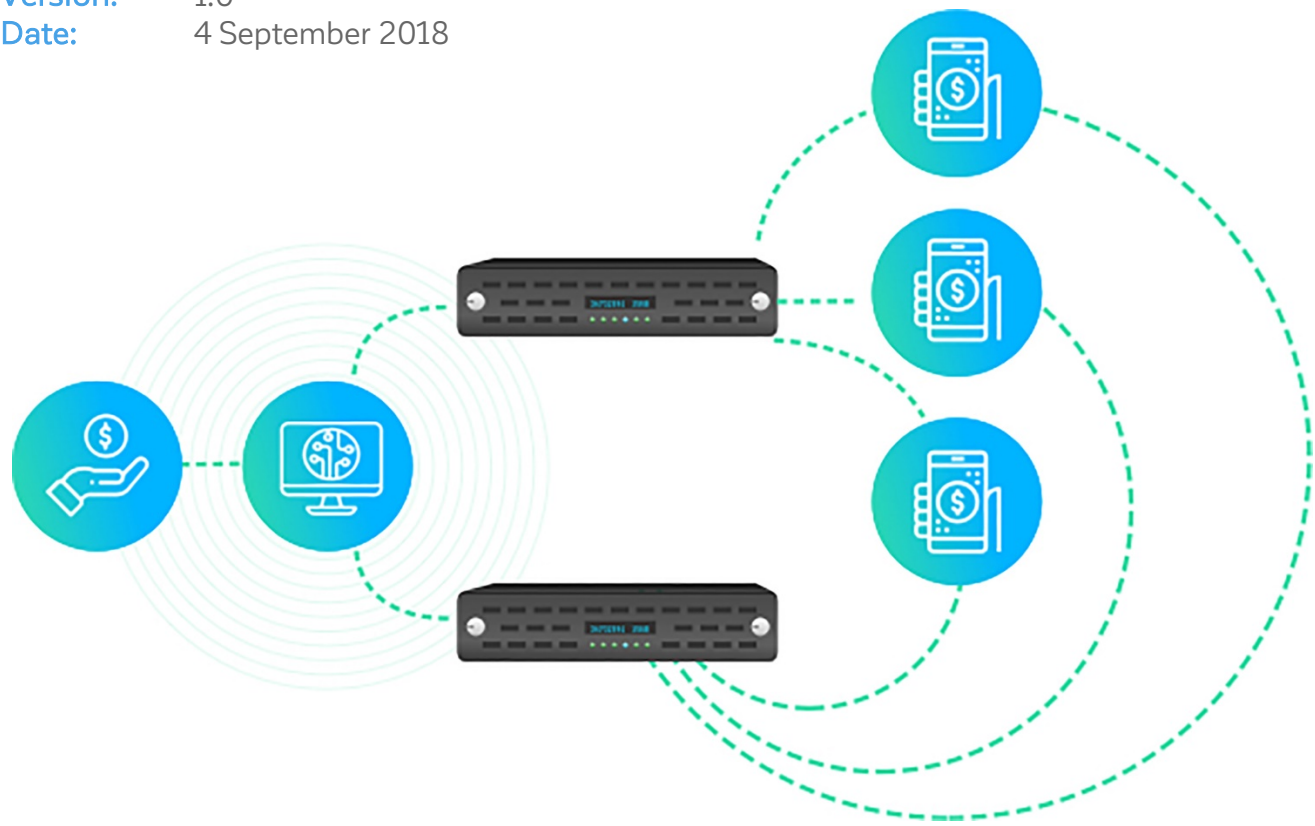
Shapeshifter Platform Whitepaper

Version: 1.0
Date: 4 September 2018



Notices:
THIS DOCUMENT IS CONFIDENTIAL TO QREDO. YOU ARE NOT AUTHORIZED, AND YOU MAY NOT REPRODUCE, FORWARD OR OTHERWISE DISTRIBUTE THIS DOCUMENT ELECTRONICALLY OR OTHERWISE, TO ANY OTHER ORGANISATION.

Table of Contents

Cybersecurity Risks Facing Cryptocurrency Exchanges 3
- Degrading customer experience becomes the norm 3
- Legacy hardware security modules (HSM) do not stop the hackers 4
- Stored keys and credentials create the cybersecurity risk 4

Qredo Shapeshifter HSMs and Multi-Factor Clients 6
- Zero-Knowledge Decryption 6
- Internals 9
- Deployment 12
- Transaction Flows 12
  - Sending Funds and Establishing Holdings 13
  - Liquidating Holdings 14
- Threat Model 16
  - Attack 1 17
  - Attack 2 18
- Open Source Cryptography 19

© Qredo Ltd 2018

Cybersecurity Risks Facing Cryptocurrency Exchanges

In 2018, cryptocurrency exchanges have lost over $760 million in the first two quarters of the year, compared to $266 million lost throughout the entire year of 2017. Overall, cryptocurrency theft has surged three times in the first half of 2018 over the whole of last year, according to a report by CipherTrace. While some of these thefts have happened on independent storage wallets, studies indicate that 78% of them have occurred on exchanges.

A loss of customer funds in many cases has become a terminal event for many cryptocurrency exchanges hacked by cybercriminals.

Degrading customer experience becomes the norm

Efforts to mitigate the risks of storing customer funds in hot wallets have seen cryptocurrency exchanges create elaborate systems of 'cold storage'. It involves storing private keys offline; meaning, away from any internet access. Keeping cryptocurrency private keys offline reduces the threat from hackers, but it can significantly hold back the speed of accessing funds and degrading the ability to act on trading opportunities in real time. Elaborate practices of splitting the exchange reserves to support the buying and selling of cryptocurrencies on order are now the norm.

Automating payouts and supporting repeating business processes requires that cryptocurrency exchanges need to eventually use a hot wallet, where keys are transferred to a system connected to the internet. These hot wallets are controlled through APIs and receive orders to sign outgoing transactions to pay customers wishing to withdraw their funds. Because exchanges need to be able to automate these wallets, the keys must be live, connected to the internet, and are therefore at risk of theft.

© Qredo Ltd 2018

Legacy hardware security modules (HSM) do not stop the hackers

A hardware security module (HSM) is a physical computing device that safeguards and manages cryptographic keys and provides secure execution of critical code. These modules come in the form of a PCI card, or an external rackable device which can be directly connected to the network. HSMs have built-in anti-tampering technology which wipes secrets in case of a physical breach. Historically, these devices are heavily used in the banking industry and in all verticals where critical secrets require stringent protection. Hardware security module vendors have been quick to spot the opportunity to package solutions for cryptocurrency exchanges repurposing legacy technology in an attempt to solve these critical threats.

However, the current offering of HSMs on the market today are built on legacy technology and concepts; the designs have not evolved to address the threat of protecting secrets that are centralized in one location. An HSM's principal value is the mitigation of key compromise. An example operation encrypts keys with a master encapsulation key stored within the secure boundary of the HSM. Implementing today's centralized HSMs is not a trivial task, and the added development overhead of integrating HSMs into an architecture built for speed and convenience can be a steep price to pay in a hypercompetitive industry.

Stored keys and credentials create the cybersecurity risk

And herein lies the issue. Any centralized storage of private keys and authentication credentials, even when encrypted, creates the incentive for criminals to hack cryptocurrency exchanges. While HSMs are effective at protecting the encryption key used to secure the private keys and mitigate monetary loss, a data breach is a data breach. In many regulated jurisdictions such as the EU, it is mandatory to publicly report and inform customers that the exchange has suffered a breach, even when no monetary theft occurs. Breach notifications can lead to a loss of customer confidence and business.

© Qredo Ltd 2018

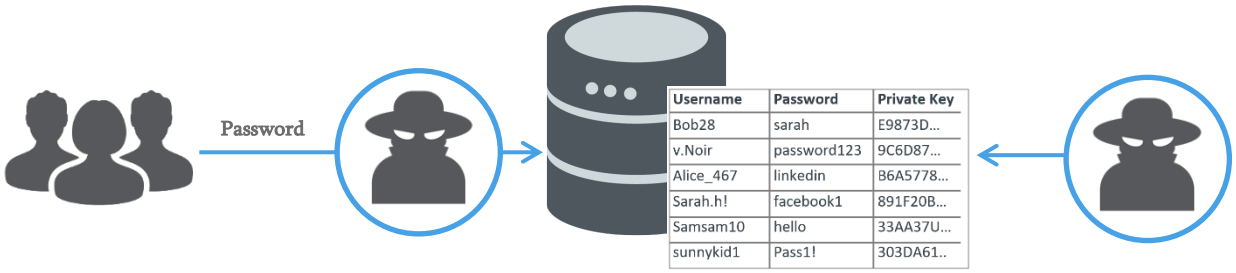


Fig 1: Centralized storage of passwords and private keys greatly increase the risk of data breaches

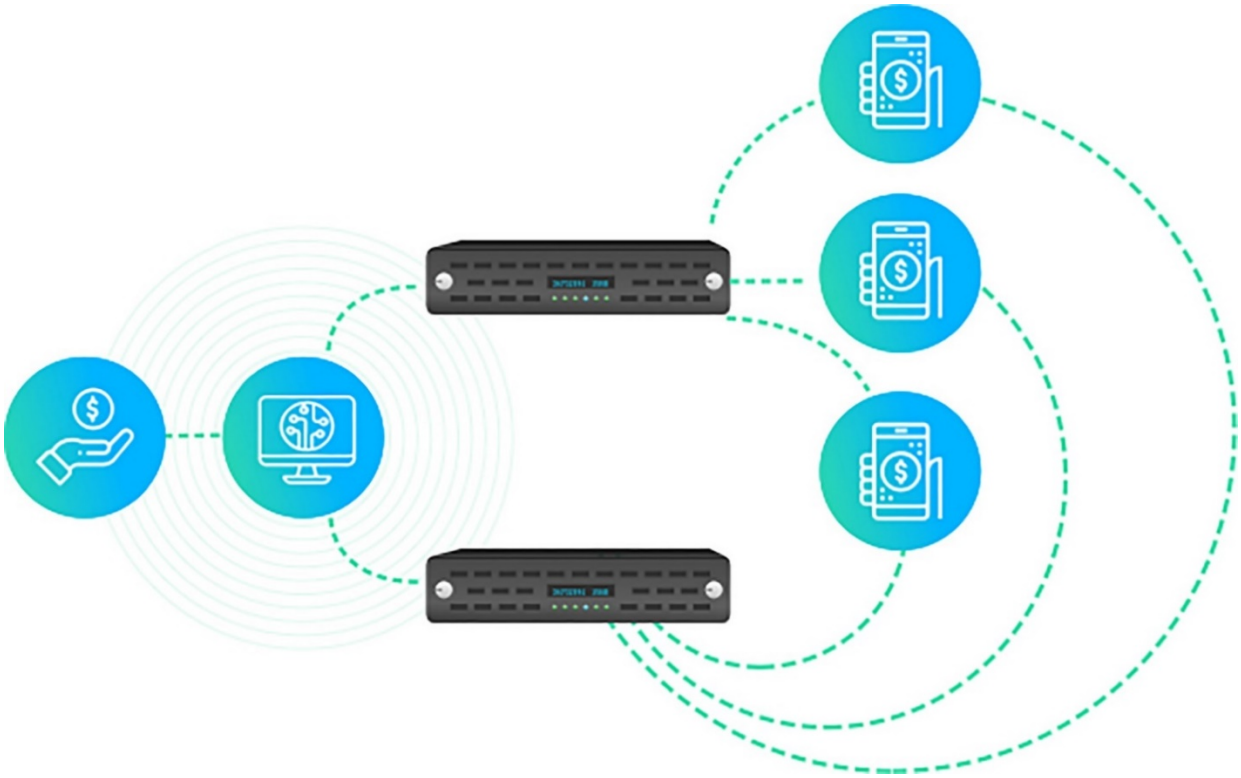
A new approach is needed that recognizes the unique requirements of cryptocurrency exchanges.

Imagine a solution that removes the threat created by private key and end user credential storage entirely, by entirely removing the requirement to store private keys and end user credentials within the cryptocurrency exchange.

To indeed be impactful, this new approach must exceed the security, operational capabilities and user convenience and confidence of existing systems to be a business enabler.

© Qredo Ltd 2018

Qredo Shapeshifter HSMs and Multi-Factor Clients



Qredo's Shapeshifter crypto security is a breakthrough in security design and capability, delivering the assurance of cold storage and the business agility of hot wallets. Shapeshifter eliminates the threat vector caused by the centralized storage of cryptographic assets through the deployment of role-based HSMs and transaction authorization smartphone apps.

Zero-Knowledge Decryption

Through innovative use of elliptic curve cryptography (the kind used by many cryptocurrencies today), Shapeshifter HSMs and transaction authorization apps create a zero-knowledge decryption system, which enables processes to decrypt a ciphertext without learning anything about the ciphertext itself.

To get a grasp on this unique capability, it is helpful to compare it to a public/private key cryptosystem like the kind used to create TLS sessions widely in use on the web today. In a

© Qredo Ltd 2018

normal public/private key system, a public key can be used to create a ciphertext that can only be decrypted with a corresponding private key.

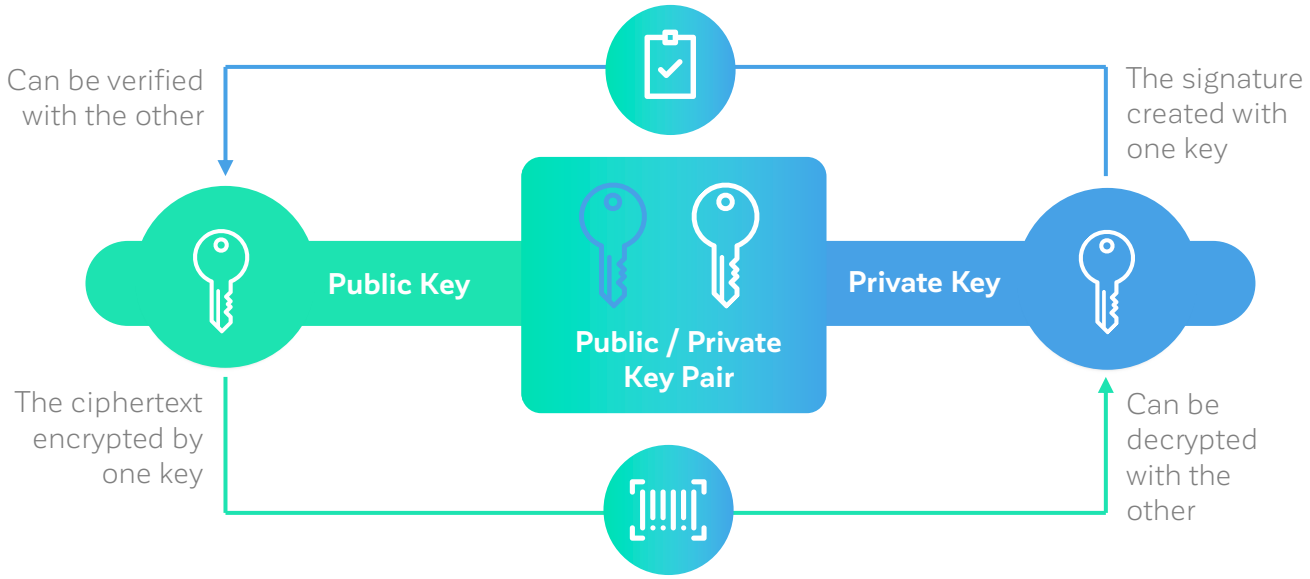


Fig 2: Public/Private Key cryptography example

In comparison, a zero-knowledge decryption system enables one role-based Shapeshifter HSM to encapsulate (encrypt) a cryptocurrency private key so it becomes secured against theft and misuse before it permanently leaves the HSM (and the exchange) and is distributed to end user(s) of the exchange.

The end user(s) obtain this encapsulated (encrypted) private key inside their multi-factor authenticator app. The end user(s) use this key to create a separate signature by successfully initiating a local multi-factor authentication sequence. A successful authentication process ultimately enables cryptocurrency transactions in a second, separate role-based Shapeshifter HSM within seconds.

A few things to make clear: The encapsulated (encrypted) private key distributed to the end user can no longer be used to create a cryptocurrency digital signature on its own, nor can the end user(s) (or anyone) who has received the encrypted private key ever decrypt it, including any Shapeshifter HSM.

© Qredo Ltd 2018

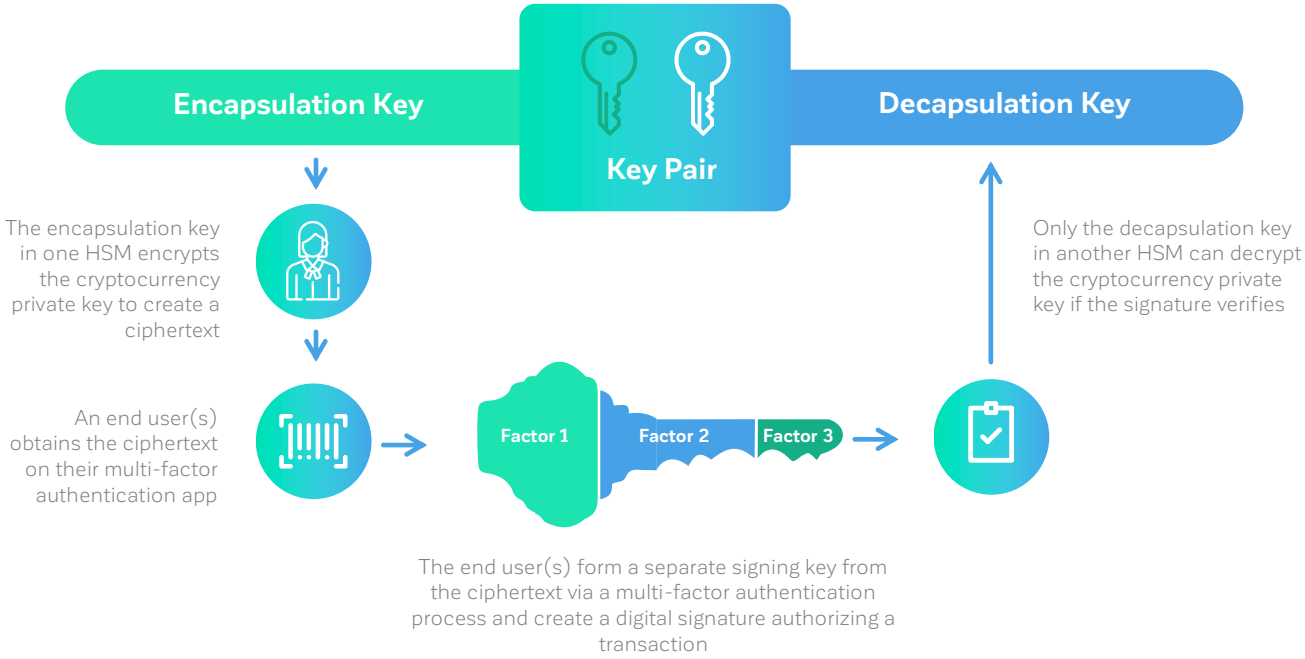


Fig 3: Zero-Knowledge Decryption

However, the encapsulated (encrypted) private key can create a digital signature that the second role-based Shapeshifter HSM can use to extract the original cryptocurrency private key. The result is that the second role-based HSM does not need access to the encapsulated (encrypted) private key in order to create a cryptocurrency transaction on an end user's behalf. It simply needs a digital signature created by a end user using the encapsulated (encrypted) private key under the end user's (or multiple end users) control.

In summary, all wallet private keys can be removed from the exchange's infrastructure and, in encapsulated form, distributed to the end user(s). The end user(s), through a successful multi-factor authentication process, can enable a role-based HSM to decapsulate the cryptocurrency private key and employ it for the benefit of the user.

© Qredo Ltd 2018

For a hacker to have a complete compromise of the system, they would need to steal keys from two different HSMs (without destroying them in the process) and gain access to all the smartphones of every single deployed customer. A following threat model section delves further into these concepts.

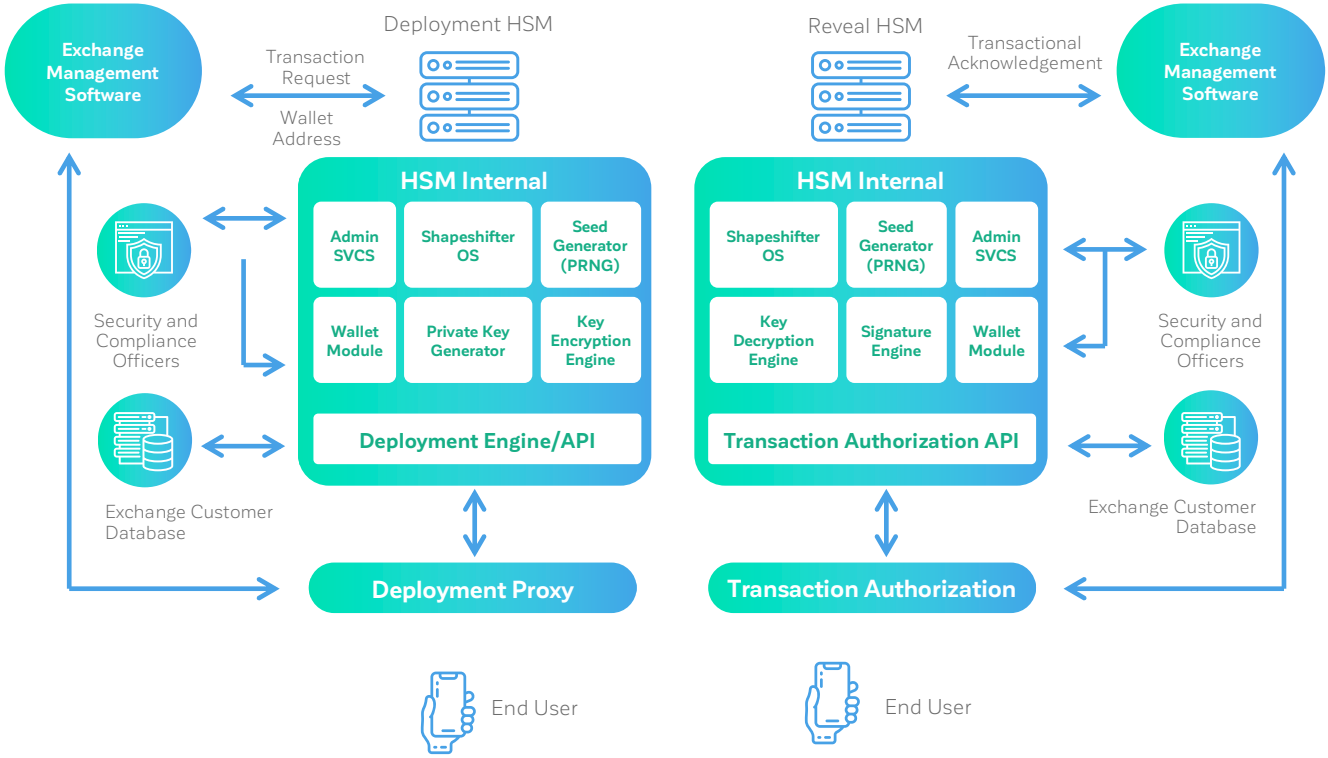


Fig 4: Qredo Shapeshifter HSM deployment for Zero-Knowledge Decryption and Multi-Factor Authentication

© Qredo Ltd 2018

Internals

Each role-based HSM contains the following hardware components and security measures:

- ARM TrustZone Architecture, a trusted execution environment for security-critical software
- Hardware-assisted virtualization-two virtual machines: Secure and Normal Worlds (processor modes)
    - Hardware firewalls
        - Control of access from the CPU and DMA peripherals to the on-chip peripherals and to both the on-chip and off-chip memories
        - Interrupt separation
        - Secure storage separation
        - Cryptographic separation
        - Manufacturing protection
        - Encrypted Boot
- Secure High-Assurance Boot
    - Security library embedded in the tamper-proof on-chip ROM
    - Authenticated boot, which protects against unauthorized software
        - Verification of the code signature during boot
        - RSA-1024/2048/3072/4096 keys anchored to the OTP fingerprint (SHA-256)
    - Image version control/image revocation (on-chip OTP-based)
- Secure storage
    - On-chip zeroizable secure RAM (32 KB)
    - Off-chip storage protection using AES-256 and the chip's unique hardware-only key
- Hardware cryptographic accelerators
    - Symmetric: AES-128/192/256, DES/3DES
    - Asymmetric: RSA (up to 4096), Elliptic Curve (up to 1023)
    - Hash message digest and HMAC: SHA-1, SHA-256
- True and pseudorandom number generator
- On-chip secure real-time clock with autonomous power domain
- Secure debugging

© Qredo Ltd 2018

    - Configurable protection against unauthorized JTAG manipulation
    - Three security levels + a complete JTAG disable
    - Support for JTAG port secure reopening for field return debugging
- Universal unique ID
- Electrical fuses (OTP Memory)
- Physical tamper detection
- Tamper detection of covers, keyboards, pin pads, and magnetic and touchless card readers
    - Tamper input signal available for cover seal and power glitch detection
    - Hardware and software tamper response
    - Temperature, Voltage, and Clock tamper
    - Wire-Mesh by combining the passive/active tamper
- Passive tamper
- Active tampers
- Hardware and software tamper response (zeroizable RAM/secure key erasure)

Each role-based HSMs contain the following software services which leverage the hardware security:

- Shapeshifter OS: a minimized embedded Linux distribution that leverages the tamper-proof hardware, accesses the root seed from which all key pairs are derived, and exposes an API so the exchange's business apps (such as the exchange's trading platform) can operate. This software distribution is tested and signed offline and cannot be altered once the HSM is deployed into production.
- Other services: Transaction rate limiter, which sets the hard limits on the velocity of what number of transactions the HSM can action per hour. The cryptocurrency Wallet App contains all the logic to build and sign transactions from a UTXO pool and is updated continually to support new cryptocurrencies (based on market demand).
- Admin Services: Qredo Shapeshifter HSMs uses a set of operations called Admin Services to provide a secure environment for all hardware security devices and key management operations. Admin Services is scalable; a Security Officer can chain multiple hardware security devices to the main HSM and share the Admin Services operations across multiple HSMs. Admin Services contains master configuration information for the HSM, the Admin Services files, and key data. It can be configured

© Qredo Ltd 2018

on any computer available via the network and enables off site backups of configurations in the event of catastrophic loss of deployed HSM units.

Deployment

Qredo Shapeshifter HSMs can be deployed in under an hour. Simple key initializing procedures with easily understood administrator operations and role assignments and a well-documented RESTful API together create a reliable, easily integrated security system that delivers immediate time to value.

1. The HSM is flashed with the Shapeshifter OS into provisioning mode using the mini-HSM OS loader, shipped with each device.
2. A Security Officer uses the Admin Services and sets up each Compliance Officer and other Security Officers with credentials and authentication files.
3. The Security Officer selects which mode (Deploy or Reveal) of operation. Note that a Deploy mode HSM must be instantiated before a Reveal mode HSM.
4. The attestation of firmware and onboard software is done using the HSM hardware component's high-assurance boot process. This ensures the integrity of the loaded software.
5. A 256-bit master seed is generated by the HSM. The Security Officer has the choice of backing the seed up into distinct backup mediums (smart card, encrypted USB drive or paper) and shares of the seed. The seed is stored within the HSM's on-chip zeroizable secure RAM.
6. The Signature Verification or Key Encapsulation Master Key is created (depending on the mode of operation selected) and stored within the HSM's on-chip zeroizable secure RAM.
7. The Security Officer creates API Keys for internal business apps and proxies with access to the HSM.
8. The HSM is switched into 'live' mode. Any attempt to physically attack the HSM would wipe the seed and keys from the HSM's on-chip zeroizable secure RAM.

Transaction Flows

Instead of storing wallet private keys in hot wallets or cold storage, all wallet private keys are submitted to Shapeshifter HSM’s API and encapsulated (encrypted) by a key encryption key

© Qredo Ltd 2018

running in the secure boundary of the role-based HSM ("the Deployment HSM"). The resulting encapsulated (encrypted) key is deployed to one or more client's Shapeshifter multi-factor authentication apps. The apps secure the encrypted key through elliptic curve subtraction, which removes slices of the encrypted key using the end user's multiple identity factors. The remaining slice of encrypted key is stored securely by the Shapeshifter multi-factor authentication app on the end user's smartphone. The stored encrypted key slice is immune to brute force attacks. This means a hacker that steals a stored encrypted key slice from a via a malicious app or compromised smartphone cannot 'guess' the rest of the slices to remake the encrypted key, even with unlimited computing power.

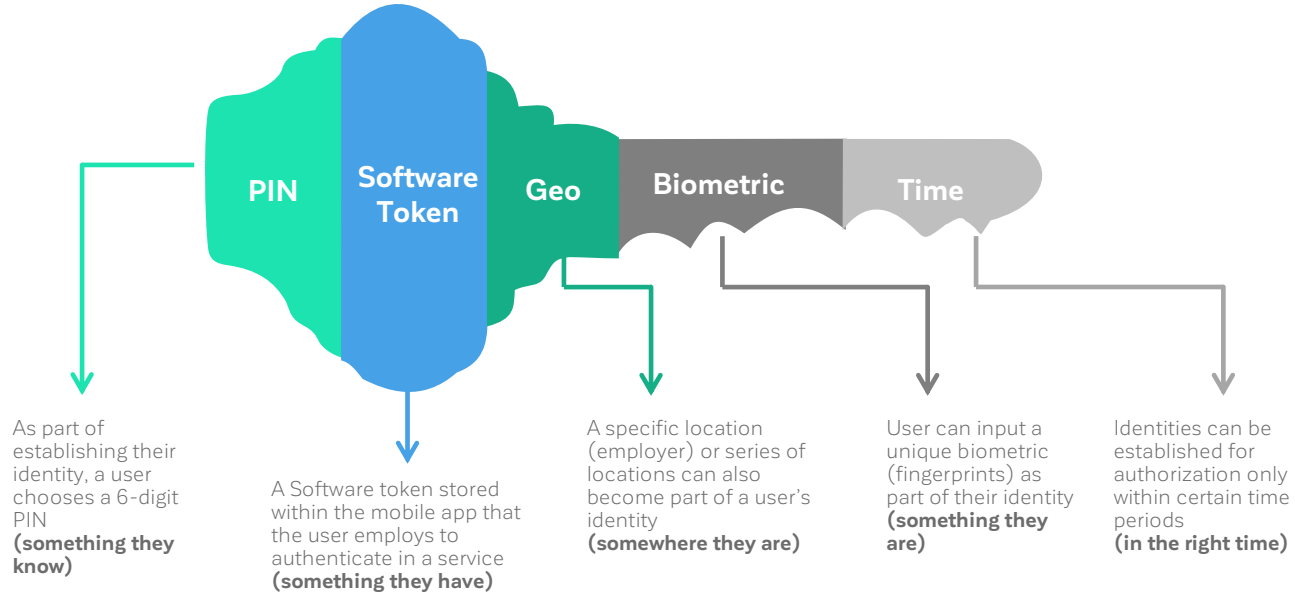


Fig 5: Ciphertext secured by subtraction of multiple identity factors using the Shapeshifter authenticator apps

Sending Funds and Establishing Holdings

The following is a simplified example workflow of an end user sending cryptocurrency to the cryptocurrency exchange with the compliance setting set to the same single end user assigned the capability to instruct the exchange to liquidate positions. Other supported scenarios include multiple Compliance Officers providing a quorum or threshold of signatures to liquidate holdings, not covered in this example:

© Qredo Ltd 2018

1. The end user accesses the cryptocurrency exchange platform in the usual way (web UI or smartphone app) and initiates a buy order of cryptocurrency.
2. The exchange's management software invokes the Shapeshifter 'Deploy' HSM's API to initiate a transaction request, which actions the on-board wallet software to create a private key and wallet address and encapsulate (encrypt) the key.
3. The wallet address is returned to the exchange's management software in the response.
4. The wallet address is displayed to the end user in the exchange's web UI or smartphone app.
5. The exchange's management software polls the cryptocurrency's ledger for transaction confirmation and receipt of funds to the wallet address. Once confirmed, the exchange's management software invokes the HSM API to provision the encapsulated (encrypted) private key to the end user's Shapeshifter multi-factor authentication app (providing the ID of the app to provision the key to).
6. The Shapeshifter HSM invokes the API of the Shapeshifter deployment proxy web service, providing the encapsulated key and the information necessary to send a notification to the end user's app.
7. The end user consents to the notification and the app obtains the encapsulated (encrypted) key from the proxy web service.
8. The end user is prompted by the app to secure the encrypted key by providing a 6-digit PIN and supplying their biometric (if the device supports it). These factors are elliptic curve subtracted from the whole encrypted key to create a modified ciphertext, which is stored securely on the device.

These factors are commonly known as something you know (PIN), something you have (device), and something you are (biometric) routinely used in multi-factor authentication. The factors can even be extended to cover location and time.

Liquidating Holdings

The following continues the simplified example workflow of an end user liquidating holdings established in the cryptocurrency exchange with the compliance setting set to the same single end user who must authorize the transaction by providing the cryptocurrency private key through successful multi-factor authentication.

© Qredo Ltd 2018

1. The end user accesses the cryptocurrency exchange platform in the usual way (web UI or smartphone app) and initiates an order to sell cryptocurrency.
2. The exchange's management software invokes the Shapeshifter 'Reveal' HSM's API to initiate a transaction request, providing a forwarding address for the liquidated funds. The ultimate end process sees the end user(s) create a digital signature which is consumed by the Shapeshifter 'Reveal' HSM in order to decapsulate the encapsulated wallet private key.
3. The Shapeshifter 'Reveal' HSM invokes the API of the Shapeshifter reveal proxy web service, providing the information necessary to send a notification to the end user's app.
4. The end user receiving the notification is prompted inside the app to provide their multiple identity factors (PIN, biometric, etc.) in order to remake the ciphertext, which contains the encapsulated cryptocurrency private key.
5. Elliptic curve addition adds the multiple authentication factors (slices) together, and the recreated ciphertext is used to generate a digital signature.
6. This digital signature, which reveals nothing about the secured ciphertext used to create it, is sent over an encrypted channel to the Shapeshifter 'Reveal' HSM deployed at the cryptocurrency exchange.
7. Inside the Shapeshifter 'Reveal' HSM's hardware security boundary is the signature verification key. The signature verification key verifies that the form of the signature is correct. The secondary process de-encapsulates the original cryptocurrency private key from the digital signature.
8. The cryptocurrency private key is used to create a new transaction using the supplied forwarding address given through the initial API call made by the exchange's management software.
9. This process happens within the tamper-resistant hardware of the HSM, and the cryptocurrency private key is instantly wiped from the secure memory of the HSM once it creates a cryptocurrency transaction.

An incorrect or fraudulent factor supplied in the authenticator app results in a ciphertext different than the one used to secure the key, ending the process without revealing the secured cryptocurrency private key. The digital signatures created from encapsulated keys/ciphertexts are immune to brute force attacks, negating the threat of intercepted communications.

© Qredo Ltd 2018

Threat Model

As previously stated in a preceding section, for a hacker to have a complete compromise of the system, they would need to steal keys from two different HSMs (without destroying them in the process) and gain access to all the smartphones of every single deployed customer.

It should be stated that there is **no perfect security**. However, when reviewing security solutions, it is necessary to compare and contrast against existing systems' threat models to see if the deployment of a new model brings substantial leaps forward in security posture and business competitiveness. We believe customers deploying Qredo's Shapeshifter HSMs will benefit from these forward leaps in capability.

For the purposes of creating a threat model, we make the following assumptions:

1. For Attack 1: An attacker gains full control of the entire operations infrastructure of the exchange.
2. For Attack 2: An attacker gains full control over the entire development infrastructure of the exchange, in addition to the operations infrastructure of the exchange. This threat model exists if the exchange is responsible for developing their own multi-factor authentication app using the open source libraries.
3. Both 1 and 2: An attacker cannot gain access to the HSMs without destroying the stored secrets within the HSMs.
4. Both 1 and 2: An attacker does not get access to the Admin Services backup settings of the HSMs which contains master configuration information for the HSM, the Admin Services files, and key data. These backups should be stored on secured medium. (ex: smart card) and in a secured location, offsite from the exchange.
5. Attack 2: An attacker does not have the means to mount an industrial scale attack targeting all deployed end users operating the multi-factor authentication app outside of gaining full control of the entire infrastructure of the exchange (development and operations). To do so would require an attack of two different smartphone OS manufacturers (Google, Apple) and every single wireless operator's infrastructure on which the multi-factor authentication apps were deployed upon.

© Qredo Ltd 2018

Attack 1

One obvious way to attack the exchange would be to issue fake liquidation orders through the exchange's management software, which would invoke the API on the Shapeshifter 'Reveal' HSM and prompt end users to authorize liquidation transactions within their multi-factor authentication app.

Obviously, among most customers, this would trigger an immediate alert since the app was requesting an authorization workflow based on an order they had not initiated. Within the Shapeshifter multi-factor authentication app, in the order detail screen, there exists an 'alert' button to immediately notify the exchange if an end user did not initiate the liquidation order.

End users who, for whatever reason, authorize a transaction they did not initiate which was created by a hacker in control of the exchange's management software would lose their funds.

There are two mitigations to this. First, insist that customers with high deposit values have multiple Compliance Officers who must each authorize the transaction, in effect creating a multi-signature requirement. One Compliance Officer may fall for the ruse, however unlikely, but two or more falling for the ruse in tandem with a breach of the exchange would suggest a breach of the exchange has occurred in tandem with a breach of a particular customer (conspiracy).

Second, educating the exchange's customer base on the expected workflow and that they should never authorize a transaction they themselves were not aware of in advance (i.e., Compliance Notification) or did not initiate themselves is important to obtain the highest possible value from the system.

Presumably, even one customer hitting the 'alert' button would cause the CISO and monitoring teams to investigate immediately and/or halt trading until the situation is clarified or remedied, mitigating any risk of loss to that immediate time frame.

The rate limit set by the exchange's Compliance Officers when setting up the HSMs would also provide an additional loss mitigation technique.

© Qredo Ltd 2018

Qredo ascertains the threat level presented by this attack method is remote, and that losses, if any occur, are minor.

Attack 2

Another more catastrophic attack would be to compromise not only the exchange's management platform (to issue false liquidation orders) but also compromise the code base housing the exchange's own implementation of the multi-factor authentication app code should it issue its own app, or put the app's capability into its own app.

Note this attack is only works when both operations infrastructure and the exchange's development infrastructure is completely compromised, and the exchange issues its own multi-factor authentication app or inserts the capability into its own app, rather than using the off-the-shelf Qredo multi-factor authentication app.

A hacker, once penetrating the code base of the exchange's trading app, would implement some envisioned vulnerability into the app's code base, such as a remote-controlled virus which would make a copy of the whole ciphertext received by a provisioned multi-factor authentication app end user during the sending funds/adding positions process.

Presumably, the hacker would operate in secret until they deemed they had stolen enough complete ciphertexts which could be used to create digital signatures to have the Shapeshifter 'Reveal' HSM create transactions of off fake orders generated by the same hacker who had compromised the exchange's management platform.

In order for this attack to work, the hacker would also need to:

1. Switch the addressing information supplied to the Shapeshifter reveal proxy web service, providing the information necessary to send a notification not to the end user's app, but to the app of the hacker, and;
2. Subvert any monitoring software that would detect rogue IP and other anomalies as the submitted signatures would come from entirely different apps than ones the ciphertexts had been deployed to.

The complexity required to pull of this attack, and the conditions under which it could occur, enables Qredo to assume the threat level presented by this attack method is also remote, assuming that the exchange has adequately deployed cybersecurity protection and is staffed

© Qredo Ltd 2018

to monitor against threats. Losses, if they occur, are also mitigated by the rate limit set by the exchange's Compliance Officers when setting up the HSMs.

Open Source Cryptography

The cryptographic concepts used in the Shapeshifter HSMs are based upon the initial cryptographic research paper co-authored by Qredo's CEO Brian Spector and published in 2015 by the International Association for Cryptologic Research.[1]

These innovations in pairing cryptography formed the basis of an Apache Foundation open source project called Apache Milagro. Apache Milagro is a distributed cryptosystem created to advance concepts in the elliptic curve pairing cryptography for the benefit of IoT security.
Apache Milagro establishes a new internet security framework purpose-built for cloud-connected app-centric software and IoT devices that require Internet scale. Milagro's purpose is to provide a secure, free, and positive open source alternative to centralized and proprietary monolithic trust providers such as commercial certificate authorities and the certificate backed cryptosystems that rely on them.

Apache Milagro is an open source, pairing-based cryptographic platform that delivers solutions for device and end user authentication, secure communications and fintech / blockchain security; issues challenging Cloud Providers and their customers. It does this without the need for certificate authorities.

Apache Milagro's M-Pin® protocol is already in use by Experian, NTT, Ingram Micro, and Gov.UK and rolled out to perform at Internet scale for multi-factor authentication and certificate-less HTTPS / secure channel.

Portions of the HSMs cryptographic code used within the HSMs onboard applications comes from the Apache Milagro open source project and is licensed under the Apache License, Version 2.0.

You can find out more about Apache Milagro on the project's website: https://milagro.apache.org/

[1] https://eprint.iacr.org/2015/576

© Qredo Ltd 2018