Ledger Vault

Securing digital assets for the financial industry

Summary

About Ledger Vault

Ledger Vault is a core business unit of Ledger, a leader in security for cryptocurrencies and blockchain applications. Leveraging Ledger's industry-leading and independently-certified security technology, the Ledger Vault provides information technology infrastructure enabling financial institutions to securely control their crypto assets with a multi-authorization management solution. With a global team of more than 200 professionals, Ledger develops a variety of products and services that safeguard critical digital assets for individuals, companies, and connected devices. Founded in 2014, the company has offices in Paris, New York, Singapore, London and Vierzon.

For a long time,

individuals were self-reliant when it came to securing their monetary assets, carrying them around in their pockets or securing them in safe or secret locations. As of the 17th century, innovation in the banking sector enabled people to delegate the security of their wealth to banks which would soon become the gateway to domestic and international payment systems.

Cryptocurrencies, starting with Bitcoin in 2009, open new possibilities to store and exchange value. For the first time in history, individuals can own their assets independently without safekeeping their physical assets or notes.
At first, it required using software wallets or paper wallets with their inherent security flaws. Soon enough, start-ups such as Ledger introduced the hardware wallet. This new paradigm provided the much-needed level of security and recoverability through a user-friendly device.

In 2013, investment managers joined the crowd of crypto enthusiasts and in a few years found themselves securing hundreds of millions of dollars' worth of cryptocurrencies on hardware wallets.

The hardware wallet solution did solve some of the security challenges, yet it fell short when it came to governance in an institutional context.

Indeed, there would be no convenient and efficient way to implement a meaningful segregation of duties for their operations. This led to unrestrained investment in personal security associated with complex device management processes. In turn, this meant slow transaction processing capabilities which would materialize the most in bull and bear market phases.

Ultimately, the lack of suitability of these solutions hindered the growth of the asset class due to residual operational risk far.

At Ledger, we think that modern challenges require modern solutions. Asset Managers investing in digital assets should not be restricted operationally by cumbersome low-tech implementations.

Our solution

The Vault is Ledger's solution for financial institutions. It is the backbone of a firm's digital assets operations.

With Ledger Vault solution, firms can:

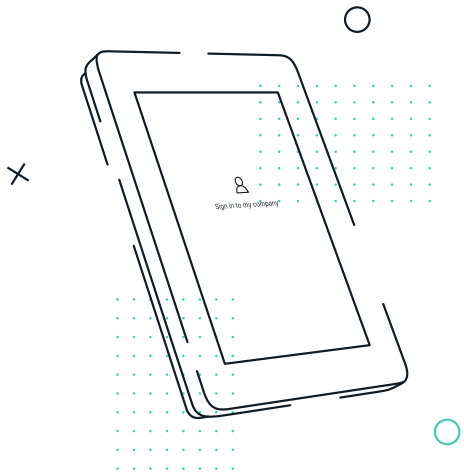
- Build their operations around a rich governance framework to reduce operational risk
- Benefit from sophisticated end-to-end hardware backed trusted execution and a made-for-purpose Operating System
- Secure and transfer more than one thousand different digital assets, quickly and from anywhere
- Take advantage of Ledger's managed services expertise to operate the Vault in line with industry standard best practices
- Maintain complete control over private keys
- Integrate our expertise within their infrastructure with Ledger Vault APIs

Key concepts

Personal security devices (PSD) and hardware security modules (HSM) are two fundamental components underpinningthe Vault platform. A glance into each element brings further insights into the Vault service architecture.

Personal security devices for Wysiwys

What-You-See-Is-What-You-Sign is the fundamental principle governing the approval of operations on the Vault platform. Users create their operations within the web browser, and confirm the accuracy of the details on a Ledger Personal Security device before the information gets sent to the HSM. Each user requires a personal security device. The PSD is one of the critical components of the security design of the platform.

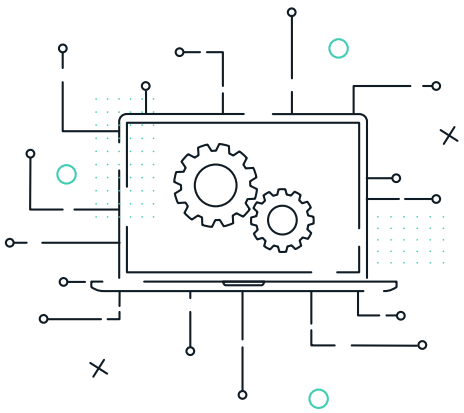


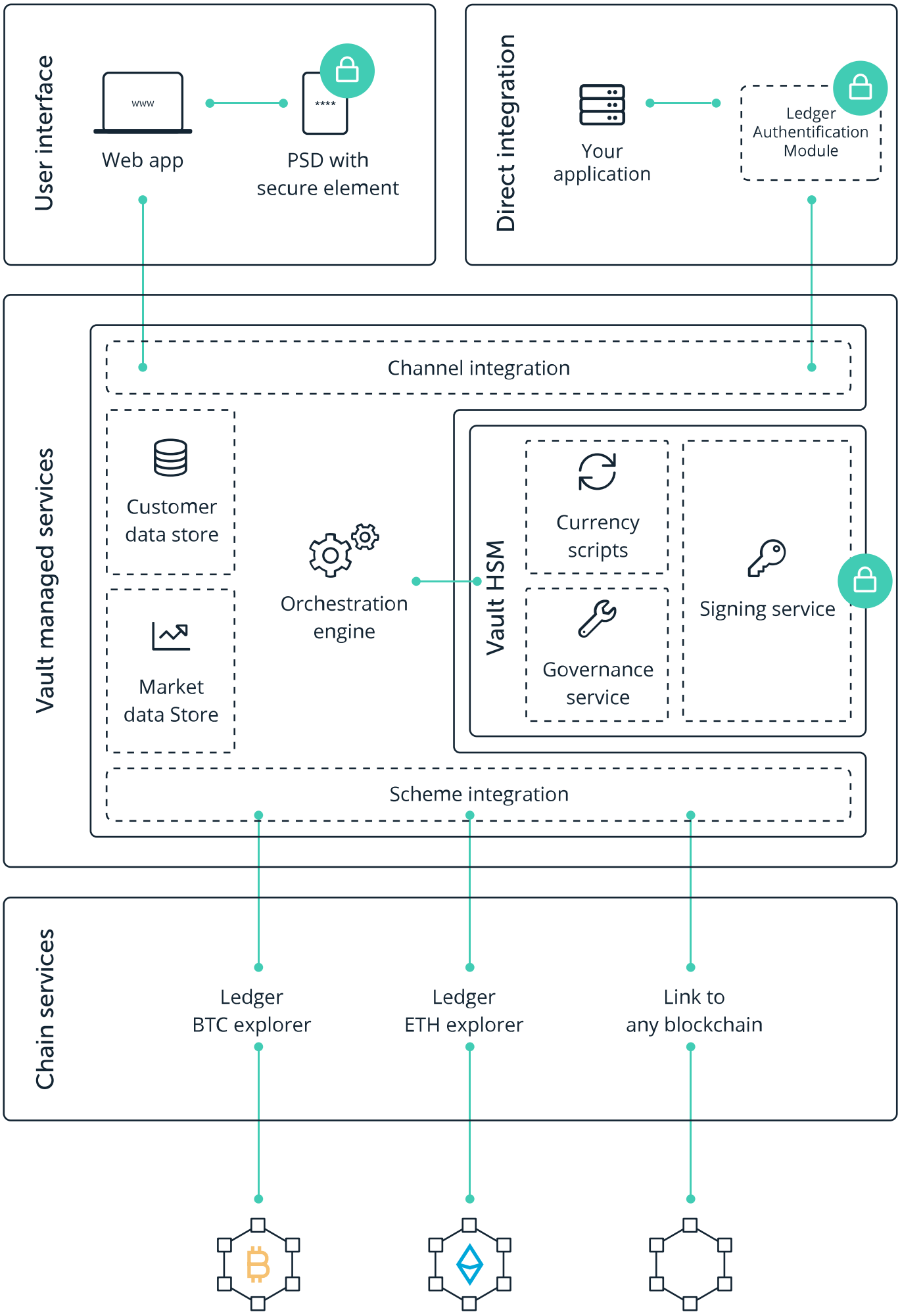
Hardware security module

The orchestration of the transaction authorisation process is managed within the secure perimeter of a hardware security module.
The hardware security module runs Ledger's proprietary operating system -- BOLOS. It protects the private keys and ensures signatures may only be performed within the context of the execution of a transaction—in compliance with the previously configured authorization flow.

Ledger Authentification Module for API

Ledger has zero access to the keys used to sign messages sent to the Vault. Maintaining this guarantee was one of our key concerns while building the Ledger Vault APIs, which led us to design an architecture based on a client-side agent: the Ledger Authentication Module (LAM). It resides on your infrastructure rather than Ledger's, the LAM is able to securely isolate the secrets that will be used to authenticate and communicate with your Vault.




User interface
www
Web app
****
PSD with
secure element
Direct integration
Your
application
Ledger
Authentification
Module
Vault managed services
Channel integration
Customer
data store
Market
data Store
Orchestration
engine
Vault HSM
Currency
scripts
Governance
service
Signing service
Scheme integration
Chain services
Ledger
BTC explorer
Ledger
ETH explorer
Link to
any blockchain

Vault governance framework

The Ledger Vault enables enterprises to implement a strong governance framework over their digital asset operations. The governance framework relies on role-based access control to accounts which can be tailored to fit the complex business processes of institutions of any size. The segregation of duties is structured around 4 user roles: Shared-Owners, Wrapping Key Custodians, Administrators and Operators.

Shared-Owners generate and safely store backups of the Master Seed. They never use the Ledger Vault platform in the context of daily operations but hold on to the Master Seed fragments for disaster recovery purposes. It is important to note that this ensures daily users never have direct interaction with any sensitive private key material.

Administrators set up and maintain the governance of all accounts throughout the platform as well as manage Operator (transaction approver) permissions. Any critical platform modifications by an Administrator must be approved by a customizable m-of-n quorum of other Administrators on the platform.

Wrapping Key Custodians generate the wrapping key which is used to encrypt your organization's HSM partition and authorize new releases. A partition is the root of all objects representing a workspace and the associated unique seed. Encryption of the partition by the Vault customer enables highly secure external storage of the information required for business continuity purpose and guarantees full independence from Ledger.

Operators oversee the process of creating, reviewing and approving transactions. On the contrary to the three other roles, Operators do not have a transversal role and can thereby only see and perform operations on specific accounts where they have been authorized by Administrators. Under the custodian use case, some Operator roles may be delegated to the custodian's customers to create a joint control model under certain constraints -- for example, requiring the end client to initiate withdrawal requests to non-whitelisted addresses in order to eliminate deposit address spoofing threats.

Transaction rules

Organizations using the Vault platform benefit from a customizable governance engine, which includes the hardware backed enforcement of rules such as multi authorisation, group based approvals, whitelists, and amount threshold limitations. These components may be combined to create flexible and scalable governance schemes tailored to any use case and to comply with internal and external policy standards.

The **multi-authorization** feature distributes the signing responsibility among multiple Operators within the institution. These operators can then be geographically distributed across the world if needed.

Approval groups allow for the creation of **complex multi-authorization** schemes based on organizational level approval flows. The rule might be set to require transactions be created by the operations team, then reviewed by and approved by the compliance team or by another operations team located in a different geographic location.

The **whitelist** enables to block outbound transactions outside a defined list of trusted public addresses.

Amount threshold limitations allow an organization to create caps on transaction sizes.

While all of these security features on their own represent improvements to existing models and workflows. Ledger has taken further steps to maximize security, scalability and availability of customer funds with its **conditional workflow features.**

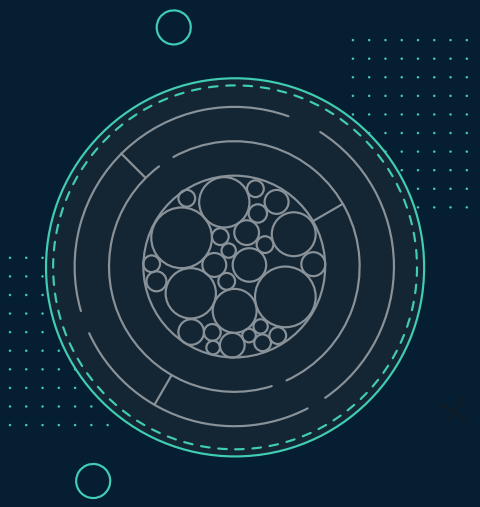
Now Ledger Vault clients can create complex approval schemes leveraging user groups, whitelists, and amount thresholds together under a **customizable conditional workflow engine**. Each wallet may have up to 4 conditional workflows allowing institutions to maximize efficiency when it comes to normal, day-to-day operations, and maximize security when it comes to transaction requests which do not meet normal criteria.

For example, the same wallet might only require 1 approval from the operations team if funds are being sent less than a certain amount and to a trusted group of whitelisted addresses. However, if that same request is made for a higher amount, then additional groups around the organization may be required to also approve; and in the event that the requested transaction is to be sent outside of the whitelist, then even more approvals from groups like compliance, senior management, or even a trusted 3rd party, may also be required.

Leveraging the flexibility of Ledger BOLOS, the ruleset is being continuously expanded to fit any organization's evolving needs.

Managed services

Cryptocurrencies unlike traditional markets do not follow scheduled business hours. Trading and transactions occur 24/7 and require support services to be highly available.



Non-critical Vault services are directly hosted with IAAS providers enabling them to leverage the scaling benefits of cloud computing. We consider as 'Criticals' the following elements: seeds, privates keys, Governance rules, signature engine and governance engine. All critical assets are hosted either within HSM powered by Ledger operating system, Ledger Blue's secure element or Cryptosteels. All Ledger hosting partners are selected to the highest standards for the management of their physical and logical access control.
Ledger applies specific security measures such as sensors to further mitigate any risk related to physical access to the HSM, preventing all attacks where a physical access is required.

Disaster recovery

Preparing for the worst is necessary in a nascent industry. Since all points of control remain fully in the hands of the institution operating the Vault platform, it is possible to recover the Master Seed in full independence from Ledger. For that purpose, the customer recovery team may use open source scripts provided by Ledger to recover the Master Seed from the input of the three 24-words recovery sheets created by the Shared Owners. Shall the Vault service be unavailable for a long period of time, assets will not be locked up. While this scenario is extremely unlikely thanks to the redundancy built in the platform, it provides further guarantee to parties willing to delegate their security infrastructure to Ledger.

Support

Ledger supports its worldwide operations from Singapore , New York and Paris sites. Trained support staff are available around the sun to ensure smooth operations.

Personal security devices for Wysiwys

Ledger obtained a pooled customized crime insurance program insuring crypto-assets for up to USD 150 million for its Ledger Vault platform led by the prestigious Arch UK Lloyds of London syndicate.

What is covered:

- Third-party theft of the master seed and private keys following a physical breach of a Vault hardware security module (HSM) in a secure data center;
- Secure transmissions of the master seed shards to the HSM as part of the client onboarding;
- Insider Ledger employee theft caused by collusion.

Security-by-design

Ledger prides itself for the usage of highly secure hardware in the components critical to the security of the Vault solution. In the hands of each Administrator or Operator a personal security device is used to interact with the Vault platform. On the back-end of the Vault platform, a hardware security module is executing sensitive operations, such as checking governance rules and signing transactions.
Unlike traditional hardware, secure hardware natively embeds advanced security protections offering protection against physical tampering. Ledger Vault is SOC II Type I attested.

> These two security devices run Ledger's advanced proprietary operating system BOLOS—standing for Blockchain Open Ledger Operating System.

Disaster recovery

The PSD enables users to generate a cryptographic secret based on the highest standards of true random number generation. The PSD access is secured by setting up a 4 to 8 digit PIN code. Three wrong inputs will erase the device memory. The PSD enables users to perform What-You-See-Is-What-You-Sign operations. Thanks to the trusted display of the devices, the user must validate the correctness of the operation to be authorized to ensure no attacks have been attempted on their local computer. Depending on user role, this pertains to: generating private key components related to cryptocurrency assets, secure storage of HSM cryptographic material, approving the creation of new rules, or approving the consumption of cryptocurrency assets.

In practice, this translates into users creating their operations within the web browser, confirming the validity of the details on a Ledger personal security device before the information gets sent to the HSM. Ledger PSD product range supports secure firmware patching. This ensures that Ledger could further strengthen security in the future or expand devices' functionalities post release.

HSM powered by Ledger operating system

Ledger's operating system for HSM is designed to provide a secure execution framework. Each application is isolated from one another and from the Operating System, offering different services to communicate with the outside world and perform cryptographic operations on user data.
User's cryptographic secrets are thereby only exposed in the context of the execution of specific applications signed by Ledger.

Cryptographic secrets are never exposed outside of the OS space.

Scripts execute Syscalls in order for the OS to execute cryptographic operations with the secrets.

The Vault HSM running Ledger BOLOS ensures that all executed stored cryptographic software and firmware follow the Vault business logic.

The HSM performs the following operations:

- Protecting and isolating the private keys related to the usage of cryptocurrency assets
- Enforcing the authorization of the usage of cryptocurrency assets following a set of dynamic rules
- Signing operations according to the governance framework

Each operation running on the Vault HSM is written as a script. Vault scripts are interpreted by the Ledger OS within a virtual machine running on the HSM, providing tenant isolation and protection against code execution exploits.

Scripts are signed and encrypted per HSM, helping to protect against reverse engineering:

- Signing scripts include the account management and matching modules which are the sole owners with access to private keys. Cryptocurrency scripts issue commands to the matching script to sign transaction data using specific algorithms. The matching script then produces human-readable data for a transaction bound to a validation device
- Governance scripts enable Admin users to set multi-authorization, amount threshold, and whitelist, and conditional approval schemes to govern accounts
- Cryptocurrency scripts manage transaction parsing logic for each digital asset

Communicating securely over the internet

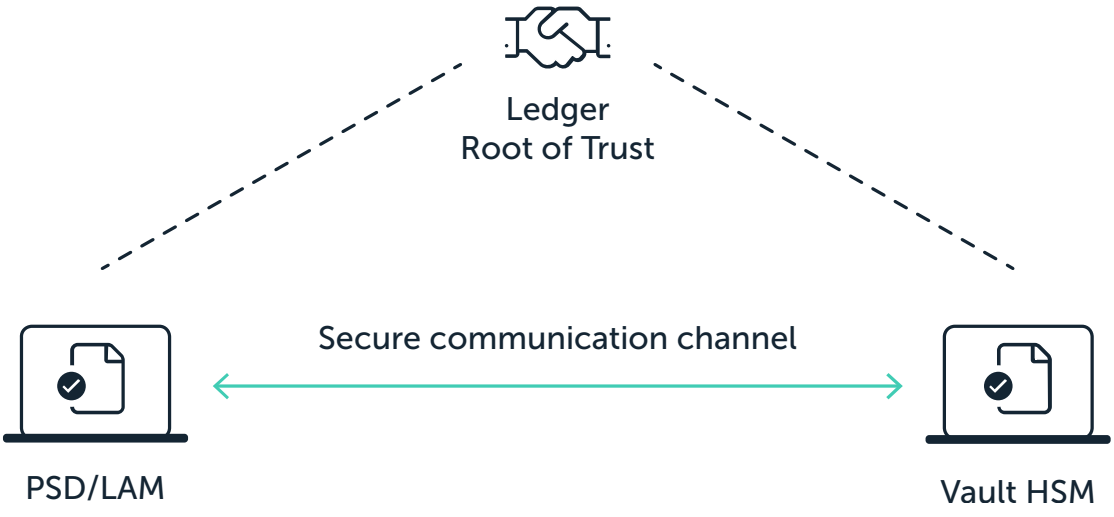
Communicating sensitive information over a public channel is a major challenge for SaaS platforms. Securing the data exchange across the internet is an endeavor that must be carefully designed and implemented in order to maintain the confidentiality and integrity of the payload.

All critical communications between the PSDs or the LAM and the Ledger Vault platform go through a **secure channel**, providing a strong protection against potential man-in-the-middle attacks.

The secure channel is based on Ledger Issuer attestation mechanism and a **Ledger Owner attestation mechanism**.

The **Ledger Issuer attestation mechanism** relies on Ledger Root of Trust. This Root of Trust is used to sign attestations for devices operated by Ledger in a similar way a certificate authority issues certificates to third parties.
An attestation is issued for all the devices interacting with sensitive data, namely the HSM and the PSD.
The **Ledger Owner attestation mechanism** enables an additional layer of validation with App-to-App authentication.
This mechanism is used by the vault PSD application to ensure it communicates with the expected script on a genuine HSM and by a Vault HSM app to ensure it communicates with a genuine PSD.

The Vault PSD owner is the customer, hence a dedicated attestation is personalized onto each client's PSD. The customer attestation in the PSD—also called the endorsement key—ensures only authorized devices can connect and send requests to the customer workspace.



Testing security

Security is a never-ending cat-and-mouse game to stay ahead of potential attackers. Ledger provides confidence in the Vault security by focusing efforts on 3 key areas:

- Continuous internal security assessments
- Periodic external security assessments
- Certifications against relevant cybersecurity frameworks

There are continuous internal security assessments performed by the Ledger Security Laboratory—the Ledger Donjon. The Ledger Donjon is a team of world-class experts with extensive backgrounds in the security and secure element industries. The team works closely with Ledger's Firmware development and hardware teams to analyze and improve the security of Ledger products.
External security assessments are performed by cybersecurity companies who specialize in the evaluation of embedded security solutions.
Lastly, Ledger is pursuing relevant security methodologies to certify the Vault. While reaching certification status is a journey that requires time, Ledger has set itself on this path to provide the needed reassurance to Ledger customers and their stakeholders.

Ledger Donjon

The Donjon team is continuously looking for vulnerabilities on Ledger products as well as Ledger subcontractors' products. This enables the Donjon to find vulnerabilities and then implement countermeasures, making Ledger solutions and the entire ecosystem more secure.

The team has a broad set of skills and applies them to expose the evaluated solutions to:

- software attacks based on reverse engineering, fuzzing static analysis or exploitation
- side channel attacks to exploit physical leakage of information during device handling
- fault attacks, perturbing the execution by putting the devices under stress such as over-heating or overclocking

The breakthroughs of the Ledger Donjon are publicly shared after the end of a responsible disclosure period.
You can get to know more about the Donjon on Ledger security blog and stay tuned by following Ledger on Twitter @Ledger

Future developments

Openness is a driving principle in Ledger's journey to become a key infrastructure provider to the digital asset markets. This translates into having a good share of the code base open source, communicating transparently on the roadmap and facilitating third-party integrations.

The Vault is to be considered as a first use case leveraging the possibilities offered by our BOLOS secure scripting architecture.
The first wave of developments was mainly internally driven with a strong focus on defining access controls, expanding the ruleset and supporting popular cryptocurrencies. All features being exposed through the graphical user interface.

Therefore, Ledger has exposed the Ledger Vault's core APIs making possible the implementation on third-party enablement. Ledger therefore plans to expose the Ledger Vault's core APIs and make possible the implementation of custom execution logic within the secure HSM environment.
New use cases can thereby be tackled building on those strong foundations.

For instance, you may integrate with the Vault APIs to build operational controls over in-house applications in the same way banking and credit card companies implement fraud platforms and sanctions filters. Transfer initiation remains fully managed by the user institution with the Vault performing the validations based on configured rate-limiter, time-lock and whitelist. In case of compromise of the enterprise environment, the operational loss would thereby be limited to the residual exposure configured on each account.

Ledger proposes as well to integrate Vault features into an existing platform in order to expand the portfolio of services. New logic can be developed and secured within the boundaries of the HSM. This approach would enable leveraging both existing features and provide an agile framework to adapt the capabilities of the platform independently from Ledger.