Little Bit
by Silver Bullion

Crypto Currency Physical Storage

The Gregersen-Gono Standard

Gregor Gregersen
Little Bit Pte Ltd
Gregor@LittleBit.sg

Clint Mark Gono
Little Bit Pte Ltd
Clint@LittleBit.sg

Abstract

In this paper, we describe a completely offline, physical storage which utilizes ultraviolet (UV) lasers to etch encrypted private keys onto polycarbonate plastic cards. These cards are stored in sealed safe deposit boxes within a high security physical vault along with gold and silver bullion.

Our cold storage implementation is designed to provide the safest storage of cryptocurrency in the market by replacing digital storage in favor of encrypted physical storage and adapting existing high-security vaulting facilities, processes and insurance coverage to securely store the physical crypto keys.

Furthermore, to minimize identity theft, video conferences are used to visually identify customers during withdrawal requests or when modifying a pre-approved withdrawal address. Although labor intensive this authentication method provides security beyond the automated 2 factor authentications used in the Industry.

Version 20180216 of this paper introduces secured partial withdrawals and pre-set withdrawal addresses for faster withdrawal.

Version 20180216 of this paper is expected to go into production in early March at The Safe House SG Pte Ltd (see www.thesafehouse.sg) after third party security reviews. The Safe House's parent company Silver Bullion Pte Ltd will soon be the first company to offer the service to customers. Service details can soon be found at https://www.silverbullion.com.sg/Info/StarStorage

Gregor Gregersen
16 February 2018

Contents

1. Crypto Currency Overview

To understand this storage specification, a basic understanding of the bitcoin protocol is required. In particular, the following concepts are essential:

1.1. Bitcoin Address

A bitcoin balance is a chain of digital signatures (akin to transactions) stored in a public ledger called the blockchain. The final digital signature is the current holder of a bitcoin amount and is identified on the network by a unique string of characters, which is the user's **public address**[1].

The public address can be loosely thought of as the equivalent of a bank account number in that bitcoins can be sent to a given address. Note that, unlike a bank account, the bitcoin balance in a given address can be viewed by anybody who knows the address, although the identity of the address owner is not recorded on the blockchain.

1.2. Address Balances

The amounts of bitcoin stored within a given address can be reliably determined at any point in time via Blockchain explorers. Blockchain explorers are tools that make it easy to search the public blockchain to see transaction details and balances.

Popular blockchain explorers are: https://live.blockcypher.com/ or https://blockchain.info/.

To use these tools, go to any of the abovementioned website and enter the Bitcoin address to view a complete history of transactions and balances at any point in time.

1.3. Private Key

Possession and control of the bitcoin balance for a given address is based on having knowledge of its **private key** (or keys for multi-signature accounts). **The private key can be thought of as the equivalent of a bank account password, security token and account number combined into one**. Whoever knows the private key of a given address is able to release (spend) bitcoins out of that address.[2]

Unlike a physical asset (e.g. gold), where the asset itself must be safeguarded, for cryptocurrencies, information (e.g. private key) must be safeguarded. For example, if somebody were to view or take a photograph of a plaintext private key that person could then withdraw bitcoins from the corresponding address. Therefore, secure physical storage

[1] *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoyy, Geoffrey M. Voelker and Stefan Savage

[2] https://en.bitcoin.it/wiki/Transaction

of private keys requires robust procedures to keep a private key protected from everybody, including the customer, until the bitcoins are released.

1.4. Public Key

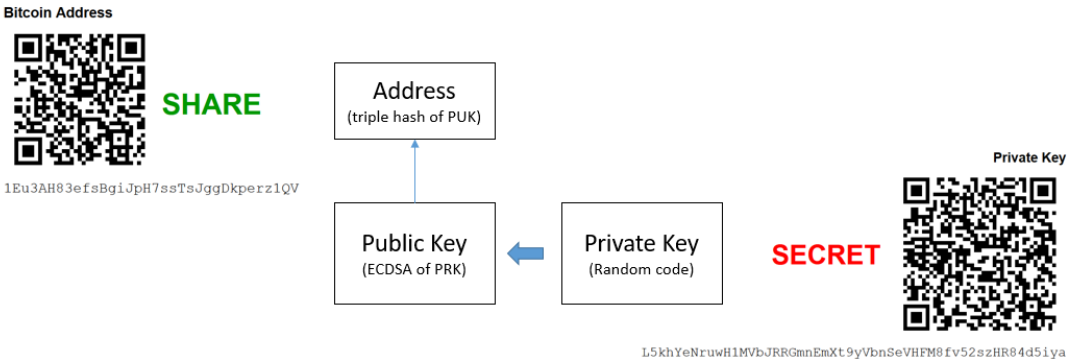
Each private key has a mathematically derived public key. The public key has a number of technical functions and, although typically hidden by wallet applications, the key is required for advanced bitcoin features such as:

- Generating additional addresses linked to a single private key
- Generating multi-signatory addresses which require multiple keys to send funds

Security implications of multi-signature accounts and the role of a storage provider will be addressed later.

1.5. Knowledge of the Private Key Equals Possession

A bitcoin address is mathematically derived from the public key which itself is derived from the private key. This means that, for a standard bitcoin address, the public key and address can be re-created from the private key as needed. Naturally, it is nearly impossible to reverse the process and obtain a private key from an address or public key.



Bitcoin schematic. For ease of use and to avoid errors, bitcoin keys and addresses are typically read via QR codes which can be easily scanned by smartphones or other readers.

This absolute dependency on the private key highlights again **that knowledge of the private key equals possession and control of the bitcoins in the address.**

Take note that the vast majority of bitcoin users – via online wallets or exchanges – do not have access to their private keys, making them fully dependent on the correct functioning, security and secured backup procedures of online wallets or exchanges, as well as the integrity of the wallet designers to manage their key. **If you do not have control of the**

private key you are, from a counterparty risk perspective, effectively a creditor of the bitcoins to the possessor of the private key.[3]

1.6. Offline Key Generation Supports High Security Storage

The blockchain itself does not know when a new random private key or address is created until bitcoins are actually transferred to the newly created address (blockchain signature). This means that keys or addresses can be created on computers that are not connected to the Internet (offline). Offline creation works because it is practically impossible that two properly randomly generated private keys will be the same across space and time.

Offline generation is a great security advantage as fully offline computers are very difficult to be compromised by external third parties (hackers). Furthermore, a private key is not needed until funds need to be sent out of the bitcoin address.[4]

1.7. Transaction Irreversibility and Private Key Loss

Once a bitcoin transaction (blockchain signature) is made, it is not possible to reverse it as no entity is allowed to alter blockchain signatures. Furthermore, if a private key is lost, it is not possible to recover the private key from the blockchain and any bitcoin in the address will be lost. Loss of Bitcoins due to owners losing or forgetting their keys has become quite common, hence the need for a reliable storage recovery mechanism is essential.

1.8. Private Keys are Perfect Hacking Targets

While the bitcoin protocol has proven to be robust, bitcoin private keys are prime targets for hackers as a private key is the banking equivalent of a bank account login name, password and security token combined into a single code.

Should an intruder obtain any private key, he can easily obtain the corresponding address, verify the corresponding bitcoin balance and transfer bitcoins to his own address.

The sensitivity of private key storage is best illustrated by the Mt. Gox exchange heist. The cryptocurrency heist was detected in 2014 when Mt. Gox, the largest bitcoin exchange at the time, publicly admitted that hackers had stolen almost 750,000 of its customers' bitcoins, and around 100,000 of its own bitcoins over a period of two years.

The exchange filed for bankruptcy resulting in its customers losing bitcoins with a combined value of USD 450 million at the time. Had the customers not lost their bitcoins, their holdings would have been worth USD 6.9 billion as of November 2017.

---

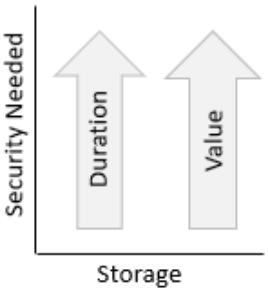
[3] https://en.bitcoin.it/wiki/Private_key

[4] *Bitcoin Private Keys: Everything You Need To Know,* Sudhir Khatwani https://coinsutra.com/bitcoin-private-key/

Today, computer viruses, trojans and other hacking tools are specifically written to find private keys given their potential value. A private key is simply a sequence of characters such as "E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA3326" and its security is fully dependent on how well it is protected from external and internal threats.

1.9. Duration and Amount Stored Determine Security Needed

The longer the amount of time bitcoins are held in a given address, the greater the likelihood of it being subject to hacking attempts and potential compromise. Obviously, if more bitcoins are held in a given address, there is a paramount need for strong storage security.



This paper aims to provide a blueprint for the, in the realm of practicability, safest long-term crypto storage system.

2. Crypto Risk Overview

2.1. Systemic Risk vs. Storage Risk

Bitcoins and other related cryptocurrencies are both a digital asset and a network. Both assets and the network itself are exposed to potential cyberattacks. Therefore, storing wealth in the form of cryptocurrencies requires that:

- The currency protocol itself, e.g. the code that runs bitcoin, is resistant from cyberattacks as otherwise the entire cryptocurrency asset class could become worthless. This is characterized as systemic risk.

- The private key, which controls the assets for a given address, is protected from third party attacks, counterparty breach of trust, negligence and accidental loss of the key. These are characterized as storage risks.

This paper focuses on storage risks and how to secure the private keys that represent ownership of a given cryptocurrency. For simplicity purposes, the paper will be using bitcoin as the reference currency, but the processes described broadly apply to other cryptocurrencies as well. The described system can be extended to other crypto currencies.

2.2. Storage Systems: Balancing Convenience, Reliability and Security

Storage systems face contrasting requirements and must therefore find a design compromise among the following desirable features:

Convenience: ease of use, cost and set up time for the user.

Reliability: the system's likelihood to continue operating and the redundancies to ensure the private key is not lost.

Security: protection against Counterparty and Hacking Risk.

It is possible to design systems that are good at only two out of these three characteristics. **Our storage system favors security and reliability over convenience.**

For example:

- **Convenient and Reliable** an online wallet is convenient and, depending on design, a quite reliable system as well. Some of the convenience precludes high security, however.

- **Secure and Reliable** a printed private key generated from an offline computer using a random key with enough entropy (true randomness) kept safely hidden can be

considered secure, as there is minimal or no hacking nor counterparty risk. Storage could also be made reasonably reliable depending on the storage medium and redundancies. However this "Do It Yourself" method is not convenient for most people and requires considerable technical skill and discipline.

- **Convenient and Secure** are akin to prepaid bitcoin. Examples of these are scratchcards concealing private keys with a certain amount of pre-deposited bitcoins. If the printing was done securely, and there was no copy or backup (online or otherwise) then this storage method could be considered secure and convenient. However, the absence of backups and the possibility of physical loss or degradation would not make it reliable over time.

In practice, for any storage application, reliability is mandatory. Therefore, there are effectively two ways of storing cryptocurrencies depending on the user's requirements.

- **Wallets and Online Accounts:** These can be thought of as checking accounts as they facilitate the sending and receiving of bitcoins. Their design focus is on reliability and convenience at the expense of high security.

- **Offline Cold Storage:** These can be thought of as saving accounts as they hold potentially large bitcoin amounts for long periods of time. The design focus is tilted towards reliability and security at the cost of convenience. Cold storage is a generic term however whose security depends fully on its implementation details. Without process transparency and implementation certainty, "cold storage" is essentially a meaningless term.

Within this context the paper goes a step beyond cold storage to introduce:

- **Gregersen-Gono Physical Storage:** Which is designed to provide the highest security level, transparency and process implementation certainty.

Process implementation certainty essentially means that the processes described in this paper, including handling of materialized Private Keys, will always be followed. This is assured by the Vault Management System which was designed specifically to provide process certainty as described later in this paper.

Properly implemented the Gregersen-Gono standard practically eliminates the risk of hacking and physical theft while minimizing counterparty risk and optionally offering additional independent safeguards such as insurance and multi-signatory security.

2.3. Storage Risks

To design a secure storage system, the type of risk that the system needs to protect against must be known. This section categorizes risk into groups that can be protected against.

2.3.1. DIY Mishandling (Security Risk)

Users can store their own keys without the need for third party storage systems but will thereby be responsible for their own security and reliably. The possibility of mishandling the key by the user is discussed in this section.

Due to a key's vulnerability and value, storing a private key in a notepad (.txt) file on a personal computer or sending it via e-mail is highly risky. It takes good discipline and technical expertise to keep a private key safe from trojan horse attacks and hacking attempts.

On the other hand, the loss of a private key would mean that the bitcoins in the corresponding address are permanently lost. Hence, considerable discipline is needed to reliably keep a private key in a safe place.

This is why there is a need for third-party storage systems to be developed, as these specialized systems can apply rigor and resources that an individual might not be able to do.

2.3.2. Counterparty Risk (Middleman Risk)

Counterparties in this context are middlemen between the bitcoin "owner" and his blockchain bitcoin balance. A large number of bitcoin private keys for example are stored in programs commonly known as wallets. With exception of the "Bitcoin Core Software Wallet" and a few others, most popular app wallets hide private keys from the user.

Such wallets create and store private keys whenever funds are received, these private keys are within control of the wallet software and, by extension, the company that wrote the wallet. Users of the wallet do not get to view the private keys as they are managed internally by the wallet.

Since knowledge of the private key equals possession of the bitcoins, using a wallet essentially makes the wallet company the owner of the bitcoins while the wallet user, who bought the bitcoins, is now a creditor to the creator of the wallet software.

Using a wallet software, or any other third-party system that controls the private key, means that you are now trusting another party and no longer enjoying the full benefits of bitcoin's trust-less architecture.[5]

Should the wallet provider break trust and utilize the private keys under their control to steal their creditors' bitcoins, there is nothing to stop them.

Furthermore, the wallet provider might be backing up keys on a third party online cloud or other hosting services. Hence, the cloud provider represents counterparty risk to the wallet provider, which in turns is additional counterparty risk to you, as

[5] *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, Tyler Moore and Nicolas Christin

the cloud provider could potentially find a way to steal the keys or they might lose the keys.

Once you surrender your key for storage to a third party your counterparty risk is the sum of all counterparties involved in processing or storing that key value.

Counterparty risk can be split into:

- **Collusion** – whereby somebody within the counterparty company colludes with an outsider to steal private keys, making it look like a hacking incident
- **Default** – whereby the counterparty itself declares default, e.g. due to hacking and returns only a small portion of the stored bitcoins (e.g. Mt Gox)
- **Theft** – whereby the counterparty, or some of the counterparty's employees, transfers out, washes the bitcoins (a process called "tumbling") and disappears
- **Incompetence** – whereby private keys are published publicly or are lost without possibility of recovery

2.3.3. Hacking Risk (Technical Risk)

Illicitly stealing bitcoin keys from the owner or a counterparty is a big problem. In 2014, Mt. Gox, one of the first bitcoin exchanges, lost 850,000 of their client's bitcoins due to poor security implementation. While exchanges and wallets are adding more security features, the efforts to steal bitcoin keys have also intensified as bitcoin's value has skyrocketed.

Whereas counterparty risk requires a counterparty to intentionally break trust, hacking risk represents a third party taking advantage of a weakness in the counterparty's procedures to get to a key.

Hacking can be classified according to the following:

- **Exploiting technical weaknesses** such as open ports, passwords which are easy to guess, unpatched operating systems, bad encryption and others to steal digitally stored private keys and/or the decryption keys to access the data.
- **Impersonating the customer** Should a hacker obtain control of a customer's e-mail account, it is possible to effectively impersonate the customer as a vast amount of personal information are usually contained in e-mail inboxes. Furthermore, e-mails are often used to reset login passwords or validate requests, often giving email intruders access to somebody's wallets by extension. A sophisticated attacker can also filter incoming emails and might be able to intercept two-factor authorization requests sent via SMS, as he will know the associated phone number from e-mails.
- **Impersonating the Counterparty** Should an attacker be able to hack a public website of the counterparty they might be able to change the bank account or

address to which funds are to be transmitted. In this case, a customer would unknowingly send funds to the attacker instead of the intended counterparty.

- **Intercepting communications (altering addresses / keys)** This is also called a Man-in-the-middle Attack (MITM). If an attacker can change the address to which bitcoins are to be transferred on the fly, due to an insecure transmission medium, this would be an easy manner to hack information.

2.3.4. Private Key Loss Risk

Should a private key whose address contains bitcoins be lost, then it will no longer be possible to utilize the bitcoins stored within the address. Unlike bank passwords, there is no recovery mechanism in the bitcoin protocol, instead the private keys themselves must be stored reliably by the owner or by the counterparty.

Private key storage should represent a balance between storage security and storage reliability. Backups improve reliability but inherently represent additional security problems.

Here are reliability issues to consider:

- **Online storage** Depending on the provider online storage can be an option, but the service may have a limited data retention timespan or the company may purge the data if they are not paid on time. Online storage is subject to the aforementioned counterparty and hacking issues.

- **Physical loss of the storage medium** USB thumbdrives, USB cold wallets, paper printouts, laptops and other hardware devices can be lost or misplaced. To increase reliability, USB cold wallets might have an online backup functions or mnemonic phrases in case of loss. However, online backups create counterparty and hacking risks while mnemonic phrases have the "you see it you lose it" security risk of paper wallets.

- **Physical degradation of the storage medium** All forms of digital media have a chance to lose data over time, especially if exposed to magnetic fields or other sub-optimal storage locations. The chance to lose data increases over time, for example: USB sticks typically can retain data reliably for five to ten years, hard disks typically last five years and rewritable CD/DVDs last only two to five years if self-recorded[6]. Paper is a more durable medium as long as it is kept in a regulated environment as heat, humidity and other factors could cause the paper to degrade. More resilient options, such as laser etching on plastic or metal are capital intensive.

[6] *Data storage lifespans: How long will media really last?*, Casey Morgan, https://www.storagecraft.com/blog/data-storage-lifespan/

3. Gregersen-Gono Physical Storage

3.1. Overview

This storage system utilizes ultraviolet lasers that physically etch encrypted private keys onto polycarbonate plastic cards, dispensing with digital backups altogether while the encryption protects the cards from physical theft. These cards are then stored in sealed safe deposit boxes, providing security and reliability for long term storage of sizable bitcoin amounts.

Gregor Gregersen is the founder of Silver Bullion Pte Ltd, The Safe House SG Pte Ltd (TSH) and Little Bit Pte Ltd, a bullion dealership and fintech P2P lending company, a 630-ton capacity vault and a technology company respectively, all located and based in Singapore. Prior to Silver Bullion, he was working as a Senior Data Architect for Commerzbank. Gregor has a software development and financial (including structured products) background.

Clint Gono is the lead developer of the TSH Vaulting Management System, and co-founder and director of Little Bit Pte Ltd. Prior to his involvement with the Silver Bullion Group, he was involved in software development and maintenance in the education and logistics industries.

3.2. Definitions and Description of Terms

Customer The entity which owns the goods and in which name the account is held. This can be a company, a trust or an individual.

Customer Representative A person who is authorized to execute transaction orders on behalf of the Customer. A Customer can be characterized by multiple representatives (e.g. employees of a company) or he can be the Customer himself.

Transactee A person(s) who is physically present at the vault to execute a transaction on behalf of the Customer. A Transactee is often not related directly to the Customer but executes the transaction on behalf of the Customer and often is employed by a logistics company (e.g. FedEx, Brink's, Certis Cisco in Singapore). The Transactee can also be an employee of the Customer or the Customer himself.

An Order is created and verified by the Secure Logistics Group (SL) based on a request made by a Customer Representative. Structurally an order is split into smaller tasks that are progressively executed and tracked through tickets.

A Ticket is a task to be executed by a Functional Group. Tickets are created automatically when a new order is placed or when a prior sequence order is closed. Tickets might be further subdivided into functions.

A Function is a process that needs to be completed or addressed by the relevant Functional Group before a ticket can be closed.

A Functional Group (FG) is a staff grouping at the vault. TSH requires three Functional Groups to be present and sign off to process orders. Each group is limited to do only certain tickets/functions and bear responsibility for those tickets. The color-coded groups are:

- **FG Security (S)** provides physical security, identifies individuals (in-person or during video calls), checks and records arrivals and departures, and verifies (signs) that physical shipments arriving at or leaving from the vault match the packing list and ticket lists. Security is provided by specialized third party organizations. In our case armed security is provided by the biggest Singapore Auxiliary Police - Certis Cisco.

- **FG Secure Logistics (SL)** handles primary interaction with Customers or Customer representatives. This includes setting up Customer accounts, accepting, verifying and closing orders as well as billing and all other Customer administrative tasks.

- **FG Vault Operations (VO)** is responsible for physically handling bullion and executing orders initiated by Secure Logistics. VO handles all interaction involving access to the vault proper as well as precious metals testing, cryptocurrency key generation and safe deposit box retrieval.

Minibox a small numbered "safe deposit box" specifically made to store encrypted private key Cards. Miniboxes are sealable using a one-time seal evidencing box integrity.

One-time Seal A tough plastic or metal strip used to seal a box. The seal has a unique ID and ensures that the cage or box has not been opened since, thereby guaranteeing box integrity.

Customer Encrypted Private Key Card a credit card-sized laser etched polycarbonate card. Printed on it are an encrypted private key and the address to be decrypted upon withdrawal. It allows for reliable long-term non-digital storage.

Recovery Encrypted Private Key Card another credit card-sized laser etched polycarbonate card having the same private key as the customer card, but encrypted in a different manner to be decrypted only as a backup in case of loss / damage of the customer card.

Crypto Address Confirmation Document The document is sent to the Customer when a new Crypto Storage Address was created. It contains the Address for transferring bitcoins and the Public Key for advanced functions such as multi-signature addresses.

Crypto Withdrawal Confirmation Document The document is sent after release of BTC / private key to formalize the closing of the Crypto Storage service for the Address in question.

Crypto Private Key Release Document This document is generated and sent as part of crypto withdrawal process. The Document contains the Private Key in plaintext and is password protected and only the Customer knows the password – having specified it in step II of the withdrawal process. This is not needed if the Customer just wants BTC transferred or for a partial withdrawal.

Crypto Release Room is a room optimized for teleconferencing with CCTV coverage and a Blue System Terminal where minibox seals are cut, and bitcoins / private keys are released to Customers remotely.

Broadcaster is a tablet that runs custom built software for the secured broadcast of crypto transactions during a crypto withdrawal or the secured release of private keys (see section 3.5.3 for further information). The broadcaster was called "decryptor" in earlier version of this standard.

Recovery Storage is an armored cabinet where recovery encrypted cards are inserted into a one way opening slit. The cabinet is stored within a secured strongroom in an off-site location, and can only be accessed in exceptional circumstances if a recovery process is required. The existence of a recovery card is important for reliability purposes and it poses a minimal security impact as no personnel in the facility could decrypt the cards.

Blue System is a high security local area network, server and blue terminals that comprise the vault management system. The Blue System controls all processes, split into tickets divided among Functional Groups, inside the facility. For security purposes the Blue System is an offline system, meaning that it is physically disconnected from outside networks and the Internet. Communication between Blue and Red System occurs via manual encoding, QR codes or physically printing of documents to be later scanned by the Red System.

Red System is a lower security local area network, server and terminals that are connected to outside networks and the Internet. Vault staff utilizes the Red network to communicate with Customers.

Private Key the randomly generated number that allows the sending of bitcoins out of a given cryptocurrency address. The private key is the security equivalent of a bank account, password and security token device combined into one. Whoever knows the private key essentially owns the bitcoins in the corresponding address.

Public Key is mathematically derived from the private key and can be used for advanced functions such as multi-signature addresses.

Pre-approved Withdrawal Address is an optional address provided by the customer upon account opening, and changeable afterward via teleconference verification, to expedite the sending of funds to a customer.

Address / Wallet Address is mathematically derived from the public key and is required to be able to send bitcoins. It can be thought of as your bank account number equivalent.

Multi-signature Address is a special kind of address that is created from multiple public keys and allows for multiple private keys to be needed to release coins. Refer to section 3.6.13 (Multi-signature Addresses) for more details.

3.3. Ensuring Processes' Certainty

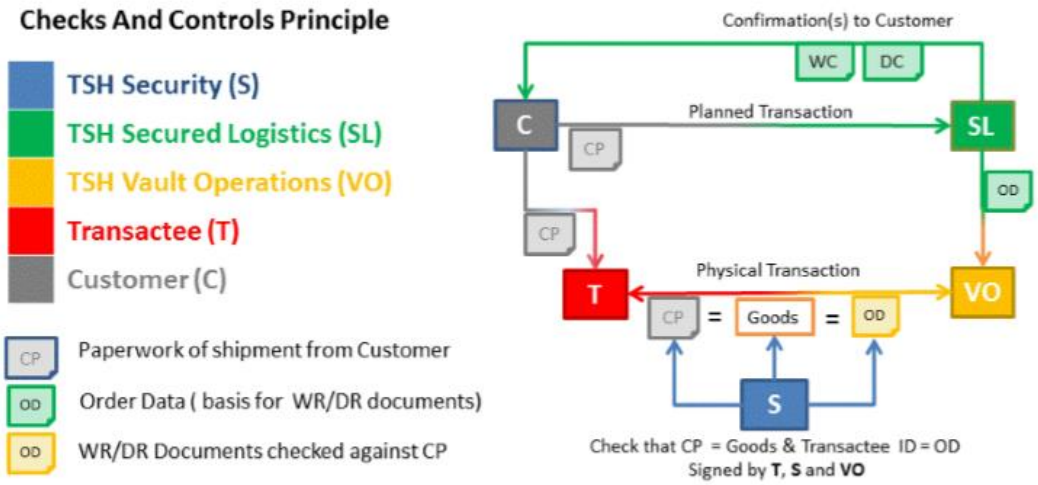
The processes described in this document ensure that each Functional Group is being checked by one or two other Functional Groups during order executions. This is achieved by splitting orders into smaller processes that are referred to as tickets and assigning ticket execution to separate Functional Groups.

Each functional group has a certain set of duties, Secure Logistics (SL) for example deals exclusively with Customers and initiates withdrawal and deposit orders while Vault Operations (VO) deals exclusively with Transactees and handles the physical movement of goods. The Security Functional Group (S) provides physical security as well as identification of Customers and Transactees as well as checking that the seal of goods is correct as per paperwork / ticket.

By Interlacing the Functional Groups via tickets and requiring Functional Group sign-off the Vault Management System ensures processes are always followed, as paperwork or release codes cannot be generated without following processes. In this paper the primary crypto orders and their constituent tickets are detailed.

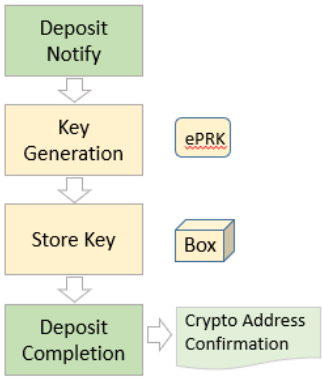
For Crypto Storage, the Transactee and Customer are typically the same entity as no logistics transport is needed for Crypto Storage. The division of roles still holds true however, as Secure Logistics is the one interacting with the Customer (Planning Transaction) while Vault Operations handles the key generation, storage and are part of the release clearance (Physical Transaction) with Security being part of the release clearance.

The system is illustrated in the color-coded schematic below:



3.4. Crypto Deposit Order (Private Key Generation)

A Crypto Deposit Order process consists of four tickets.



The Secure Logistics group (green) handles communication with the Customer, starting with the Notify Deposit Ticket and later closing the order by sending the Crypto Address Confirmation document to the Customer.

The Vault Operations group (yellow) handles encrypted key card generation and storage of the card tickets. The encrypted private key, address and minibox ID are assigned automatically by the Blue System, only the Seal ID is set by the VO group.

3.4.1. Deposit Notify Ticket

An order is started when a Customer account requests a new crypto address to be opened using a standard communication option.

The following options are also determined:

- Type of cryptocurrency (e.g. BTC or Ethereum)
- Optional liability protection / insurance amounts

Once Secure Logistics confirms the order, the Notify Ticket is closed and the Key Generation ticket is opened for vault personnel.

3.4.2. Crypto Key Generation Ticket

Vault Operations will activate the "Create Key" function which generates the following:

- Customer Encrypted X Private Key Card for Laser Etching
- Backup Encrypted Y Private Key Card for Laser Etching
- Crypto Address Confirmation PDF

The private key is generated in memory along with the public key and the address. See "Private Key Entropy" section (3.6.1) for details. The private key is then immediately encrypted using two encryption algorithms (Customer and Recovery) and the plaintext is flushed from memory. For transparency purposes the code handling the key generation, encryption and flushing will be open sourced and published on github at https://github.com/littlebitpteltd once the service is officially launched.

The public key and the address are then stored permanently in the Blue System to generate the Crypto Address Confirmation document, while the encrypted Customer and Recovery Private Keys are etched using laser on their respective polycarbonate

plastic cards and are then flushed, as are the laser etcher records (refer to Key Generation Function section for additional details).

This process ensures that no private key data is stored anywhere in digital format, and only the public key and address are stored on our secured offline vault management system (Blue System). Upon completion of the etching, Vault Operators will perform a quality check on the etched card with a separate Verifier tool, close the corresponding ticket and open a "Crypto Store" ticket.

3.4.3. Store Key Ticket

In this step the Encrypted Customer card is placed in its minibox or card container and sealed. The minibox is then assigned a secure storage location and optional liability protection or insurance is applied.

The minibox is intended for long term physical storage and will not be removed until box closure / private key withdrawal request by the Customer is requested. The "Crypto Deposit Ticket" is closed and a "Close Crypto Deposit Ticket" is opened for Secure Logistics to process.

The two vault operators who processed the storage also physically sign the Crypto Deposit Confirmation which will be later scanned and mailed to the Customer.

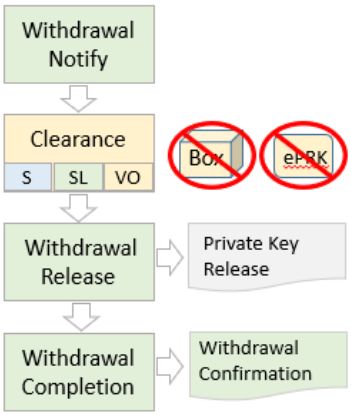
3.4.4. Deposit Completion Ticket

Upon Crypto Storage Confirmation, Secure Logistics will also sign the Crypto Deposit Confirmation and scan the document on the red network for sending to the Customer.

The primary concern in this ticket is that the Crypto Address Confirmation Document is indeed received by the Customer. Upon confirming receipt of the document by the Customer, Secure Logistics will close the Order and upon receipt the Customer can transfer bitcoins into the new physical bitcoin address.

3.5. Crypto Withdrawal Order (Private Key Release)

A Crypto Withdrawal Order has four steps.



The Secure Logistics group (green) handles communication with the Customer, operates the broadcaster and completes the withdrawal paperwork.

The Vault Operations Group (yellow) is part of the clearance process, retrieves the minibox, breaks the seal and retrieves the Customer Encrypted Private Key Card.

The Security Group (blue) is part of the clearance process to verify the identity of the customer.

3.5.1. Withdrawal Notify Ticket

This ticket is opened by Secure Logistics and confirms with the Customer the date and time of withdrawal, address and whether the withdrawal will be in-person or remote.

Upon confirming the date and time, Secure Logistics will close the Withdrawal Notify ticket which will open three new sub-tickets:

- a **Security Withdraw Clearance Ticket** for security, specifying the release date/time and Customer ID to verify.
- a **Vault Operator Withdraw Clearance Ticket** for Vault Operations specifying the date/time for release, box ID and Seal ID.
- a **Secure Logistics Withdraw Clearance ticket** for Secure Logistics specifying the date/time for release and Customer.

The ticket also requires the printing of the Crypto Withdrawal Confirmation document to be signed during the upcoming release process.

3.5.2. Withdrawal Clearance Ticket

At a pre-determined release date / time, a video call with the Customer is established originating from the crypto release room.

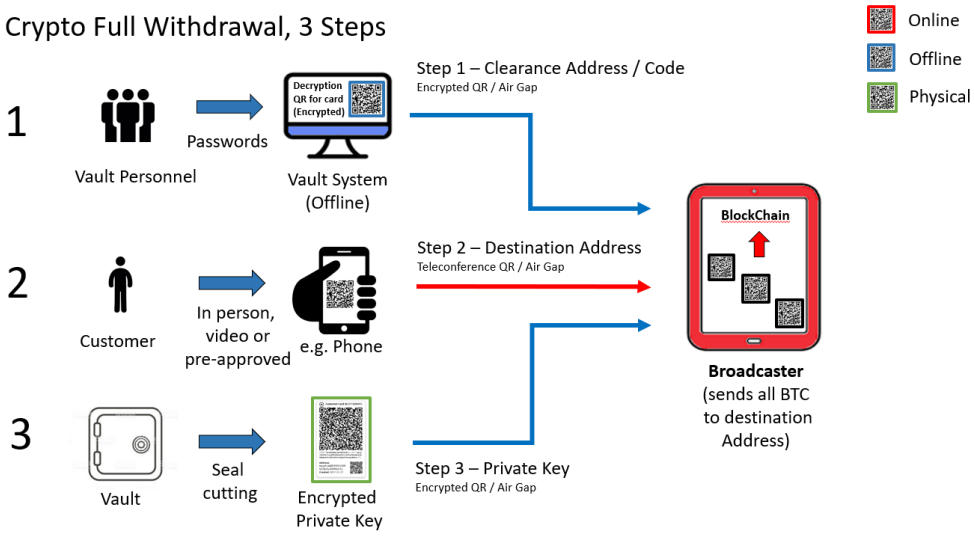
In the crypto release room, Security, Vault Operations and Secure Logistics representatives will be present as per release rules. Vault Operations would have brought the sealed minibox as identified by Box / Seal ID. Secure Logistics would have brought the unsigned Crypto Withdrawal Confirmation document for the pending release.

The customer is then contacted via a video call and his identity verified by the functional groups as per the verification process. Once verified, each group representative will close their respective clearance tickets and sign the Crypto Withdrawal Confirmation document. An alternative to teleconferencing with the customer is to utilize pre-approved withdrawal addresses provided by the customer upon account opening. The Blue System will then generate an encrypted clearance QR code to initiate the decryption process.

3.5.3. Withdrawal Release Ticket – Full Withdrawal

The broadcaster is a tablet that runs custom built software for the secured release of private keys and bitcoins directly to customers during a crypto withdrawal. The broadcaster is the only tool in the Crypto Storage system that is not permanently offline.

The broadcaster is designed to minimize the chance of errors or fraud attempts by using encrypted QR codes. The broadcaster is kept simple and transparent by design, requiring only 3 sequential QR scans as illustrated in the graphical chart below:



Each step is now explained in greater detail:

3.5.3.1. Step 1 - The Clearance QR Code and Minibox Opening

The clearance QR code, itself encrypted to prevent alteration, is generated after customer identification is confirmed by three vault personnel, each of whom vouch for correct identification by confirming their passwords in the Blue System. This code contains the card specific decryption key as well as eventual outstanding fees and a time window for the decryption.

The broadcaster tablet is used to scan the clearance QR code. Transmitting data via QR code provides a one-way air-gapped data transmission between the Blue (offline) and Red (online) system.

This process ensures that the broadcaster tablet will only be able to decrypt a card if the release process is followed, as the tablet itself does not store decrypted keys, making the tablet useless to steal.

Note that at this point the broadcaster tablet has a card specific decryption key (which only works for the card to be released) provided by the clearance QR code but does not have the encrypted private key nor a destination address to release bitcoins to.

Vault Operations will now commence cutting the seal to retrieve the Customer Encrypted Private Key Card.

3.5.3.2. Step 2 – Obtaining the Customer's "Release To Address"

The customer's "Release To Address" is obtained by requesting the customer to show the QR Code of the destination address (e.g. an address generated by a wallet or a paper printed QR code) during the video call. The broadcaster

will then scan the QR code over the video connection (in person if the Customer is at the facility).

Note that this mechanism is an elegant way to eliminate potential man-in-the-middle (MITM) attacks by third parties while being convenient, secure and reliable.

An alternative to providing an address via video call at the time of withdrawal is for the customer to provide a preapproved "withdrawal address" upon account opening. Should a withdrawal address be changed afterwards, a video call to identify the customer would be required to verify the address change. If a withdrawal address is specified, withdrawals to this address will not require a separate video call.

3.5.3.3. Step 3 – Decryption of Private Key / Release Funds

At this step, the broadcaster has a release authorization and a destination/release address. Secure Logistics personnel will now confirm the crypto amount to be sent minus eventual outstanding fees and the destination address's last five digits with the user / Customer.

Lastly, the Customer Encrypted Private Key Card, which was just unsealed by Vault Operations, will be scanned by the broadcaster. Upon scanning and decrypting the Customer's private key, the broadcaster will immediately release the funds to the user's destination address.

By sending the funds immediately using air-gapped encrypted QR codes and never storing the private key digitally, the decryption process minimizes the available points of attack by malicious third-parties.

There will be cases however, whereby the Customer does not wish to send BTC out or there is no balance in the address. An example of such a scenario would be that the private key is used by the customer as part of a multi-signature address. In such cases, no BTC will be sent and the system will proceed to the Private Key Release phase.

The Private Key Release cannot occur via decrypted QR as was done with the "release to" address - due the continued security sensitivity of the private key. Therefore, the broadcaster will generate a password protected file which can be accessed only with the PRK Document password which only the Customer has. The document is then transmitted to the Customer via secured communication.

The video call is then concluded and the Withdrawal Closure Ticket is opened next.

3.5.4. Withdrawal Release Ticket – Partial Withdrawal

Partial withdrawals allow for only a portion of the cryptocurrency stored on a card to be withdrawn. Advantages include:

- **Flexibility**: It is not necessary to make new addresses / cards every time a small withdrawal is needed.
- **Usability**: Most customers prefer to have a fixed address they can deposit and withdraw from rather than keep track of their latest address. This is also a requirement for Secured Peer to Peer Crypto Lending.
- **Security:** Although it is technically considered a good practice to create a new address on every withdrawal, frequently changing the addresses greatly increases the chances that customers might send funds to old addresses by mistake. Allowing for more permanent addresses minimizes this risk.

Unlike a full withdrawal, the customer card will still be in use after a partial withdrawal. It is, therefore, important to ensure that the private key of the account remains protected even after the partial withdrawal.

Taking this security requirement into account, the customer card decryption mechanism and the blockchain broadcasting mechanism needs to be on separate machines, one being offline (so that the private key is never read by an online machine) and the other being online (to broadcast to the blockchain) respectively.

To accomplish this, a partial withdrawal involves the use of an online broadcaster device that generates and later broadcast the transaction onto the blockchain and an offline *verifier* device that signs a transaction using the private key.

Communication between these devices occurs using air gapped QR codes as follows:

3.5.4.1. Generate an Unsigned Transaction

Step 1 - Like a full withdrawal, a partial withdrawal ticket will require the visual verification of the customer (via a video call or in-person) by vault personnel or a pre-approved withdrawal address. Once verified, the Blue System will generate an encrypted Metadata QR code containing the following data:

- Card Address – The crypto address from which funds are to be sent
- Card ID – The internal ID of the Card
- Reserved Function
- Crypto Type – Crypto Currency Type, such as Bitcoin, Ethereum, etc...
- Transaction Type – e.g. Partial Withdrawal

- Valid Until – A date/time field to during which time the transaction can be performed. This prevents the potential unauthorized re-use of a Metadata QR code.

The above data is encrypted using AES-256 before it is rendered as a Metadata QR code, thereby ensuring that:

- The data cannot be read by any device other than the broadcaster device which has the QR Metadata decryption key.
- The Metadata QR code data cannot be modified by a man-in-the-middle attack nor can a fictitious code be generated by an unauthorized tool.
- The Metadata QR code cannot be re-used multiple times as the 'valid until' time limit will prevent re-use. The broadcaster ensures its time is accurate by checking current time online. Typically, the time limit is set to 20 minutes from issuance of Metadata QR code.

The above described security mechanism is used every time a Metadata QR code is generated. In our process diagrams, this process is referred to as "Encrypted QR / Air Gap". It ensures data integrity and safe data transmission between online and offline systems.

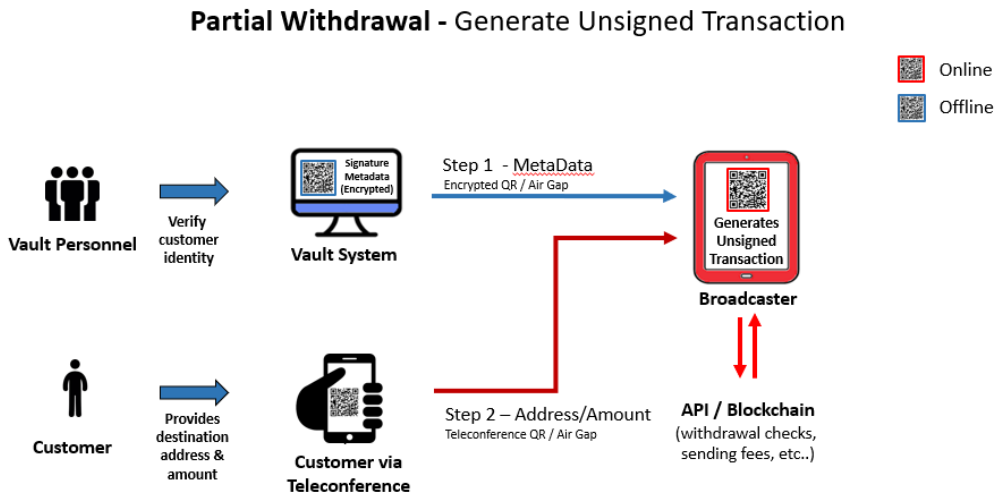
Step 2 – Once the encrypted Metadata QR code is scanned by the broadcaster the following data is displayed by the broadcaster, some being retrieved online:

- Crypto balance, type and valuation in USD / SGD
- Eventual crypto balance locked as collateral for P2P loans
- Eventual unpaid storage fees
- Card ID
- Select Customer Details

The vault personnel will then request for the destination address and amount to be sent from the verified customer during the video call. The destination address will be scanned using the broadcaster over the video call by having the customer show a QR code of his destination address. The customer will then specify how much crypto is to be sent to this destination address. Alternatively, a pre-approved withdrawal address can be used, in such a case the amount will be provided by the customer in a withdrawal form.

The requested crypto amount will be entered by vault personnel into the broadcaster device. Note that this is the only manually entered data of the withdrawal ticket process. The broadcaster will verify that enough funds are available for sending and, depending on crypto currency, add an eventual blockchain sending fee to ensure timely delivery.

The broadcaster device will then generate the unsigned transaction string and encrypt it using AES-256 to produce the encrypted unsigned transaction QR code which will then be prominently displayed on the broadcaster screen.



3.5.4.2. Sign and Broadcast Transaction

The unsigned transaction now needs to be signed as follows:

Step 1 – Vault personnel uses the offline verifier device to scan the encrypted unsigned transaction QR from the broadcast device which initiates the signing process.

Step 2 – Vault personnel scans the card specific decryption code from the vault system which allows the decryption of the encrypted private key on the Customer Encrypted Private Key Card in the next step.

Step 3– Vault personnel scans the Customer Encrypted Private Key Card to decrypt the private key which is needed to sign the transaction.

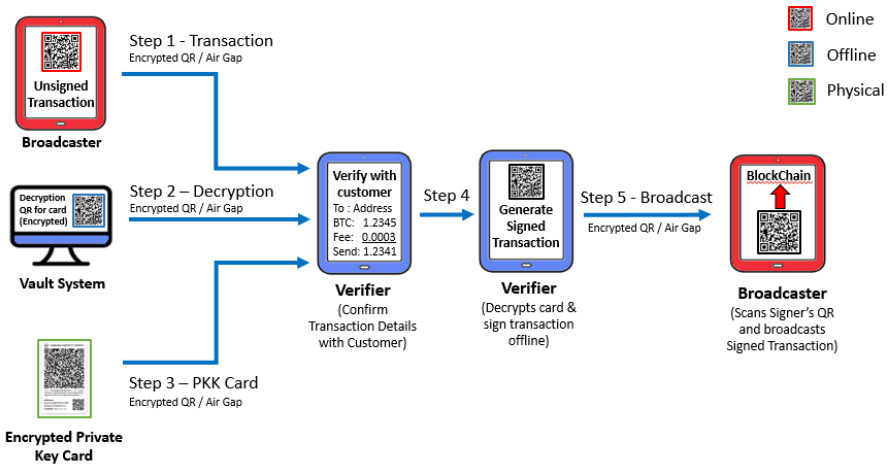
Once the Customer Encrypted Private Key Card is successfully scanned, the verifier will provide a transaction summary. Note that using the wrong private key card would cause a decryption failure here. In case of a video conference the Vault personnel will use this summary to reconfirm with the customer on:

- The destination address
- The net amount to be sent

Step 4 – Upon confirmation, the Verifier will display the encrypted signed transaction QR which is ready to be broadcasted to the blockchain.

Step 5 – Vault personnel will use the broadcaster to scan the signed transaction QR from the verifier. Once scanned, the broadcaster will broadcast the transaction onto the blockchain, thereby completing the withdrawal process.

Partial Withdrawal - Sign and Broadcast Transaction



3.5.5. Withdrawal Completion Ticket

Secure Logistics will scan and send the signed Withdrawal Confirmation via the Red network. Upon confirming receipt of the document by the Customer, Secure Logistics will close Withdrawal Closure Ticket and thereby conclude the Withdrawal Order.

3.6. Selected Process Details

3.6.1. Private Key Entropy

Given a blockchain's truly distributed architecture, the creation of private keys and addresses can be done offline using well known, publicly available algorithms.

Of great importance in this process is utilizing private keys that have enough true randomness (entropy) so that the keys are extremely difficult to reproduce. A good random crypto key is mathematically almost impossible to reproduce and therefore very safe from external attackers trying to guess a private key on the blockchain.

We utilize FIPS 140-2 certified (Security Requirements for Cryptographic Modules) offline crypto libraries (RNGCryptoServiceProvider) to ensure high entropy keys are generated and, after etching, we delete them from all digital media. This process is open sourced and can be downloaded at https://github.com/littlebitpteltd once the system is launched.

3.6.2. Private Key Security

Private keys are created, encrypted, physically etched and deleted from memory on the offline Blue System as part of the Crypto Key Generation Ticket. It is important to take note of the following:

- The key generation occurs on a hardened offline network (Blue System) making direct remote access impossible.

- The private keys are created and immediately encrypted in DRAM memory within the same process that generates the key. At no point is the unencrypted key stored elsewhere.

- The encrypted keys are sent to the laser for etching. Upon etching and verification, the encrypted keys are then deleted from memory. The laser uses volatile memory to hold its etching image and the data will also be flushed upon completion.

- The complete process occurs within the lifespan of the Crypto Key Generation Ticket and is typically concluded within 15 minutes.

Given the offline system and immediate key encryption and plaintext flushing it is practically impossible for an attacker to obtain access to these private keys remotely.

3.6.3. Customer Encrypted Key Card

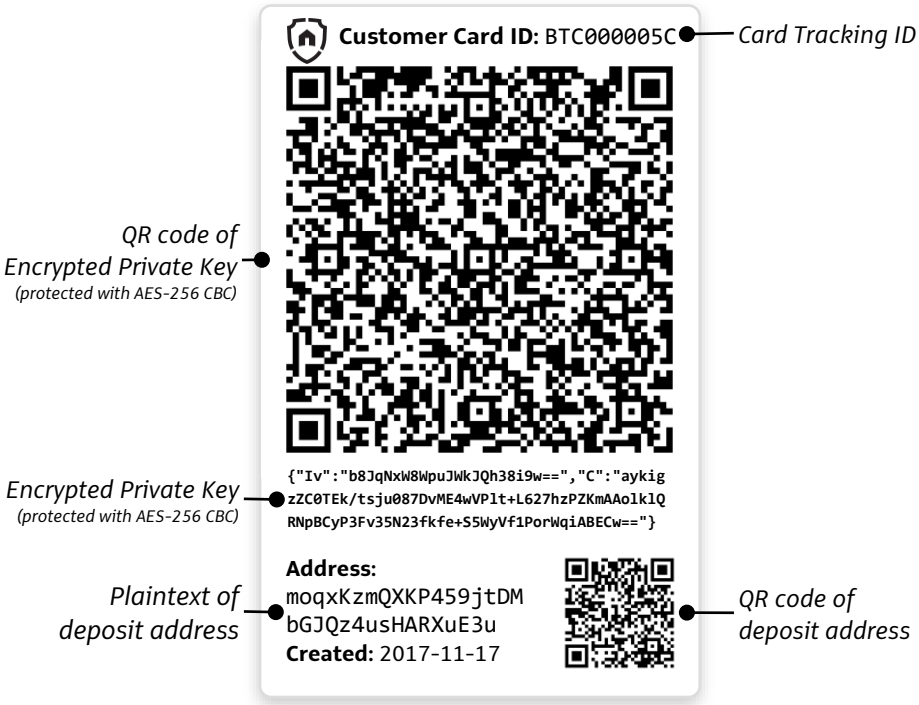
For **security** reasons, private keys are not stored in any kind of digital format. Instead, an ultraviolet laser is used to irreversibly etch the encrypted (Customer) private key onto a highly durable polycarbonate plastic card. The encrypted private key (PRK) is written in alphanumerical format as well as QR code for easy scanning.

The customer private key is encrypted at the top section of the card using AES-256 in CBC (cipher block chaining) mode, using a different encryption key for each card. Each card's encryption key is itself encrypted on the offline Blue System database and identified by card ID and address. Note that the encryption key is useless without the physically stored Customer Encrypted Private Key Card and the Customer Encrypted Private Key Card is useless without the database encryption key which is retrieved only upon following the Crypto Withdrawal procedure detailed separately.

The encryption ensures internal security and makes the theft of the card itself useless, as only the broadcaster tablet can decrypt it. Stealing a broadcaster tablet plus a customer card will also serve no purpose as the decryption key for a given card is passed from the Blue System as part of the clearance code. Therefore, adherence to the full Crypto Withdrawal ticketing process and functional group participation (as described earlier in this paper) is always required.

On the lower part of the card, the address is etched as a QR code and in plaintext. Additional information is the date of etching and an internal card tracking code.

This card will then be physically slotted into a custom design minibox and sealed with a tamper evident seal.



Customer Encrypted Key Card

3.6.4. Customer Encrypted Key Card Storage

Once etched and verified, the Customer Encrypted Private Key Card is slotted into its assigned protective Minibox or Multicard box for long term storage. The box is then sealed with a one-way numbered seal which provides proof of box integrity.

The Minibox or Muticard box is then stored within a Class II Vault safe deposit box as assigned by the Blue System and recorded on the Crypto Address Confirmation Document which will be signed by the vault operators depositing the document.

Protective Miniboxes for long term physical storage

Seals provide proof of box integrity

Sealed boxes are then stored within a class II vault

3.6.5. Recovery Encrypted Key Card

For **reliability** reasons, the private key for each Customer Encrypted Private Key Card is also etched onto a Recovery Encrypted Private Key Card. The Recovery Encrypted Private Key Card is essentially a precautionary measure in the unlikely event that the Customer Encrypted Private Key Card should be lost or damaged.

Recovery Encrypted Private Key Cards utilize a different asymmetric encryption process (RSA-2048) thereby generating a different encrypted alphanumerical string and QR code. Asymmetric encryption means that data can be encrypted without needing a decryption key during encryption. This is important as, for security and reliability purposes, the recovery broadcaster key is not located in the storage facility, therefore the Recovery Encrypted Private Key Card cannot be decrypted there.

This encryption means that neither potential thief nor vault personnel itself can decrypt the Recovery Encrypted Private Key Card. Instead, a specialized recovery process would be initiated in the very unlikely event of the loss of the Customer Encrypted Private Key Card (Recovery Process in 3.6.6).

For reliability purposes, Recovery Encrypted Private Key Cards are securely stored offsite in an armored "recovery box" custom built with a slit that allows the one-way insertion of the Recovery Encrypted Private Key Cards. The Recovery Encrypted Private Key Card has a similar layout and functionality as the Customer Encrypted Private Key Card and used the same Card ID with an "R" to indicate recovery.

Recovery Card

3.6.6. Recovery Process

The Recovery Encrypted Private Key Cards are stored in our strong room in the headquarters of the Singapore Auxiliary Police (Certis Cisco) in whose building our primary office is located (4 km from the vault). Off-site storage of the Recovery Encrypted Private Key Cards increases reliability in case of fires or other location specific disasters.

Recovery cards are inside an armoured cabinet having a small one-way slit into which the recovery cards are inserted for long term storage. This is akin to a check deposit boxes used by banks. The cabinet is locked and sealed via numbered seal, under 24/7 CCTV coverage. Access to the strong room itself is secured via facial recognition and access card verification.

For a recovery, the following items are necessary:

- The Specific RSA 2048 Encrypted Recovery Card(s) to be recovered
- The Recovery Decryption Clearance Card
- The Verifier/ Decryption Device

Recovery Card Retrieval: During a recovery, the armoured cabinet would be opened by at least 2 vault operators and a director. The relevant Recovery Encrypted Private Key Card would be retrieved based on its Card ID / Address. The cabinet would then be re-sealed with a new numbered seal.

Recovery Decryption Key Retrieval: The Recovery Decryption Clearance Card is stored in a third-party – Singapore Auxiliary Police (Certis Cisco) Safe Deposit Box which requires two directors to access.

The Verifier would be brought from the vault by vault personnel. Should no verifier be available at the vault, a new verifier would first need to be set up by Little Bit.

Once all items are retrieved, the verifier tablet would scan the Recovery Decryption Clearance Card followed by a scan of the Recovery Encrypted Private Key Card.

The verifier would then generate a new Customer Encrypted Private Key Card Image to replace the lost customer card. This image can then be utilized by the standard customer verifier to release bitcoins or retrieve the private key.

3.6.7. Crypto Address Confirmation Document

This document is generated and printed by the Blue System after the laser etching process is completed and verified. The document confirms the creation and verification of the Customer Encrypted Private Key Card and lists the public key and address that have been generated.

The document also lists the safe deposit box number where the Customer Encrypted Private Key Card is secured as well as three signatures, two being from vault personnel and one from Secure Logistics. This document will be later scanned on the Red System and securely sent to the Customer.

The **address** in this document can be used to securely send and store bitcoins knowing the that the encrypted private key is safely stored on a durable polycarbonate plastic in a sealed safe deposit box inside a highly secured premise (Reliability) and no copy of the data is in stored in digital format anywhere (Security).

The **public key** can be optionally used by advanced users to create multi-signatory addresses for additional security or to create secondary addresses for additional privacy.

3.6.8. Crypto Withdrawal Confirmation Document

This document is generated and printed by the Blue System upon Withdraw Notify Ticket, is signed during release clearance and later scanned and sent to the Customer as part of the Withdraw Closure ticket by secure logistics functional group.

The document confirms the closure / withdrawal of the private key, breaking of the associated numbered seal and specifies the closed minibox. The document contains three signatures from the function groups involved in the withdrawal clearance.

3.6.9. Private Key Release Document

This document will be generated by the broadcaster upon step 3 of the Broadcaster Release Process. It contains the decrypted (plain text) Private Key of the Customer. To protect the document from both vault personnel and third parties, the document is password protected using a password chosen by the Customer in step 2 of the Broadcaster Release Process. A more detailed Implementation of the Private Key release system will be described in a future Gregersen-Gono revision.

3.6.10. Communication Options:

High Security Authentication Options for / Crypto Withdrawal

- Encrypted Video Link with verification (see section 3.6.11, Customer Video Verification)
- Customer being at facility in person

Secured transmission for Address Confirmation / Withdrawal Confirmation Documents:

- Transfer PDF via Encrypted Instant Messenger:
- Transfer Password Protected PDF via e-mail with password sent via SMS

Standard Communication

- E-mail
- Phone
- Messenger

3.6.11. Customer Video Verification

When a video call with the Customer is established, the Customer is identified visually by comparing his appearance with the passport copy on record.

This visual identification is designed to prevent attackers, who might have compromised the Customer's e-mail, from successfully impersonating the Customer.

In addition to the physical appearance, the following verification request can be requested live during the video call to further ascertain his identity:

- Request Customer to present his physical passport or ID while on video
- Call the Customer on his phone number on record while on video
- Send a verification code over SMS to his phone to be repeated on video
- Other options as determined by Secure Logistics, depending on Customer / situation

3.6.12. Clearance Group Representatives

To generate the Clearance QR Code from Blue System in order to initiate the broadcaster, the following signatories are needed:

- For Customer Decryption Release / Crypto Withdrawal signatures
    - 1 x Secure Logistics + 1 x Vault Ops + 1 x security (default)
    - 1 x Secure Logistics + 2 x Vault Ops
- For a Recovery Decryption
    - 1 x Secure Logistics + 1 x Vault Ops + 1 x **administrator**

3.6.13. Multi-signature Addresses

Multi-signature addresses are addresses which require X/Y Private Keys to release bitcoins, where X is the number of required private keys to release bitcoins and Y is the number of participating private keys. For example:

- A normal bitcoin address is essentially a 1/1 as it requires one private key and it only has one private key.
- A multi-signature 2/2 address would have two private keys and both are required to release bitcoins.
- A multi-signature 2/3 address would have three private keys of which any two are required to release bitcoins.

To create multi-signature addresses, only the public keys of participating private keys are needed. A sufficient number of private keys are then needed to release bitcoins.

For example, a customer could use the public key (sent via the Crypto Address Confirmation Document) along with his own separately stored public/private keys to create multi-signature addresses to store bitcoins in. For example:

A 2/2 address would increase security against unauthorized withdrawals as neither the Vault Stored Private Key nor the Customer's private key is enough by itself to release bitcoins. The downside is that reliability suffers, as a loss of either private key will result in the bitcoins become permanently inaccessible.

A 2/3 address could make sense if two separate customers need each other to approve a bitcoin release and utilize the vault stored key as a backup, in case one of the customers lose their private key.

Multi-signature addresses can be a very powerful tool but they should not be used by a crypto storage system itself because multi-signature addresses cannot be nested. Nested in this context means that it is not possible for a multi-signature address to be made up of another multi-signature address.

Therefore, any storage system that uses multi-signature addresses prevent the client from using this powerful capability.

Because of this reason the Gregersen-Gono Standard does not utilize multi-signature functionality as it would provide very little additional security given the extensive encryption system. Instead the public key is made available to customers thereby allowing advanced users to make their own multi-signature addresses and thereby taking full advantage of bitcoin multi-signature capabilities.

4. Threat Scenarios

4.1. DIY Mishandling (Protection Against)

By outsourcing the private key storage, a customer does not need to worry about securing the private key as he is subscribing to a service rendered by the storage system.

However, advanced users might choose not to use the bitcoin address created for them and instead use the public key as part of a multi-signature address and transfer funds into the multi-signature address instead.

In a typical 2/2 multi-signature address arrangement this would mean that the customer would need the Gregersen-Gono secured private key in addition to his own private key to release funds from the given address.

While such an arrangement increases security, it can lower reliability, because there is a risk that the customer might lose his own private key, in which case the bitcoins in the multi-signature address would be lost. Advanced users must be aware of the potential DIY mishandling risk involved with multi-signature addresses.

4.2. Counterparty Risk (Protection from)

This is the risk that something goes wrong within the vaulting storage provider.

4.2.1. Collusion (Protection Against)

Collusion involves personnel at a counterparty company or a counterparty's counterparty to collude with a third party to steal private keys, potentially making it look like a hacking incident.

Collusion is nearly impossible in the Gregersen-Gono Standard as all private keys are encrypted and the plaintext keys are never seen by vault personnel. The encrypted private key card is useless without a broadcaster. The broadcaster in turn can only be used with a clearance code which requires a six-eye principle and the customer presence via video call.

These processes cannot be bypassed as they are enforced by a series of tickets designed to check operations among the three functional groups as per vault management system requiring passwords from Security, Vault Operations and Secure Logistics personnel.

Note that that customer can elect to use multi-signature addresses to further increase protection against any form of unauthorized withdrawal. Refer to multi-signature addressee section.

4.2.2. Default (Protection Against)

Default / bankruptcy involves a counterparty declaring insolvency and refusing to return the cryptocurrency assets stored on behalf of customers. (e.g. Mt Gox case).

Cryptocurrencies and their private keys stored as per the Gregersen-Gono Standard is not controlled by the vault / storage provider as might be the case for an exchange or wallet.

Under the standard, the vault operator simply acts as an agent to store the crypto card for the customer and eventual bitcoins are not on the balance sheet of the vault operator so they cannot be legally defaulted upon.

Should a default of the operator occur, the bitcoins would be released to their owners by the liquidators in the same manner and the same process as gold / silver holdings would be released.

4.2.3. Theft (Protection Against)

Whereby the counterparty, or a portion of its staff, transfers out, washes the bitcoins (a process called "tumbling") and disappears.

Cryptocurrencies and their private keys stored as per the Gregersen-Gono Standard can only be released as per the withdrawal process. Theft would therefore require at least three personnel, including security (auxiliary police), to act in unison without detection by other staff.

While theoretically possible for this to occur, it would be considerably easier to steal or smuggle out physical bullion than execute decryption processes. This makes the process even less likely to occur.

Vault staff personnel are subject to stringent security procedures, are long term residents of Singapore / Singaporeans, many of whom are also shareholders in the company, and are extremely unlikely to collude.

Note that that customer can elect to use multi-signature addresses to further increase protection against any form of unauthorized withdrawal. Refer to multi-signature addressee section.

4.2.4. Incompetence (Protection Against)

Whereby private keys are published publicly, lost without possibility of recovery or other cases involving incompetence.

The Gregersen-Gono Standard uses automation, simple interfaces and includes checks at every step of the process. Critical mistakes are extremely unlikely to occur. Below is a list of the most likely critical mistakes and how they will be addressed:

- **Laser etching error causing non-readable keys**. This is addressed by:

- The card verification process which occurs immediately after etching to ensure the card has been written properly (see verification process).
- The recovery card acts as a failsafe should anything happen to the primary card.

- **Wrong customer card being scanned upon decryption**. This is addressed by:
  - The clearance code sent by the Blue System upon decryption start contains the address of the card to decrypt. If the scanned card is the incorrect card the decryption process will automatically abort.

- **Loss / Destruction of encrypted private key card**. This is addressed by:
  - The Recovery Card acts as a failsafe should anything happen to the primary card.

- **Software Error**. This is addressed by:
  - Software is extensively tested and uses standard crypto best practices / code. For transparency purposes the code for key processes will be open sourced and released on https://github.com/littlebitpteltd

- **Release to the wrong customer.** This is addressed by:
  - The six-eye withdrawal principle (at least three individuals checking) and the video call requirement makes it very unlikely that bitcoins are released to a wrong customer.

- **Wrong system input / typos.** This is addressed by:
  - The Gregersen-Gono process eliminates / automates most user input that could have typos. The sensitive withdrawal process for example consists only of QR code scans and all documents are re-confirmed by multiple functional groups and the customer themselves. The only text input is the amount to be withdrawn in case of partial withdrawals.
  - The Vault operating system is built to catch errors by requiring multiple Functional groups to reconfirm / check input from each other.

4.3. Third Party Hacking (Protection from Digital Theft)

Hacking in this context is defined as taking advantage of security lapses at the storage provider to remotely obtain access to unencrypted private keys which would allow an attacker to take ownership of the bitcoins. The attack vectors are categorized below.

4.3.1. Exploiting Technical Weaknesses (Protection Against)

Physical crypto storage is essentially immune to traditional hacking attempts as the private keys are not stored in digital format anywhere. The only use of computers, attack vectors, occurs in the following instances:

- **Key Creation.** This occurs on a secured offline computer. The generated key is immediately encrypted in volatile memory, laser etched and destroyed. The key is never written into permanent storage. Attack opportunity is virtually none. See Private Key Generation (section 3.6.2).

- **Physical Etched Key Verification.** This occurs on an offline verifier device which only verifies that the encrypted text is readable on the laser etched polycarbonate card no sensitive data is stored. Attack opportunity is virtually none.

- **Bitcoin / Private Key Release** This occurs during the video call with the customer upon positive identification (see release process). The broadcaster will connect to the blockchain secured by a MAC address and VPN. In addition, the private key will only be read and decrypted from the physical card at the last moment upon sending the bitcoins out and will then be immediately deleted from memory. In case of partial withdrawals, the broadcaster utilizes offline signed transactions thereby ensuring that the private key is not decrypted on the online broadcaster. Opportunity for an attack is therefore extremely low.

The "physicality" of the system means that a decrypted private key is on an online system for a few seconds only upon account closure if the private key needs to be transmitted. This system ensures highly effective and reliable protection against any kind of technical exploit. Physical storage is virtually hack-proof.

4.3.2. Impersonating the Customer (Protection Against)

In practice, customer impersonation might be the greatest security threat to the Cryptocurrency Storage Industry. An attacker has access to a customer's smartphone for example typically would get control of the customer's e-mail and phone connection which in turn bypass most online security precautions.

In such a scenario two-factor authentication would be useless as would the vast majority of other security precautions. The Gregersen-Gono Standard addresses this issue by requiring a visual identification of the customer over a video call or in-person, or based on customer choice a pre-approved withdrawal address.

The identification is based on a 6-eye principle as per vaulting release processes and can be further enhanced by requiring the customer to show his photo ID over the video connection or using a 2-factor authentication of his phone live over the video connection.

The video call release requirement greatly increases security against impersonation attempts, especially since attackers are unlikely to want to risk exposing themselves

in a video call. Customers will need to book a video call appointment during Vault operation hours, reducing convenience.

4.3.3. Impersonating the Counterparty (Protection Against)

TSH vault has a minimal online presence as sensitive data is on the offline Blue System. The primary concern here is a third party trying to impersonate TSH and sending a forged e-mail and documents that a customer might believe to be from TSH.

To be effective, such attacks only work if the attacker knows that the client has the intention to open an account and sends documents containing addresses controlled by the attacker. The attacker would also need to intercept and hide communication from TSH to the customer, so he would likely need to already have control over the client's e-mail accounts.

The best defense against such eventualities is for the customer to reconfirm with TSH Secure Logistics the last or first 10 digits of the address.

4.3.4. Intercepting Communications (Protection Against)

To avoid a man-in-the-middle attack (MITM), TSH encrypts or password protects sensitive information with the customer. For expected large transactions or for heightened security, it is possible to re-confirm received communications (e.g. last 10 digits of an address) with TSH Secure Logistics via phone call or via SMS.

4.4. Private Key Loss Risk (Avoiding)

This is the risk that the storage provider somehow loses the customer's private key(s).

4.4.1. Physical Loss of the storage medium (Protection Against)

The physical cards must be stored in a safe location to minimize the risk of loss.

In the case of TSH, the encrypted private keys are stored within miniboxes sealed with numbered one-time heavy-duty metal seals or multicard boxes. These boxes are in turn are stored within Class II safe deposit boxes which themselves are stored in a Class II vault consisting of composite steel walls, ceiling and floor that are each a foot thick (30cm). The Class II vault is located within a much larger Class I vault (TSH) located in Singapore and secured by the Singapore Auxiliary Police.

Should a loss still occur, the Gregersen-Gono Standard has a recovery card etched for each Customer Encrypted Private Key Card (see recovery card) to provide a fallback in the unlikely event that the Customer Encrypted Private Key Card should be lost or destroyed.

4.4.2. Degradation of the storage medium (Protection Against)

Physical storage implies long-term storage of crypto, requiring a storage medium that can reliably store a private key over many decades without degradation or

becoming illegible regardless of conditions. Loss of the private key would be disastrous for cryptocurrency storage.

Digital storage such as hard disk and flash drives for example are sensitive to magnetic sources and could even be wiped clear by a recurrence of strong solar flares. These types of storage media, along with tape and CD/DVD also degrade over time and have a high chance to lose data beyond the 5-year mark.

Paper is sensitive to humidity, UV light and heat. Ink-based printing can smear, fade or decay over decades. Laminating paper will improve survivability over time but is sub-optimal for long term storage.

The Gregersen-Gono standard utilizes an ultraviolet laser to irreversibly etch the encrypted key with precision onto a polycarbonate plastic card. The encrypted key is written twice - once in alphanumeric format and once as a QR Code for easy scanning.

The UV laser physically changes the physical properties of the polycarbonate surface in an extremely precise manner, with no ink to decay or smear. The polycarbonate material is a durable plastic (also used for bullet proof panels) which is further protected in the miniboxes or multiboxes within the vault, allowing it to last for centuries.

Conclusion & Notes

As of December 15th, the standard is approaching implementation. Feedback and improvement suggestions are greatly appreciated and are best directed to info@littlebit.sg.

Details on the standard implementation at The Safe House SG Pte Ltd and an overview video of it can be found at https://www.thesafehouse.sg/physical-crypto-storage and The Safe House's parent company Silver Bullion Pte Ltd will soon be the first company to offer the service to customers. Service details can soon be found at https://www.silverbullion.com.sg/Info/StarStorage

This crypto standard as described can be freely adapted by third parties, however using the term "Gregersen-Gono Standard" will require full implementation of the critical standard components and approval by Little Bit Pte Ltd.

For Licensing of a full Vault Management Software, as implemented by The Safe House SG Pte Ltd, which includes the Gregersen-Gono Crypto Implementation, please contact info@littlebit.sg

Special thanks for the creation of this standard also go to:

Dias Lonappan whose crypto wallet know-how was critical to development

The Safe House SG Pte Ltd staff for helping with the Standard Implementation

Silver Bullion Pte Ltd staff for supporting the standard in countless ways