Redefining Security

Use Case: Finance - Digital Assets Storage

The Quantum Vault

Securing Custody of Digital Assets

Customer: Mt Pelerin

Industry: Fintech

Country: Switzerland

Mt Pelerin

Business need

Provide ultra-secure storage of digital assets

Solution

QRNG and QKD on HSM, with an application layer

Results

Most secure digital asset custody system

Business need

The wave of blockchain-based digitalization of financial assets is gaining momentum and starting to enter the focus of traditional banks and financial organizations. However, today there is a lack of institutional-grade security solutions for digital asset custody (DAC). This is a major technological concern for institutions like banks, custodians, prime brokers, cryptocurrency exchanges or any other corporations dealing with cryptocurrencies or tokenized assets.

Mt Pelerin is a Swiss company based in Geneva building a digital financial institution through a blockchain-based compliant and open ecosystem where individuals and businesses will be able to issue, deposit and trade tokenized securities straight from their bank account. They wanted a custody solution that will meet the security requirements for bank-grade security on HSMs and improve them with an extra layer of security provided by quantum technologies.

The issues were related to the generation, backup and storage (custody) of these assets.

Solution

Mt Pelerin chose to partner with ID Quantique to combine their expertise to provide state-of-the-art, bank-grade secure digital asset custody by adding an extra layer of quantum technologies on top of conventional custody solution.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

The solution combines hardware and software components. It relies on three elements:

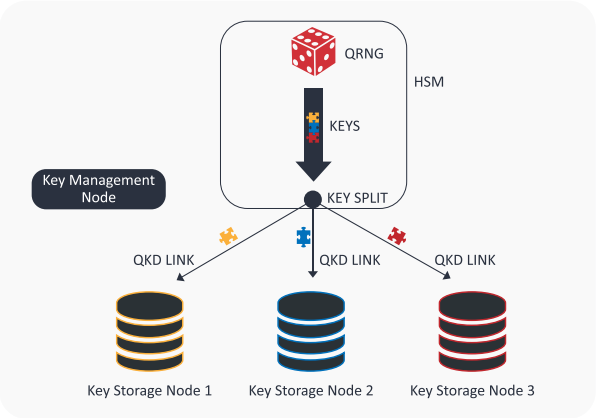
1. Generation of private keys by true random number generation, based on IDQ's Quantum Random Number Generators (QRNGs). This provides the highest security for the generated assets.

2. Custody of the assets (cryptocurrencies, tokens or other assets) in several distributed servers, or Hardware Security Modules (HSMs).

3. The assets are split into several components using a cryptographic protocol known as Shamir Secret Sharing Protocol (SSSP). Each of the component is encrypted with One-Time-Pad (OTP) and sent to a spatially separated secure location. The keys necessary for the OTP encryption are distributed by IDQ's Quantum Key Distribution (QKD). The combination of OTP with QKD ensures that the transportation of the assets is totally secure.

The main strength lies in the strict separation between the three elements: keys and assets generation, assets storage, and access to assets. Each can be optimized separately, to provide a secure solution, which matches the security requirement of the most demanding customers.

The solution is temperature agnostic (transfer from cold to hot storage in a split second) and it allows for asset backup without private keys duplication. By combining several cryptosystems (QKD, one time pad, secret sharing schemes), it ensures that the safe storage of private keys (the proof of a digital asset's ownership) is "Information-Theoretically Secure" (ITS), meaning that according to information theory, such a system cannot be hacked by an external adversary even with unlimited computing power.



Results

This solution is suitable for all types of crypto-assets, on any blockchain. It solves both issues of backup and storage. It relies on a physical optical fiber infrastructure for the physical storage of the assets and combines hardware aspects with software development. As such, it is a high-end proposition, designed to address the needs of private high net worth individuals and of various companies and financial institutions, who have a significant amount stored in cryptocurrencies. The solution can also be implemented as a turnkey solution for custodians, who wish to add, for example, a cryptocurrency facet to their business, with banking-grade security. It complements the more standard use of crypto-wallets, which are not necessarily well adapted to the storage of high-value assets.

Mt Pelerin is integrating the solution in its blockchain banking system, in order to provide its customers with the most secure digital asset custody system possible. It can also be implemented as a high-end turnkey solution for global custodians, prime brokers, crypto vaults, crypto exchanges and other institutional corporations for which the secure storage of digital assets is a vital requirement.

Mt Pelerin envisions a new era of financial freedom through a facilitated and disintermediated access to financing and investment for all.

> *This partnership with IDQ enables us to add an extra layer of quantum-safe security on top of our bank-grade custody solution and contributes to push tokenized finance forward.*
>
> **Arnaud Salomon, CEO of Mt Pelerin**

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com