cpl.thalesgroup.com

THALES

# Fressets, Inc. Implements First Japanese Offline Multi-Sig Solution to Protect Private Wallet Keys with Thales HSMs

## Summary

The crypto assets (cryptocurrency) market is vibrant once again. Financial institutions, including banks and securities companies, are expected to enter the market. Furthermore, digital assets that go beyond crypto assets, such as security tokens and stable coins, are also brought to the fore. Due to the importance of the digital assets and the industries entering the market, the enhancement of security infrastructures is gaining growing attention as the biggest requirement for market expansion.

In blockchain systems, the protection and management of private keys is the key to security. Fressets, Inc. (hereinafter referred to as Fressets), a company that provides wallet management systems for crypto asset exchanges and large-scale business operators, has created an innovative solution that relies on Hardware Security Modules (HSMs) to manage the private keys. By using Thales ProtectServer HSM, Fressets has successfully created an extremely robust and secure mechanism for key protection and management, whilst paying very close attention to the individual needs of the respective business operators.

## Selection points

Fressets provides the Fressets EWM System™ wallet service, the first Japanese cryptocurrency wallet package (domestically patented) for business operators, that enables the combined use of multiple hot wallets[1] and cold wallets[1] using multi-sig.[2] This wallet service, which already supports Bitcoin, Bitcoin Cash, Ethereum, Ethereum ERC20-based tokens, Litecoin, and XRP cryptocurrencies, is now the most widely used in Japan. Furthermore, their corporate stance and technical competence have earned acclaim through continuous security enhancements, by gradually adding support for cold wallets and multi-sig. This service is quickly becoming the standard way of managing digital asset wallets services that include crypto assets.

Meanwhile, in the market, many crypto assets continue to be leaked. The larger the market size, the higher the risk of malicious attacks. In response, Fressets decided to implement a more secure wallet using Thales HSMs. Fressets chose to store its electronic keys in the hardware-based ProtectServer HSM, increasing the security level to that of financial institution compliance standards.

Fressets

> “ While a lot of business operators have introduced and operated robust wallet systems, there are not sufficient measures implemented against physical attacks, such as the destruction and intrusion of a server room. HSMs physically protect private keys and are critical to supporting future market expansion. This technology will be a promising solution for Fressets to pursue business opportunities overseas.”
>
> – Representative Director/ CEO Yosuke Yunoki
> Fressets Inc.

[1] Hot wallet, cold wallet - A wallet is a place where a cryptocurrency is temporarily stored. A wallet that is connected to the Internet is a hot wallet, and a wallet that is kept disconnected from the Internet is a cold wallet. The Fressets EWM System™ uses paper media (QR code) for relaying information online or offline in order to allow a cold wallet to be signed completely offline.

[2] Multi-sig - Multi-sig is an abbreviation for Multi Signature, a technology that requires the signatures of multiple approvers (approval for remittance) to remit the crypto assets or other security-sensitive operations. Compared with single-sig, which uses one private key for the signature, multi-sig has a high security level and can prevent internal crimes and human errors.

In selecting a key management solution, the following items were also taken into account:

- In the event of a server being compromised via the Internet, removing the private key is not possible in principle; even in the event of physical theft, it is impossible to obtain any private keys by external analysis;
- Multiple private keys can be stored on the same ProtectServer HSM appliance, requiring approval (electronic signature) from multiple persons and thus preventing internal crime; and private keys can be safely and easily stored without the need for crypto experts;
- After comparing a variety of HSMs available on the market and hardware wallets other than an HSM, Fressets chose ProtectServer HSM due to:
  - Fressets holds a large market share, number of records, and name recognition worldwide. The fact that Thales HSMs have been widely deployed gives business operators both high assurance and trust in the product.
  - Fressets chose ProtectServer HSM due to its customization and flexibility. The Fressets EWM System enables the creation of an exclusive wallet package for each crypto asset that can then be provided as an on-premises solution or through SaaS. In order for business operators to maintain a tight security posture and reap the benefits of this solution, ProtectServer HSM was chosen due to its ability to implement and enhance functions within the secure confines of the HSM.

## Solution

In January 2020, Fressets updated the Fressets EWM System to include the secure storage of cryptography keys inside the FIPS 140-2 Level 3 ProtectServer HSM, and the benefits were soon realized. The Ethereum operators, who were previously unable to implement multi-sig on a blockchain layer with conventional technologies, successfully implemented secure multi-sigs in a completely offline environment using a ProtectServer HSM. Additionally, Fressets used the threshold signature technology that generates an electronic signature, by allowing multiple approvers to communicate with each other without publishing their respective key shares when no private key is restored. By successfully using this threshold signature technology on the Thales HSM, Fressets achieved a very secure multi-sig for cold wallets solution in a completely offline environment.

As a result of the integration, Fressets has seen an uptake on inquiries for the ProtectServer HSM-enabled Fressets EWM System from banks, security companies, and other financial institutions attempting to create a trading system that includes a wallet system, as well as the operators who have already introduced the service and are considering enhancing the functions. The Fressets security infrastructure is now well positioned to expand the crypto asset market size and the entire digital assets that are managed by blockchain.

### Issues

- The crypto assets market has been revitalized. As the market expands, the risk of security threats increases; therefore, security needs to be enhanced.
- Many business operators do not take sufficient precaution against physical attacks, such as the destruction of a server room.
- In addition to the wallet management services that have been gradually enhanced for business operators with cold wallet and multi-sig, HSMs should be supported to defend against possible physical attacks and to achieve security equal to the level of the compliance standards followed by financial institutions.

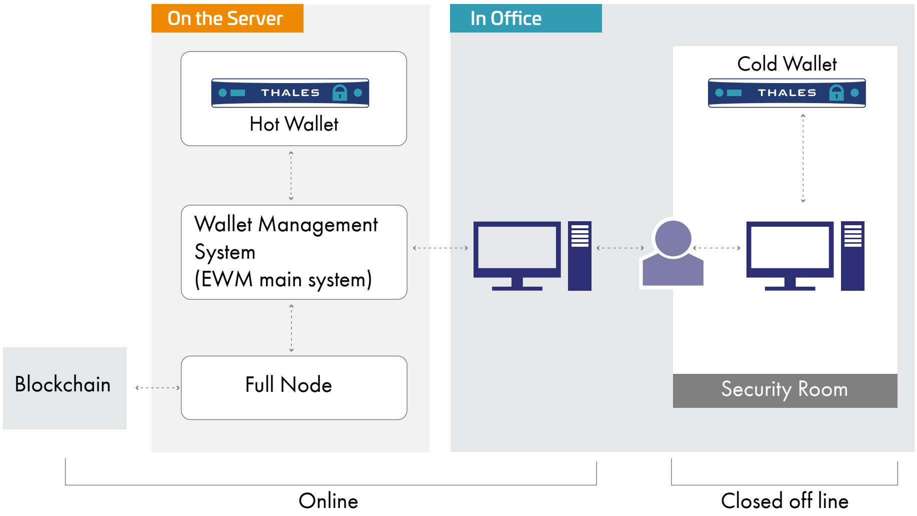
### Solution

- The function has been enhanced so that private keys can be managed using a ProtectServer HSM, which had never been achieved by wallet management services for business operators.
- A robust mechanism for key management has been developed using the customizable ProtectServer HSM while paying very close attention to the individual needs of the respective business operators.

### Advantages

- Security at the financial institution compliance standards level has been achieved for the management of private keys by wallet management services.
- Thales HSM's are widely recognized worldwide with many successful implementations including financial institutions. The high-assurance security levels are very likely to satisfy business operator requirements.
- Business operators can now easily customize functions to meet business needs, benefiting from the flexibility while maintaining security.
- Development was completed within the planned period of time, the enhanced functioned worked as expected, and the well written documentation added to the project's success.
- The use of an HSM led to the successful implementation of multi-sig in a completely offline environment for Ethereum, where conventional technologies had not enabled multi-sig to be implemented on a layer lower than the blockchain.
- There are many inquiries for the solution from banks, security companies, and other financial institutions interested in entering the market. Fressets is now best prepared to expand the size of the crypto assets market.

## HSM use case in Fressets EWM System



ProtectServer HSM safely stores private keys in a cold environment while linking to the hot wallet where encryption, digital signatures, and other services are processed at high speed.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

© Thales - January 2021 • EH V8

> cpl.thalesgroup.com <

**Contact us –** For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us