5M HOLDINGS

Unlocking Wealth from the Blockchain for Everyone

5M White Paper

Token Security Scheme (TSS) incorporating

Distributed Hardware Security Modules (DHSMs) for Crypto-Currencies Key Management System (CKMS) in SecureCryptoVault within Enhanced Payment Card Industry (EPCI) Certified Facilities

4 October 2017

Version 5.5.11

http://www.5M-holdings.com

EXECUTIVE SUMMARY

The attacks on exchanges and platforms/repositories for coins and keys storage have resulted in massive losses as shown in the MtGox incident, and with a growing list of exchanges shutting down as a result of such massive theft and joining the infamous "Blockchain Graveyard" list. The nature of these attacks are varied, and may involve direct attacks, DDoS attacks, phishing from stakeholders, data theft etc. As such, there is an immediate and dire need for a complete relook at how digital keys are properly secured and managed and how all blockchain technologies can be properly stored and protected so as to completely minimise the theft of crypto-assets and any other digital assets, whether such are held personally, by corporate repositories or otherwise

Our cyber security experts' in depth experience and knowledge in the payment and banking industry's (PBI) digital key management have revealed critical findings that could be applied to the crypto-currency eco-system. We noted that major global institutions have been implementing Hardware Security Modules (HSMs) for decades to protect their users' and customers' assets successfully. In a decentralised crypto-currencies eco-system, our proposed Distributed HSM (DHSMs) within our revolutionary Token Security Scheme (TSS) and its enhanced features and applications, aim to properly and fully address the existing security gaps for the crypto-currencies eco-system with the aim of arresting any attacks (whether simple, complex, professional or otherwise) on any exchange or facility storing such digital assets.

Our team aims to implement the TSS so as to present the PBI best practices to the crypto-currencies eco-system. The DHSMs infrastructure will be set up within the Enhanced Payment Card Industry (EPCI) security compliant facilities in geographically dispersed locations and regularly audited by certified professionals to ensure up to date compliances. These DHSMs will provide a safe "Vault", namely SecureCryptoVault, with a proper Crypto-currencies Key Management System™ (CKMS) and procedures to mitigate and wholly minimise the risks of such storage and provide a safer environment for all stakeholders in the crypto-currencies eco-system, as well as enable a timely and secure access to the digital.

Our proposed TSS will allow all crypto-currencies stakeholders to safeguard their digital assets effectively and leave a lasting legacy for their future generations.

TOKEN SECURITY SCHEME

THE HISTORY/BACKGROUND

Wherever there is recognized value stored in a repository accessible over a network (such as in the case of a crypto-coin exchange), there will always be attempts to steal such value. The fact that current technologies are based largely on ad-hoc systems, where they do not fully protect the stakeholders in a systematic and consistent manner, and coupled with the dramatic increase in the value of crypto-coins has attracted hackers' attacks on the exchanges due to their potentially large rewards. Examples of high-profile and successful attacks (and at times, blatant theft) on coin repositories (whether these are exchanges or otherwise) include the following:

- 2011: Allinvain - a personal member of the BitcoinTalk forums who lost a reported 25,000 bitcoins from a hack;
- 2012 & 2014: Mt Gox - the well-publicized breach in security at Mt Gox which caused the price of Bitcoins to fall dramatically and it was estimated that MtGox was attacked 150,000 times per second in the days leading up to its collapse in 2014;
- 2012: Bitcoinica - the exchange was successfully hacked twice in a matter of months which eventually brought the entire exchange down;
- 2013: Inputs.io - the online wallet services was brought down by two breaches with 4,100 Bitcoins being stolen;
- Other repositories suffering a successful breach in security and eventual theft include Picostocks, Cointerra, Flexcoin, Poloniex, Bitcurex etc.

Needless to say, the security of keys and tokens (whether these reside in individual repositories or institutional repositories) continue to be threatened on a regular basis. The most recent example (as at the time of writing) occurred on 4 July 2017, where it was reported that the largest bitcoin and Ether exchange in South Korea by volume, Bithumb, was hacked through the use of compromised accounts with monetary losses reaching billions of won. Apparently, this was largely due to inappropriate key management storage and security procedures, with users inadvertently revealing their keys and personal information to attackers - a common human error, one of numerous errors which our proposed solution serves to solve.

In the Blockchain Graveyard, the list of Bitcoin exchanges which have been successfully hacked into and/or stolen from continues to grow constantly. This is adversely affecting the general public's trust in the crypto-currencies eco-system, and correspondingly, the prices of these crypto-assets. The drastic volatility in market prices of tokens is made worse whenever news of another exchange/repository being stolen from is announced. With our solution, it is our aim to ensure that the additional security rendered to customers will lessen such extreme volatility in token market prices and trading volumes, and serve to contribute to a more stable market.

Currently, Blockchain-based systems typically rely on software cyber-wallets to store digital keys for their digital assets. However, because these keys/assets are residing on the network servers, they are often vulnerable to network breaches, as shown in the examples above. The fact that the value of these digital assets has increased has also led to a corresponding increase in hacking attempts (whether successful or otherwise). Breaches of this sort could be prevented with best practice security approaches, including the utilisation of HSMs, which the banking institutions, telecoms, credit cards issuers and governments have been relying on for decades in order to store encrypted assets, personal pins, transactions codes and digital keys. From our research and reviews of the various crypto-currencies exchanges, we note that the only mission critical industry which is not using HSMs is the Bitcoin exchange industry (with the exception of Gemini).

Further, a common method to automate payouts and transfers is through the utilisation of hot wallets which are controlled through APIs. Activating the automation process within these wallets requires the keys to be live and is therefore inherently vulnerable to possible hacking and cyber-theft. It is noted that these hot wallets' security architectures are based on ad-hoc solutions built around off-the-shelf hardware, with no recognised security standards applied to the wallets. This means that the wallets are wholly uncertified with respect to security standards such as the Common Criteria or FIPS 140. On the other hand, cold wallets like paper wallets and hardware wallets are off-line and are not susceptible to online threats. However, the physical security of these devices varies greatly and is also susceptible to theft and damage by fire or natural disasters.

These risks that the crypto-currencies community has somehow not properly addressed could impair the proper growth of stakeholders' assets, and consequently, bear an impact on the wealth of future generations. This is especially frightening in situations where private keys are improperly stored or lost, and cannot be recalled, resulting in the unnecessary loss of their respective coins and value.

In conclusion, and in light of all the common risks highlighted above, there is a critical need for a more stringent security regimen within the crypto-currencies eco-system. Our solution to implement TSS that incorporates a robust CKMS with DHSMs residing within EPCI certified facilities instead of just relying on simple server architecture and/or uncertified wallets to safeguard these critical keys and digital assets.

THE SOLUTION

TSS with DHSMs and CKMS residing in EPCI certified facilities

A Hardware Security Module (HSM) is a physical computing device with a crypto-processor that generates, safeguards, protects and manages cryptographic keys and provides secure execution of critical codes. These modules come in the form of a PCI card or an external device that is directly connected to the network. This is further enhanced with the PCI Data Security Standard which is a set of security standards designed to ensure that all companies that process credit card information maintain an effective and secured environment. For example, the keys stored in the Thales DHSM architecture cannot be extracted or used except under a highly controlled protocol. The new Thales solution is based on the widely used nShield HSM which creates a simple path to large-scale commercial use of Blockchain technology. This latest technology development provides the same kind of physical security that banks have relied on for decades to keep money and transaction records safe from cyberthieves. The developed HSM solution makes it extremely difficult if not impossible for digital keys to be misappropriated because they are stored in physical isolation from IT networks and are designed and built with highly sophisticated, deterministic security mechanisms.

Many security-conscious institutions rely on HSMs to safeguard and manage their digital keys and protect assets like ATM machines, mainframe access and operations, point-of-sale (POS) machines as well as to verify and sign SWIFT messages. Basically, they are used in virtually any application that requires secure and verified digital signatures. For example, HSMs in a bank's data centre, are used to validate your PIN when you withdraw cash from an ATM, or validate the transaction cryptogram when you purchase goods at a merchant POS terminal. In these cases, only the HSMs under the bank's control have access to the correct keys to perform the secure processing.

The HSMs have built-in anti-tampering technology to wipe clean any confidential information in case of one or more physical breaches. Their architectures are designed with secure crypto-processor chips and various active physical security measures to alleviate and effectively mitigate side channel attacks or bus probing. These devices are heavily used in the banking, governments and institutions where critical confidential information must be protected and have been successful in their roles to mitigate and prevent any successful hacking from happening. An analogy of the information flow, key management activities and the HSM applications is illustrated in Figure 1.

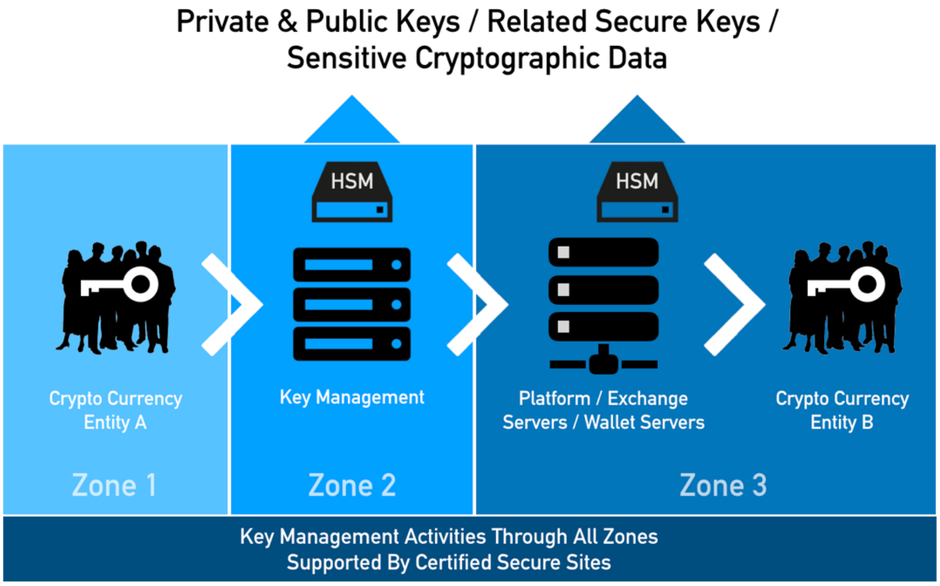

Private & Public Keys / Related Secure Keys / Sensitive Cryptographic Data
HSM
HSM
Crypto Currency Entity A
Key Management
Platform / Exchange Servers / Wallet Servers
Crypto Currency Entity B
Zone 1
Zone 2
Zone 3
Key Management Activities Through All Zones Supported By Certified Secure Sites

Figure 1: Key Management Activities within a Crypto-currencies Eco-system

In order to enhance the security features and minimize the possibility of a successful attack for the crypto-currencies eco-system, our team of cyber-experts advocate a new project and standard (called the Token Security Scheme [TSS]) to bring the best practices from the Payment Card Industry, which will be further improved upon and called the EPCI Standards. Our proposal allows the flexibility for our customers' and stakeholders' to have their private keys safely managed with the HSMs that are housed within our 168 partners' network of PCI certified facilities. Each of these facilities acts as a 'hot standby' for any and all of the others in times of crisis as a means of business contingency management for our customers. These DHSMs, coupled with our proposed architecture, makes it extremely unlikely for any hacker to successfully extract any desired master seed.

Our multi-layered approach in security implementation presents a higher barrier and drastically increases the difficulty for hackers to achieve any success by a few orders of magnitude higher when compared with "just" taking control of a full IT architecture. Figure 2 shows the locations of some of our DHSM facilities network that stakeholders could tap into across the continents and geographical areas.

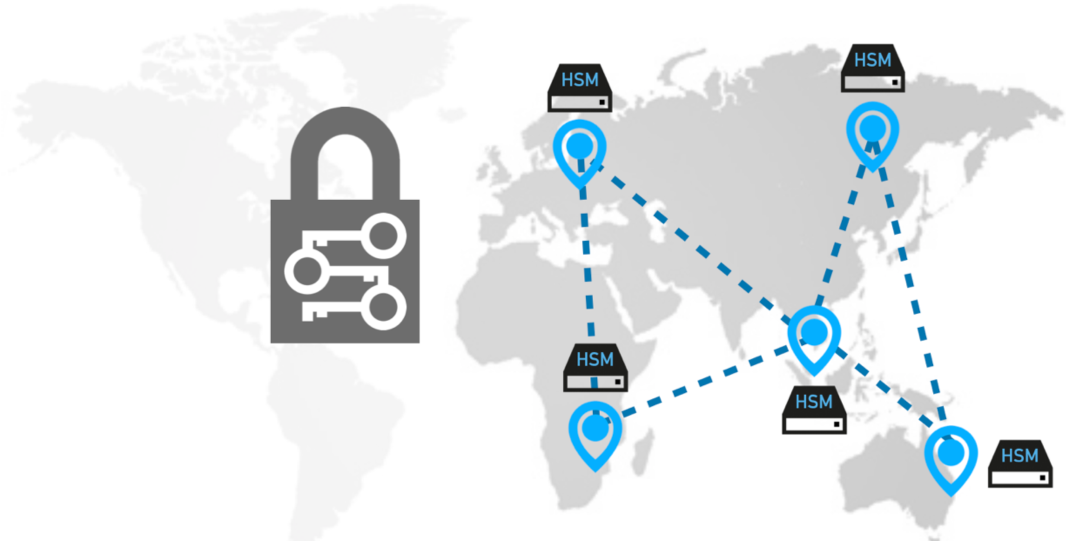
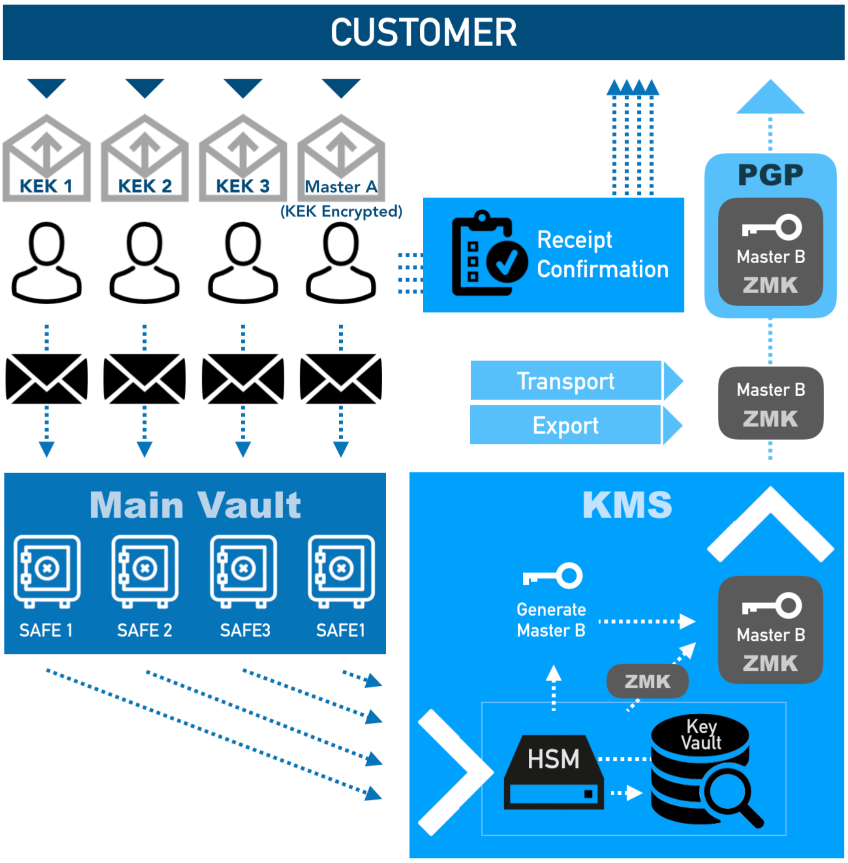


Figure 2: TSS network of Geographically diversified EPCI certified sites with DHSMs

For crypto-currencies, the private key is a critical asset where the person who has access to the key shall also have full control of the asset. Thus, private key safety and management are of the highest importance. Figure 3 shows how the keys in a crypto-currency transaction are generally transmitted, encrypted, processed and managed.



- Defined procedures and instructions
- Documented roles and responsibilities
- Standard forms for key handling

Figure 3: An illustration of the Key Management process of a Crypto-currency transaction

Our team's reviews of various exchanges found that currently, most of the crypto-currencies exchanges and their related entities do not have a standard and effective key management system that is equivalent to the PCI compliance standard. Most of them are based on ad hoc systems which are open to attack by malicious hackers. They are also software based and not hardware based systems with dedicated HSM (which is a common PCI practice and standard). Incidents like the raiding of Mt Gox highlights the dangers of deploying such ad-hoc security systems and we advocate for an enhanced security feature of the Crypto-currencies Key Management System (CKMS) to eliminate the recurrence of similar incidents. Figure 4 shows the various key management modules within the crypto-currencies eco-system.

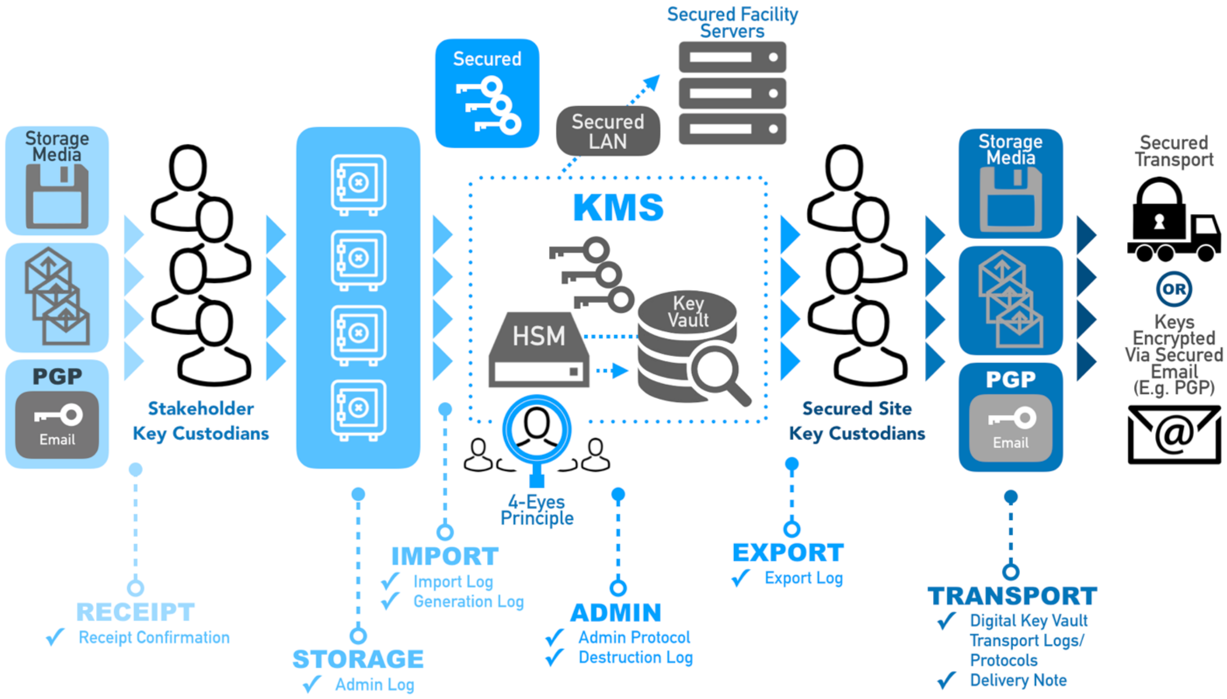


Figure 4: KMS within the crypto-currencies eco-system.

Within the CKMS, we will develop and implement a hybrid version of the combination of Secret Key and Public Key algorithms where it will fulfil the requirements of Symmetric cryptography for fast processing and Asymmetric cryptography for large network.

The robustness of our proposed CKMS is further enhanced with regular audits conducted by EPCI certified auditors to ensure full compliance to the EPCI standards at all time. This is necessary in order to avoid human error and ensure that even the best of security technology is carefully audited within its internal processes. This audit process is clearly illustrated in Figure 5.

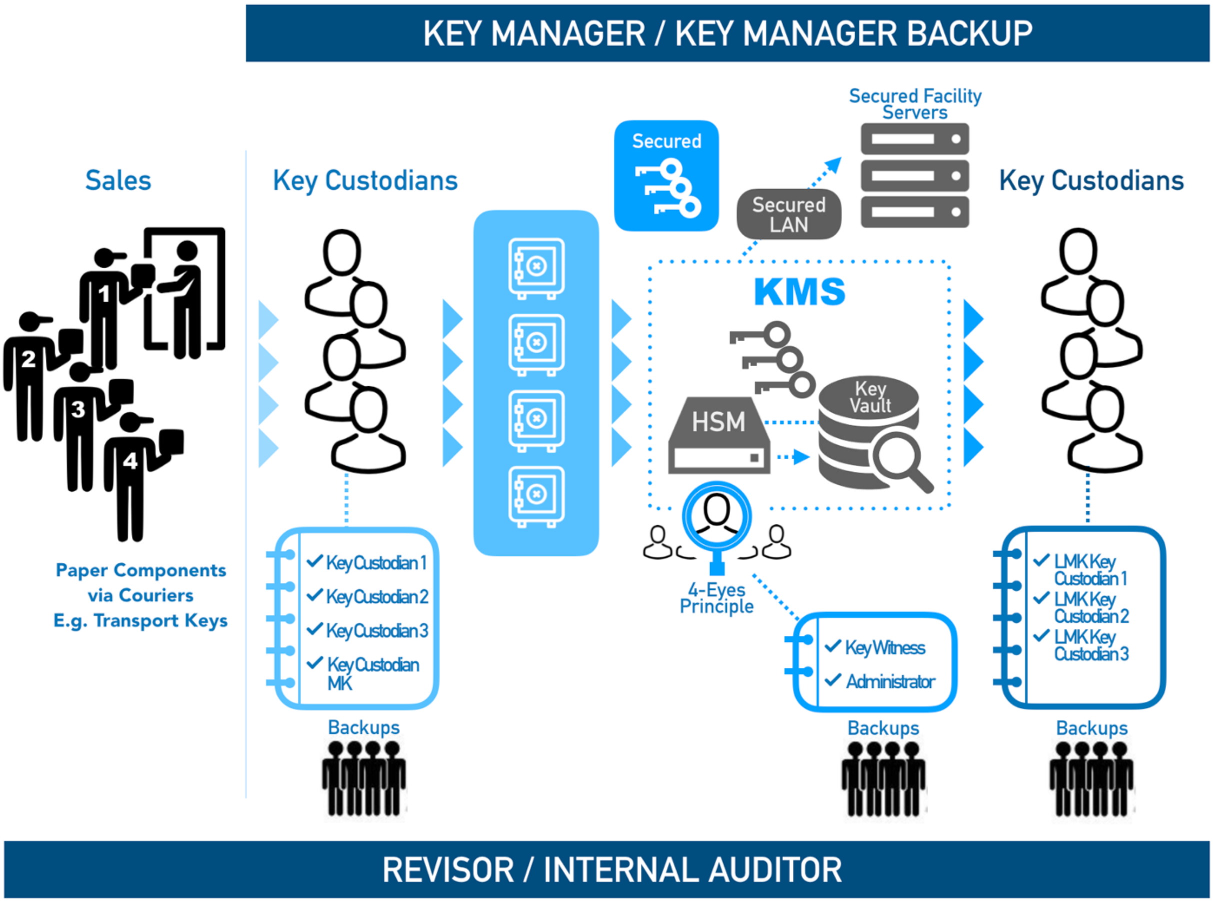


Figure 5: CKMS robustness reinforced by regular certified EPCI audits

The Design Patents Protections

Our proposed security features, enhancements and distributed architectures are in the process of being drafted and filed for patent protection. It is our intention to eventually license these patents to third parties who wish to apply these inventions to their solutions/structures/processes or for further development of the platform's security or to tie up with financial institutions with the aim of developing future implementations within the FINTECH landscape.

The Benefits

Our TSS solutions allow for customers' crypto-currencies to be secured within our network of DHSMs housed inside EPCI-certified facilities across the globe, thus ensuring security and a legacy of wealth for future generations. This will ensure that not only can we safely develop and integrate the crypto-currencies uses within the traditional financial and card payment industries, but also help to establish the newly enhanced standards for future crypto-currencies eco-system.

Some of the benefits of our proposed DHSMs include:

a. **Keys are stored within secured DHSM boundary:** the keys always live inside the secured, certified EPCI and DHSM boundaries.
b. **Tamper–resistant hardware:** FIPS 140-2 Level 2 and 3 certified DHSMs are tested to stringent standards.
c. **Sophisticated cryptography:** DHSMs use a certified, cryptographically secure random number generator to create keys to provide superior quality keys.

Institutional and Ultra High Net-worth Individuals (UHNWI) holding millions in crypto-currencies would rest assured that their assets would not be easily stolen, simply because (a) their private keys are generated by and securely maintained in high security wallets instead of on vulnerable platforms with software wallets, and (b) these physical wallets are secured within EPCI-Standard facilities; and (c) all security processes are stringently applied and subjected to regular professional audits.

Future Use-Cases

Our proposed TSS network of DHSMs within EPCI certified facilities with thorough CKMS procedures will provide a robust, safe place for long term storage with digital assets given the same treatment and security as many real word assets. This level of security encourages a host of use cases to be developed in many industries (including the traditional financial industry) to leverage on the power of Blockchain technology.

Our network of partners, including Mr. Uwe Martin Wittig, will work jointly with us to develop additional safety and security features for authentication and identity verification to provide an even safer and more convenient way to carry out financial activities online with greater privacy.

We intend to further develop enhanced security applications and integrate them with physical crypto-currency wallets, payment cards, crypto-currencies exchanges for safety redundancy. Eventually, as a premium, we will create a SecureCryptoVault for the fund management industry, family estate offices and UHNWI.

Our solution could also be used for the management of cold wallet keys and for keys recovery purposes as shown in Figure 6.

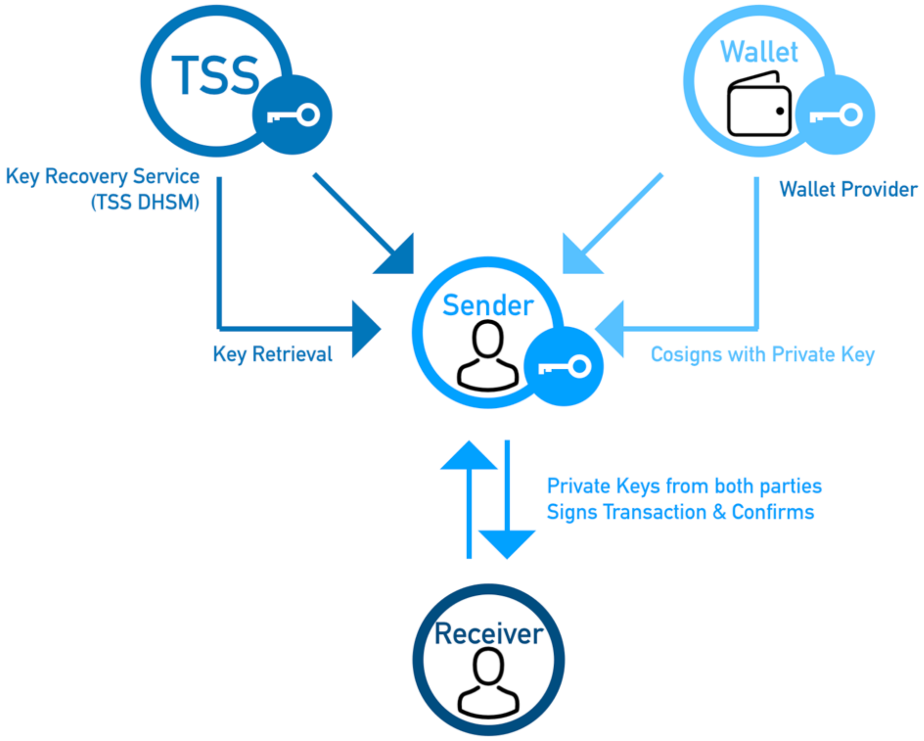


Figure 6: Application of TSS in cold wallet key recovery

Our ultimate objectives are to integrate our proposed TSS, DHSMs, EPCI, CKMS and SecureCryptoVault with the physical wallets and payment cards to be built with safe redundancy features and other more advanced features with different categories of users' privileges. With a more secure environment made possible by our proposed TSS (which will be implemented in a systematic and holistic manner) within the Blockchain eco-system, this, in turn, opens doors to other use-cases limited only by our imaginations.

The Roadmap of TSS Implementation

Our roadmap in developing the TSS is illustrated in Figure 7.

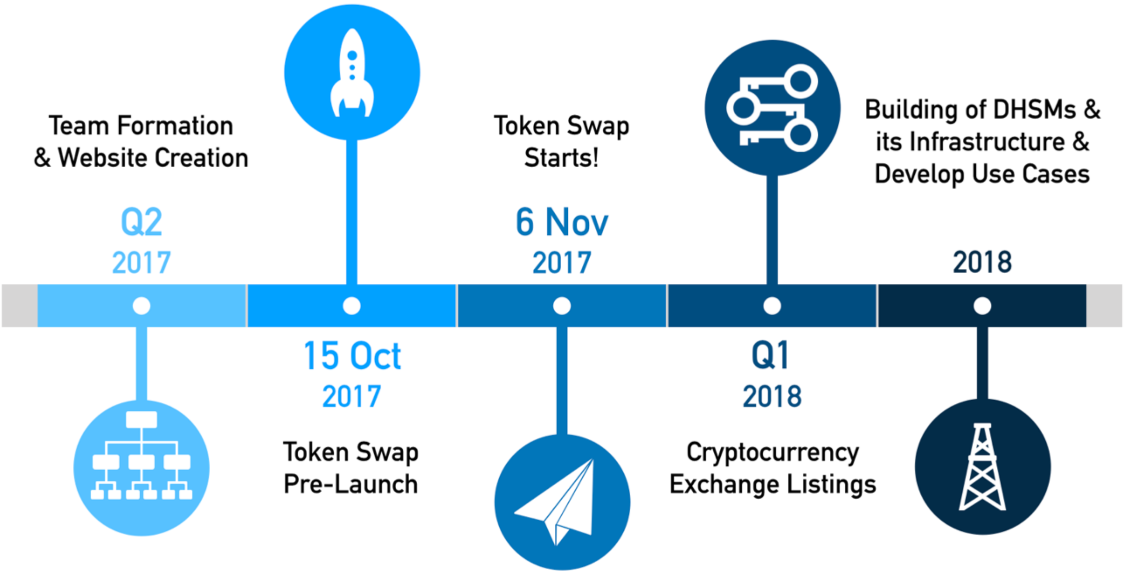

Team Formation & Website Creation
Q2 2017
15 Oct 2017
Token Swap Pre-Launch
Token Swap Starts!
6 Nov 2017
Q1 2018
Cryptocurrency Exchange Listings
Building of DHSMs & its Infrastructure & Develop Use Cases
2018

Figure 7: TSS ICO Roadmap

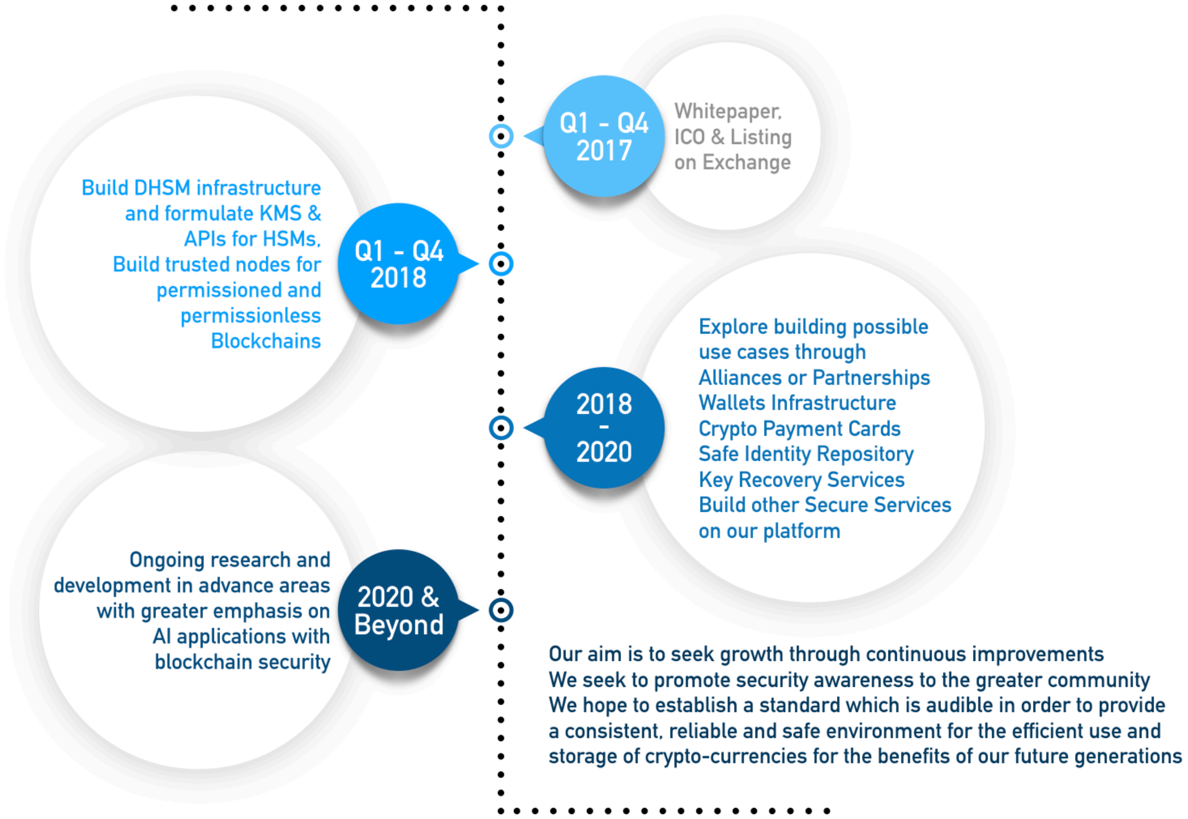

Q1 - Q4 2017
Whitepaper, ICO & Listing on Exchange
Q1 - Q4 2018
Build DHSM infrastructure and formulate KMS & APIs for HSMs, Build trusted nodes for permissioned and permissionless Blockchains
2018 - 2020
Explore building possible use cases through Alliances or Partnerships
Wallets Infrastructure
Crypto Payment Cards
Safe Identity Repository
Key Recovery Services
Build other Secure Services on our platform
2020 & Beyond
Ongoing research and development in advance areas with greater emphasis on AI applications with blockchain security
Our aim is to seek growth through continuous improvements
We seek to promote security awareness to the greater community
We hope to establish a standard which is audible in order to provide a consistent, reliable and safe environment for the efficient use and storage of crypto-currencies for the benefits of our future generations

Figure 8: TSS Master Plan

TSS Token Sale Agreement

As part of our ICO launch, you are required to read TSS Token Sale Agreement Exhibit A and acquainted yourselves with the agreement details.

TOKEN SECURITY SCHEME

www.tsstoken.com

enquiry@tsstoken.com