC	**P**in **T**ry **C**ounter
RGS	**R**éférentiel **G**énéral de **S**écurité
RSA	**R**ivest **S**hamir **A**delman
SE	**S**ecure **E**lement
SEPROXYHAL	**S**ecure **E**lement **PROXY** **H**ardware **A**bstract **L**ayer
SEC	**S**tandards for **E**fficient **C**ryptography
SF	**S**ecurity **F**unctions
SHA	**S**ecure **H**ash **A**lgorithm
SPI	**S**erial **P**eripheral **I**nterface
ToE	**T**arget **o**f **E**valuation
TRNG	**T**rue **R**andom **N**umber **G**enerator
U2F	**U**niversal **2** (Second) **F**actor
UM	**U**ser **M**anual
USB	**U**niversal **S**erial **B**us
UX	**U**ser e**X**perience

5.3 Terminology

Terminology	Definition
Adversary	Person trying to compromise the `Ledger Nano S Plus`.
Attestation	One of the core security features developed by Ledger to prove by cryptographic means the `Ledger Nano S Plus` is genuine. The attestation mechanism implementation relies on a set of cryptographic protocols based on Elliptic Curve.
BOLOS	The open native Operating System developed by Ledger. One of BOLOS's features is to manage Apps (delete, install) after issuance on the field. This capability offering flexibility allows to enrich the 'Ledger Nano S Plus experience.
Blockchain	A list of blocks which are all linked together and validated via a consensus mechanism.
Command/Response	The Host and the `Ledger Nano S Plus` exchanges though a set of commands/responses (e.g. VALIDATE_TARGET_ID, INITIALIZE_AUTHENTICATION, VALIDATE_CERTIFICATE_LAST)
Consent	The `Ledger Nano S Plus` security design is strengthened by the End-User. As soon as a sensitive operation is required, the End-User must confirm the operation via the 2 buttons.
Crypto Asset	One of the digital asset whose value is saved on the blockchain
Crypto Asset address	It is a public address provided by the End-User to transfer crypto assets.This address is derived from the Public Key.
Device App	Software running in the SE on top of BOLOS. These Device Apps can be either developed by Ledger or a third-party. A Device App offers a service.
End-User	Owner of a `Ledger Nano S Plus`. End-User is defined by general public.
Firmware	Software running on top of a hardware (both MCU -SEPROXYHAL- and SE -BOLOS-).
Hardware Wallet	Physical wallet leveraging hardware to secure sensitive assets and sensitive operations.
Host	End-User machine (desktop, laptop, tablet or smartphone) running Ledger Live.
Key Pair	Includes both a Private Key and a Public Key
Ledger Live	Ledger Live a companion app running on the Host to support the `Ledger Nano S Plus` services. The Ledger Live can either be desktop/laptop/tablet/smartphone-oriented. Other third-party softwares can also be used such as Mycelium, MyEtherWallet, Coinomi.
`Nano S Plus`	State-of-the-art device designed, developed and manufactured by Ledger offering a set of secure services. In this Security Target, PSD and `Nano S Plus` are interchangeable.
NESCRYPT	Coprocessor for public key cryptography algorithm embedded in [ST33J2M0]. For instance, Ledger leverages NESCRYPT to perform some operations on the elliptic curve.
Onboarding	Set of operations (seed generation, PIN configuration...) performed during the initialization of the `Ledger Nano S Plus`.

Terminology	Definition
Private Key	Set of secret data involved for signing a transaction under the End-User Control.
Public Key	Set of data, generated from the private key, distributed and used to verify the signature.
SE Firmware	The SE firmware is composed of: BOLOS & BOLOS UX Dashboard Device App.
secp256k1	Elliptic Curve defined by Certicom Research in Standards for Efficient Cryptography ([SEC_2]).
Secure Element	A Secure Element is composed of a secure IC and a Secure Software.
Secure IC	It is an hardware embedding a set of physical security countermeasures. The Secure IC included in the `Ledger Nano S Plus` is Common Criteria certified [ST33_CC].
Secure Software	It is a software embedding a set of logical security countermeasures. In the `Ledger Nano S Plus`, Ledger has developed BOLOS and a set of Device Apps for the `Ledger Nano S Plus`.
Seed	Set of data located at the top of a hierarchical tree. In the Ledger context it refers to the master key which every application on a Ledger device uses to calculate their private keys from.
SEPROXYHAL	Firmware name running on top of [STM32F042K6].
Service	Crypto asset management, Password Manager, Second Factor Authentication are typical services offered by the `Ledger Nano S Plus`.
Wallet	Solution to manage your crypto assets (hardware wallet, software wallet, paper wallet...).
Wallet Type	There are 2 types of wallet: non-deterministic wallet and deterministic wallet.