



ENTRUST



Helenix Delivers Trusted Cryptocurrency HSM Wallet Based on Entrust nShield HSM

Ensure the complete security of crypto assets management by taking full advantage of the HSM-based solution

HIGHLIGHTS

Security by design. Create, store, and use private keys solely inside a highly secure tamper-proof hardware environment.

Wide range of functions. Support for different types of cryptocurrencies, transaction processing, and address generation.

Compliance with PSD2. Employ both strong customer authentication (SCA) and dynamic linking for maximum security of digital payments.

Flexible implementation. Excellent scalability and easy integration without disrupting the established workflow.

The Problem:

Increasing theft of cryptocurrencies through crypto exchange platforms

Blockchain is a new reality that revolutionized the financial market. However, it also introduced new threats and vulnerabilities that can be exploited. The main characteristic of cryptocurrency trade is its absolute irrevocability. Unlike traditional bank payments, once the transaction has been made, it's impossible to cancel or appeal to a specific authority to retract it. Due to this fact, and the rising popularity of the cryptocurrency market with an overall value of billions of dollars, cryptocurrency exchanges became an ideal target for cybercriminals. By 2020, every major crypto exchange platform reported at least one case of cryptocurrency theft. These alarming numbers raise awareness of the paramount necessity for bank-grade protection of blockchain, a solution that will be able to ensure a secure way for crypto traders to store and operate with their assets.



Learn more about our HSMs at [entrust.com/HSM](https://www.entrust.com/HSM)



Entrust and Helenix Integrated Solution

The Challenge:

Effectively applying security mechanisms from the banking industry to crypto transactions

The sheer amount of daily traffic on exchange platforms makes it nearly impossible for cryptocurrency companies to fully focus on complex security. They have to prioritize innovation and maintenance of their heavily utilized platforms, leaving the security aspect weakened by relying mostly on software-only protection. However, at the core of cryptocurrency and blockchain is cryptography. Key management is both essential and at the same time the weakest link in every digital-currency system: side-channel attacks, compromised keys, unauthorized access, etc. Software-only solutions are simply not enough to address these issues and secure the critical parts of the system. Multi-level protection built on hardware security modules (HSMs) as the root of trust, similar to the ones applied in traditional bank payments, is required to accomplish this task.

The Solution:

HSM Wallet – HSM-based security solution for crypto assets

HSM Wallet is a secure implementation of a cryptocurrency wallet designed specifically with all of the above challenges in mind. The hardware core of the HSM Wallet security is the Entrust nShield® FIPS 140-2 Level 3 certified general purpose HSM. Cryptocurrency is stored in a trusted HSM environment with robust cryptographic algorithms in effect that neither hackers nor unauthorized insiders can breach. The same applies to operations related to them; cryptocurrency transactions can be executed only after passing the multi-factor authentication built on SCA principles.

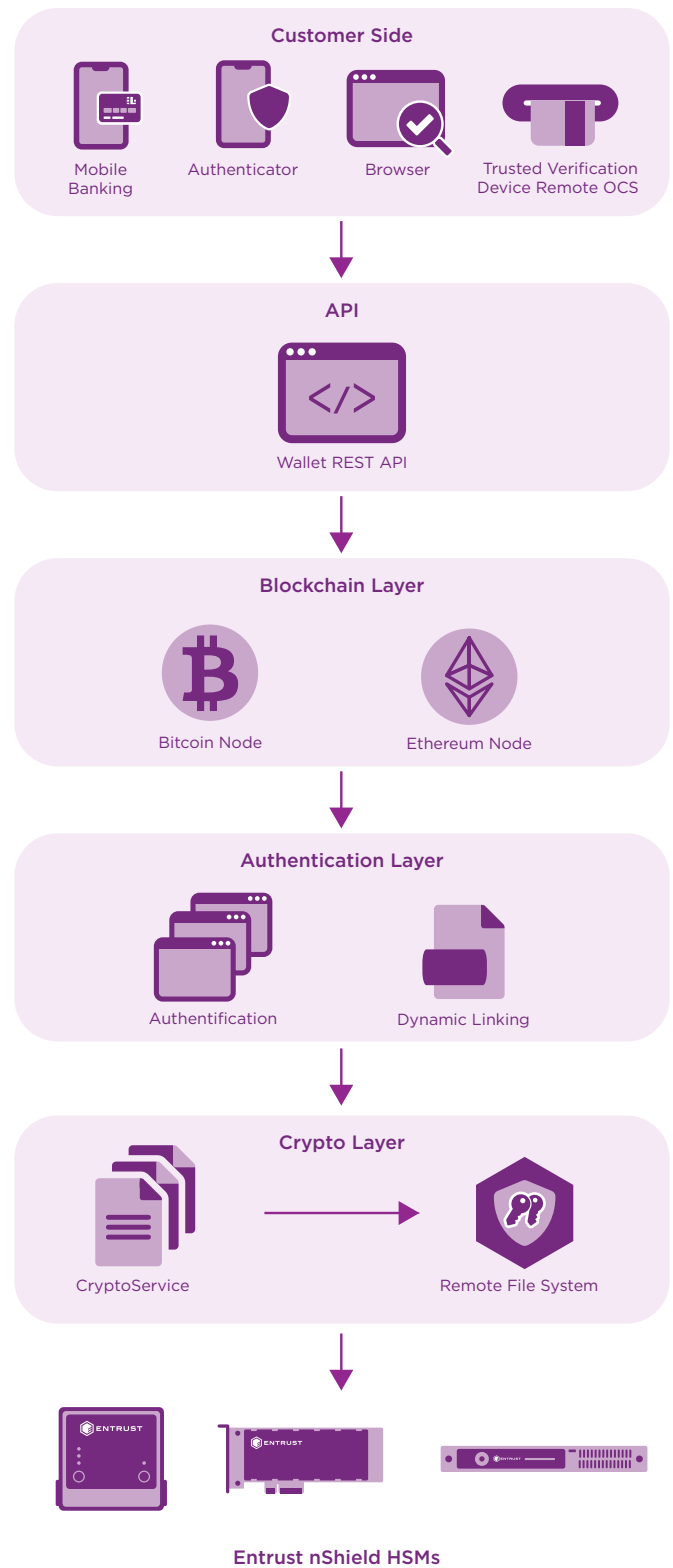
Unlike other personal hardware wallets in the market, the HSM Wallet solution is oriented toward server systems with a high number of user keys. Private keys are generated and stored encrypted in a tamper-proof environment that prevents their extraction in clear-text, even if you have physical access to the hardware. HSM Wallet focuses on the vital parts of a key management process by including additional measures of protection with the support of dynamic linking. A specific one-time code is automatically generated to confirm any initiated transaction.

Another benefit of HSM-based solutions is the fact that they provide both robust



Entrust and Helenix Integrated Solution

security and flexibility when it comes to implementation. nShield HSM architecture allows you to easily expand the capacity of the solution, or scale it down according to your current needs. At the same time, it can be integrated smoothly into an already existing digital ecosystem without disrupting any critical business processes. HSM Wallet was created to be extensively configurable and able to address a variety of specific challenges, making it the perfect blockchain security tool.





Entrust and Helenix Integrated Solution

Why use HSM Wallet and Entrust nShield HSMs?

Encryption keys handled outside the cryptographic boundaries of HSM are significantly more vulnerable to attacks, which can lead to a potential compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. HSM Wallet uses Entrust nShield HSM to securely store user keys, the most sensitive part of the Blockchain systems. Combined with SCA and Dynamic Linking, it achieves unmatched security of cryptocurrency funds. The solution enables appropriate levels of physical and logical control to be enforced over server-based applications, where software-based cryptography fails to meet the risk management targets.

About Helenix

Helenix specializes in developing and providing top-tier cybersecurity solutions based on hardware security modules as a root of trust. A dedicated team, with more than 10 years of experience in cryptography and security software development, brings innovative solutions in the area of digital payments and blockchain. For more information visit helenix.com

About Entrust nShield HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easiest-to-integrate HSMs available. They help facilitate regulatory compliance and deliver the highest levels of data and application security for enterprise, financial, and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.



Learn more at
entrust.com



ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223