Little Bit
by Silver Bullion

# Cryptocurrency 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 system 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 on the market. We replace digital storage with encrypted physical storage utilizing insurance coverage and existing high-security vaulting facility processes to store private 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 two-factor authentication systems typically used in the industry.

Version 20180921 updates the standard to use RSA-4096 encryption for the recovery cards, adds secret sharing of the recovery card decryption key and allows for multiple customer authorized representatives to be required during a withdrawal process.

The Gregersen-Gono Standard is implemented by Daenerys & Co. Pte Ltd at The Safe House SG Pte Ltd. Further service details will be published at https://www.daenerys.co.

*Gregor Gregersen*
*21 September 2018*

# Contents

# 1. Cryptocurrency 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 anyone who knows the address, although the identity of the address owner is not recorded on the Bitcoin 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 a public blockchain to see transaction details and balances.

Two popular blockchain explorers are BlockCypher and Blockchain.com.

To use these tools, go to one of the abovementioned websites and enter a bitcoin address to view a complete history of transactions and balances for that address 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 to spend any bitcoins belonging to that address.[2]

Unlike physical assets, such as gold and silver, where the asset itself must be safeguarded, information, like private keys, must be safeguarded when using cryptocurrencies. 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(es). 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 private keys protected from everybody, including the customer, until the bitcoins are released.

## 1.4. Public Key

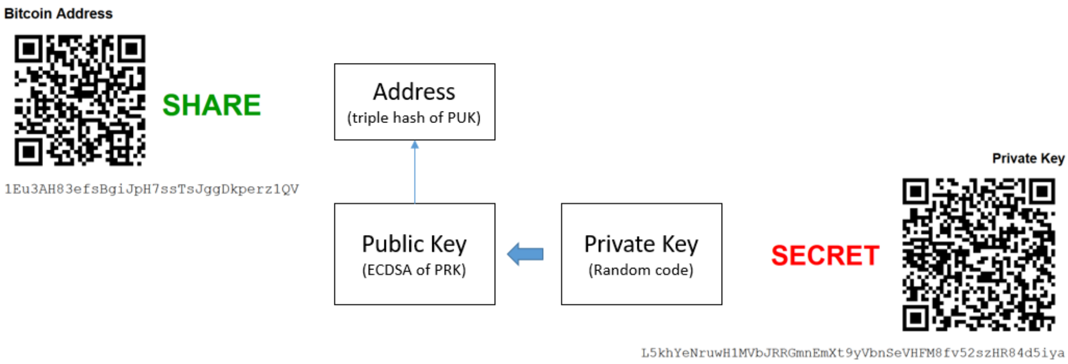
Each private key has a mathematically derived public key. The public key has a number of technical functions and, although typically hidden by wallet applications, the public key is required for advanced bitcoin features such as:

- Generating additional addresses linked to a single private key
- Generating multi-signatory addresses which require multiple private keys to authorize a transfer of 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 mathematically 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. Conversely, it is 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 private keys, public keys and addresses are typically read via QR codes which can be easily scanned by smartphones or other devices.*

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

Take note that the vast majority of bitcoin users – via online wallets or exchanges – do not have access to their private keys. This makes them fully dependent on the proper functionality, security and backup procedures of online wallets or exchanges, as well as the integrity of the wallet designers to effectively manage private keys. From a counterparty risk perspective, if you do not have control of the private key, you are essential a creditor of the private key holder.[3]

"Counterparties" in this context are middlemen between bitcoin owners and their on-chain bitcoin balances.

## 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. This means that private keys, public keys and addresses can be created on computers that are offline and not connected to the Internet. Offline key generation works because it is practically impossible that two properly generated private keys will be the same.

Offline generation is a great security advantage as fully offline computers are very difficult to be compromised by external third parties (hackers). Furthermore, the private key is required until funds need to be transferred.[4]

## 1.7. Transaction Irreversibility and Private Key Loss

Once a bitcoin transaction is made, it is not possible to reverse it as no entity is allowed to alter signed transactions on the blockchain. Furthermore, if a private key is lost it is not possible to recover it from the blockchain. Any bitcoins connected to a lost private key will be lost. Loss of bitcoins due to owners losing or forgetting their private keys has become quite common, hence the need for a reliable storage and 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 one.

Should an intruder obtain a private key, the intruder would be capable of stealing all bitcoins stored in the associated address(es) by transferring them to their own personal wallet address.

The sensitivity of private key storage is best illustrated by the Mt. Gox exchange heist. The cryptocurrency robbery 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 the exchange's own bitcoins over a period of two years.

---

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

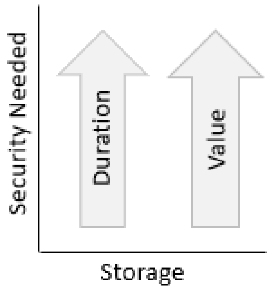
[4] *Bitcoin Private Keys: Everything You Need To Know,* Sudhir Khatwani https://coinsutra.com/bitcoin-private-key/

The exchange filed for bankruptcy resulting in its customers losing bitcoins with a combined value of approximately $450 million USD at the time. The stolen bitcoins appreciated in value and would have been worth $6.2 billion USD as of September 2018.

Today, computer viruses, trojans and other hacking tools are specifically written to seek and capture private keys. 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 due to the fact that the current balance of any given bitcoin address is public information.




This paper aims to provide a blueprint for the safest practical 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 bitcoin code, is resistant from cyberattacks. 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. These are characterized as storage risks.

This paper focuses on storage risks and how to secure 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 applies to other cryptocurrencies as well. This standard can therefore be easily adapted to support any cryptocurrency or digital asset that is secured via private keys.

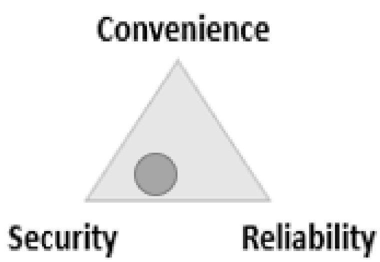
## 2.2. Storage Systems: Balancing Convenience, Reliability and Security

Storage systems face contrasting requirements and therefore require a design compromise between the following desirable features:

**Convenience:** the ease of use and set up time for the user, and any costs involved.

**Reliability:** the system's likelihood to continue operating and redundancies to ensure private keys are not lost.

**Security:** the protection against hacking and counterparty risks and threats.




It is possible to design systems that excel in only two out of these three area. **Our storage standard favors security and reliability over convenience.**

For example:

- **Convenient and Reliable:** An online wallet is convenient and, depending on design, a reliable system as well. However, the convenience precludes high security features.

- **Secure and Reliable:** A printed private key generated from an offline computer using a random key with enough entropy (true randomness). When kept safely hidden can be considered secure, as there is little to no hacking or counterparty risk. Storage could also be made reasonably reliable depending on the storage medium and implemented redundancies. However, this "do-it-yourself" method is not convenient for most people and requires considerable technical skill as well as discipline.

- **Convenient and Secure:** Scratchcards concealing private keys with a certain amount of pre-deposited bitcoins are readily available for sale online and in brick-and-mortar locations. If the printing was done securely, and there was no copy or backup (online or otherwise) then this storage method could be considered both secure and convenient. However, the absence of backups and the possibility of physical loss or degradation of the media makes prepaid bitcoin cards unreliable over time.

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

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

- **Offline Cold Storage:** Can be thought of as savings accounts as they hold potentially large bitcoin balances for long periods of time. Their design focus is concentrated upon reliability and security at the expense of convenience. "Cold storage" is a somewhat generic term where security depends fully on the details of the specific implementation. Without process transparency and implementation certainty, "cold storage" is essentially a meaningless term.

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

> **GREGERSEN-GONO PHYSICAL STORAGE:** DESIGNED TO PROVIDE THE HIGHEST SECURITY LEVEL, TRANSPARENCY AND PROCESS IMPLEMENTATION CERTAINTY.

"Process implementation certainty" means that the procedures 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 further described in Section 3.4. "Crypto Deposit Order (Private Key Generation)", and in other sections of this paper.

Properly implemented, the Gregersen-Gono Standard virtually eliminates the risk of hacking and physical theft while minimizing counterparty risk. The Standard supports optionally offering additional independent safeguards, such as liability protection backed by the vault's insurance policy and the use of multi-signatory addresses.

## 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 specifies four key risk groups that can be defended against.

### 2.3.1. Mishandling Risk

Users can store their own private keys without the need for third-party storage systems, but will thus be responsible for their own security and reliably. The possibility of end-users mishandling their private keys is discussed in this section.

Due to the vulnerability and value of a private key, storing a private key in a notepad (.txt) file on a personal computer or sending it via e-mail is extremely risky. It takes discipline and technical expertise to keep a private key safe from Trojan horse viruses and other hacking attacks.

On the other hand, the loss of a private key would mean that the bitcoins in the corresponding address(es) would be permanently lost. Hence, considerable discipline is needed to reliably and safely store private keys.

This is why there is a need for third-party storage systems, as these specialized systems can apply rigor and resources that individuals may not be able to access.

### 2.3.2. Counterparty Risk (Middleman Risk)

A large number of bitcoin private keys for example are stored in software programs commonly known as wallets. While some wallets, such as the "Bitcoin Core Wallet", store the private keys locally on the user's hard drive, there are also web wallets, online wallets and cryptocurrency exchange wallets where the private keys are stored and controlled by a service provider.

Since knowledge of private keys equals possession of bitcoins, using an online service essentially makes the service provider the owner of the bitcoins while the user who owns the bitcoins actually becomes just a creditor to the service provider.

**Using online services, or any other system that controls the private key, means that you are now trusting another party, and no longer enjoying the full benefits of bitcoin's trustless architecture.**[5]

There is nothing to stop a service provider from breaking their users' trust, utilizing the private keys under their control and stealing their creditors' bitcoins.

Furthermore, the service provider might be backing up keys to a third-party online cloud or other hosting service. Hence, the cloud provider represents counterparty risk to the service provider, which in turn is additional counterparty risk to you, as the cloud provider could potentially find a way to steal or lose the keys.

**Once you surrender your private key for storage to a third-party your counterparty risk is determined by all counterparties involved in processing or storing that private key.**

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

Counterparty risk can be split into:

- **Collusion**: Somebody within the counterparty company colludes with an outsider to steal private keys, making it look like a hacking incident.
- **Default**: The counterparty itself declares default, and returns only a small portion of the stored bitcoins (e.g. the Mt. Gox hacking case discussed in Section 1.8. "Private Keys are Perfect Hacking Targets").
- **Theft**: The counterparty, or some of the counterparty's employees, transfers bitcoins out of a wallet, washes the bitcoins using a process called "tumbling" or "mixing", and disappears.
- **Incompetence**: When private keys are lost without the possibility of recovery.

### 2.3.3. Hacking Risk

Stealing private keys from the owner or from a counterparty is a big problem. Mt. Gox 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 private 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 gain access to private keys.

Hacking can be classified according to the following:

- **Exploiting technical weaknesses:** Methods used to steal digitally-stored private keys and/or the decryption keys to access the data, such as open ports, uncomplicated passwords, unpatched operating systems, and bad encryption.
- **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 is usually contained in e-mail inboxes. Furthermore, e-mails are frequently used to reset login passwords or validate requests, often giving email intruders access to somebody's bitcoins by extension. A sophisticated attacker can also filter incoming emails and may be able to intercept two-factor authorization requests sent via SMS, as he may gain knowledge of the associated phone number from the user's e-mail.
- **Impersonating the counterparty:** Should an attacker succeed in hacking the website of the counterparty, they might be able to change the bank account or address where funds are to be transmitted. In this case, a customer would unknowingly send funds to the attacker instead of the intended counterparty.
- **Intercepting communications:** Also called a man-in-the-middle attack (MITM), if an attacker can intercept and change the address to which bitcoins are to be

transferred due to an insecure transmission medium, this would be an easy manner to steal bitcoins.

### 2.3.4. Private Key Loss Risk

Should a private key be lost, it will no longer be possible to access the bitcoins stored it the associated address(es). 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 a counterparty.

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

Here are reliability issues to consider:

- **Online storage:** Depending on the provider, online storage can be a sufficient 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 risks.

- **Physical loss of the storage medium:** USB thumb drives, paper printouts, laptops and other hardware devices can be lost, misplaced, damaged or subject to malfunction and failure. To increase reliability, USB cold wallets might have an online backup function or mnemonic phrases in case of loss. However, online backups create counterparty and hacking risks while mnemonic phrases have the same “if you see it you can steal it” security risk as paper wallets.

- **Physical degradation of the storage medium:** All forms of digital media have a risk of data loss over time, especially if exposed to magnetic fields or other sub-optimal storage conditions. The chance of data loss 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. Heat, humidity and other environmental factors can cause paper to degrade more quickly than usual.

[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 encryption protects the cards from physical theft or copying. These cards are then stored in sealed safe deposit boxes, providing security and reliability for long term storage of sizable amounts of bitcoin.

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

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 at DHL and Apple.

## 3.2. Definitions and Description of Terms

**Address:** Mathematically derived from the public key and is required to be able to send bitcoins. It can be thought of as the equivalent of a bank account number.

**Authorization List:** The document listing the authorized representatives for a given customer. This document is provided by the customer.

**Authorization Mandate:** A document specifying customer-specific rules and requirements for the release of cryptocurrencies and/or private keys. This document might specify, for example, that X of Y authorized representatives are required to approve a cryptocurrency release over a certain value. The Authorization Mandate can also specify standing order details, such as a request to transfer a fixed amount of cryptocurrency to a predetermined fixed address on a regular basis. Changes to the Authorization Mandate will require a written request from the customer.

**Authorized Representative:** A person who is authorized to initiate and approve transactions on behalf of the customer. Authorized representatives are selected by and can be removed by the hirer.

**Blue System:** Is a high security local area network comprised of a server and terminals that provide the Vault Management System. The Blue System controls all processes, split into tickets divided among Functional Groups, within the vault. For security purposes the Blue System is an offline system, meaning that it is physically disconnected from the public internet as well as other outside networks. Communication between Blue and Red System occurs via manual data entry, QR codes or scanning of printed documents.

**Broadcaster**[7]**:** A tablet that runs custom software for the secured broadcast of crypto transactions during a crypto withdrawal or the secured release of private keys (see Section 3.5.3. "Withdrawal Release Ticket – Full Withdrawal" for more information).

**Crypto Address Confirmation Document:** The document is sent to the customer when a new crypto storage address is created. It contains the address for depositing bitcoins for secure storage and the public key for advanced functions such as the creation of multi-signature addresses.

**Crypto Private Key Release Document:** This document is generated and sent as part of the full withdrawal process. The document contains the private key in plaintext, is password protected and only the customer will know the password having specified it in Step II of the withdrawal process. This document will not be sent if the customer requests a partial withdrawal.

**Crypto Release Room:** A room optimized for teleconferencing with CCTV coverage and a Blue System Terminal where Minibox and Multibox seals are cut, and bitcoins and/or private keys are released to customers remotely.

**Crypto Withdrawal Confirmation Document:** The document is sent after a full withdrawal of bitcoins to formalize the closing of the crypto storage service for the address in question.

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

**Customer Encrypted Private Key Card**: A credit card-sized laser etched polycarbonate card with a customer's private key and an associated deposit address laser etched upon the card. Customer Encrypted Private Key Cards allow for reliable long-term non-digital storage.

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

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

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

[7] The Broadcaster was previously referred to as a "Decryptor" in an earlier version of this document and is the only part of the system that can access external networks. Since decryption of the private key actually takes place on the Verifier device, the name was changed to "Broadcaster" to more accurately describe the device's function of announcing a transaction.

- **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.

- **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 as well as precious metals testing, cryptocurrency key generation and safe deposit box retrieval.

**Hirer:** Person(s) authorized to enter into an agreement and change the authorized representatives on the Authorization List. For natural persons the hirer is the customer. For companies or trusts the hirers are board appointed staff members or trusted individuals that have been nominated via board resolution or according to trust bylaws.

**Minibox:** A small, numbered safe deposit box specifically designed to store encrypted private key cards. Miniboxes are sealable using a one-time seal ensuring box integrity.

**Multibox:** A numbered box specifically designed to store multiple encrypted private key cards. Miniboxes are designed to fit within Class II safety deposit boxes which are in turn sealable with one-time seals ensuring box integrity.

**Multi-signature Address:** A special kind of address that is created from multiple public keys and allows for multiple private keys to be needed to release coins (see Section 3.6.12. "Multi-signature Addresses" for more information).

**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.

**Order**: 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.

**Pre-approved Withdrawal Address:** An optional address provided by the customer upon account opening, which can be updated via teleconference verification, to expedite the sending of funds to a customer.

**Private Key:** The randomly generated number that allows the signing of transactions for a given cryptocurrency address. The private key is the security equivalent of a bank account, password and security token device combined into one. Anyone with access to the private key can transfer any bitcoins in the corresponding address(es) at any time.

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

**Recovery Encrypted Private Key Card**: Another credit card-sized laser etched polycarbonate card with the same private key as the customer card, but encrypted using a different algorithm, designed to be decrypted only in case of loss or damage to the customer card.

**Recovery Storage**: Is an armored cabinet where recovery encrypted cards are inserted into a one-way slit. The cabinet is stored within a secure strong room at an off-site location, and can only be accessed in exceptional circumstances if recovery is required. The existence of a recovery card is important for reliability purposes and poses minimal security impact as none of the personnel at the vault possess the recovery key needed for recovery card decryption.

**Red System:** A lower security local area network, with a server and terminals that are connected to outside networks and the internet. Vault staff utilizes the Red network to communicate with customers.

**Ticket:** 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.

**Transactee:** A person 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). The transactee can also be an employee of the customer or the customer himself.

**Verifier:** A tablet that runs custom software to verify that cards have been etched correctly, perform recovery operations and allow for offline transaction signing during the withdrawal process.

## 3.3. Ensuring Processes' Certainty

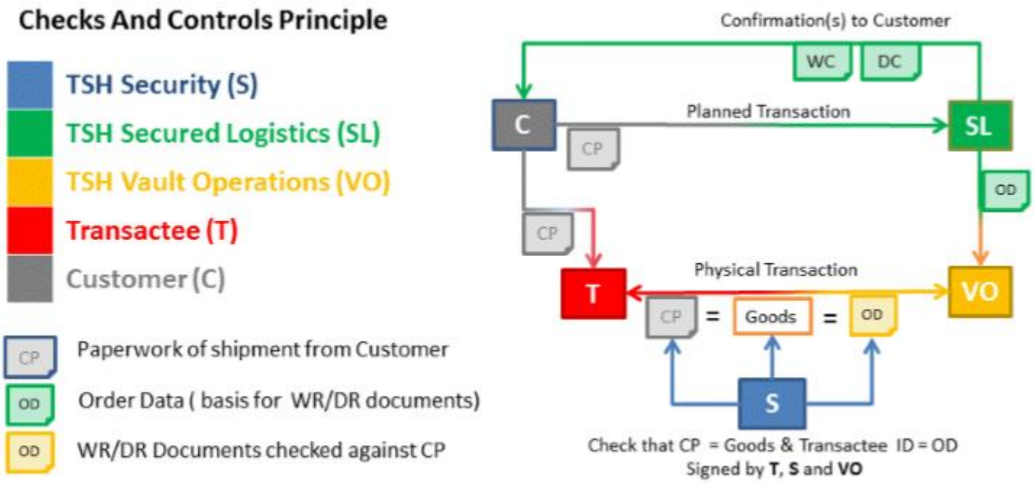
The processes described in this document ensure that each functional group is being checked by one or two other functional groups during order executions. This is achieved by splitting orders into smaller processes that are referred to as tickets and assigning ticket execution to separate functional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

By managing the work of the functional groups via tickets and requiring functional group sign-off, the Vault Management System ensures processes are always followed, as the required paperwork and/or release codes cannot be generated without following the prescribed processes. In this paper the primary crypto orders and their constituent tickets are detailed.

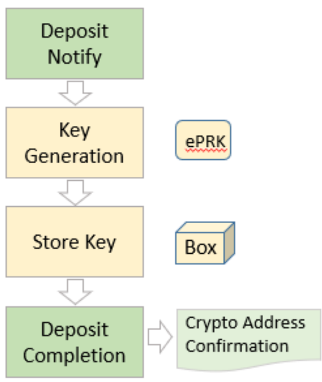
For Crypto Storage, the transactee and customer are typically the same entity as no logistics transport is needed for crypto storage. The division of roles still holds true however, as Secure Logistics is the one interacting with the customer (planning transaction) while Vault Operations handles the 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 Deposit Notify 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 ETH)
- Optional liability protection

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 private key card for laser etching
- Backup Recovery Encrypted 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 Section 3.6.1. "Private Key Entropy" for more information). The private key is then immediately encrypted using two encryption algorithms (AES-256 for the customer card and RSA-4096 for the recovery card) and the plaintext private key is flushed from memory. For transparency purposes the code handling the key generation, encryption and flushing will be open sourced and published on GitHub once the service is officially launched.

The public key and the address are then stored permanently in the Blue System in order to generate the Crypto Address Confirmation Document, while the encrypted customer and recovery private keys are etched using a laser onto their respective polycarbonate cards and are then flushed, as are the laser etcher records (see Section 3.4. "Crypto Deposit Order (Private Key Generation)").

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 the Verifier device, 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 is applied.

The Minibox is intended for long term physical storage and will not be removed until a Withdrawal Request is received and verified. 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 Store Key Ticket also physically sign the Crypto Deposit Confirmation which will be later scanned and mailed to the customer.

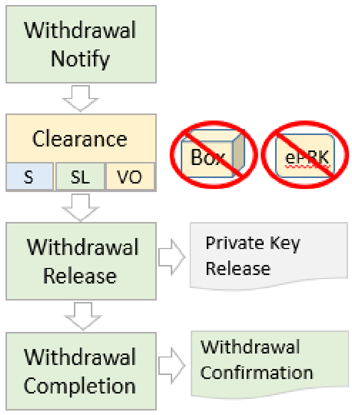
### 3.4.4. Deposit Completion Ticket

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 of this ticket is to ensure 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 the customer may then transfer bitcoins to the address(es) associated with their Crypto Storage Account.

## 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, the 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:

- **Security Withdraw Clearance Ticket** for security, specifying the release date/time and customer ID to verify.
- **Vault Operator Withdraw Clearance Ticket** for Vault Operations specifying the date/time for release, box ID and Seal ID.
- **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 and time, a video call with the customer is established originating from the crypto release room if the customer or their representative is not present in person.

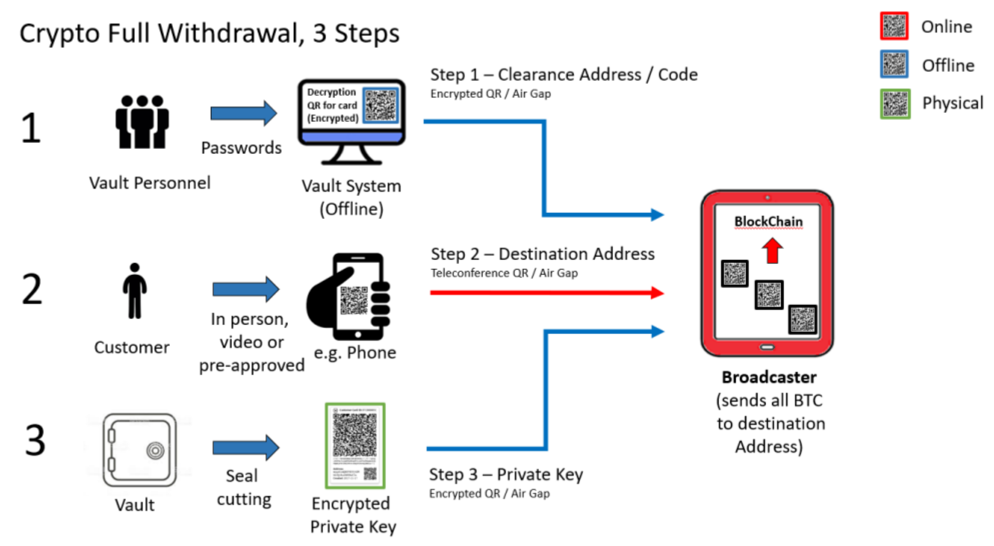
In the crypto release room, Security, Vault Operations and Secure Logistics representatives will be present as per release rules. Vault Operations delivers the sealed Minibox as identified by the Box and Seal ID. Secure Logistics will provide the unsigned Crypto Withdrawal Confirmation Document for the pending release.

The customer is then contacted via a video call and their identity is verified by the functional groups as per the verification process. Once verified, each functional 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 secure 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 three 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, is itself encrypted with AES-256 to prevent alteration, and is generated after customer identification is confirmed by three vault personnel, each of whom vouch for correct identification of the customer by confirming their passwords in the Blue System. This code contains the card specific decryption key as well as the outstanding fees and a time window for the decryption to be completed within.

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

This process ensures that the Broadcaster 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 has a card-specific decryption key (which only works for the specific card to be released) provided by the clearance QR code but does not have the encrypted private key nor a destination address where released bitcoins are to be sent.

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 and Release of Funds*

At this step, the Broadcaster has a release authorization and a destination address. Secure Logistics personnel will now confirm the crypto amount to be sent minus eventual outstanding fees and the destination address’s last five characters with the 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 where 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 code as was done with the "release to" address due to the continued security sensitivity of the private key. Therefore, the Broadcaster will generate a password protected file which can be accessed only with the Private Key Release Document password that only the customer has. The document is then transmitted to the customer via secured communication.

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

#### 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 generate new addresses and new encrypted private key cards every time a small withdrawal is needed.
- **Usability**: Most customers prefer to have a fixed address that they can deposit and withdraw from rather than keeping track of newly generated addresses for each transaction. 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 permanent addresses minimizes this risk.

Unlike a full withdrawal, the Customer Encrypted Private Key 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).

To accomplish this, a partial withdrawal involves the use of the Broadcaster that generates and later broadcasts the transaction onto the blockchain and an offline Verifier device that signs the 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 – As in the case of 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
- Crypto Type: The cryptocurrency involved, such as bitcoin or ether
- Transaction Type: The sort of transaction, such as partial withdrawal
- Valid Until: A date and time field that defines a transaction expiry. This prevents the potential unauthorized re-use of a 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 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 the 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 of which is retrieved online:

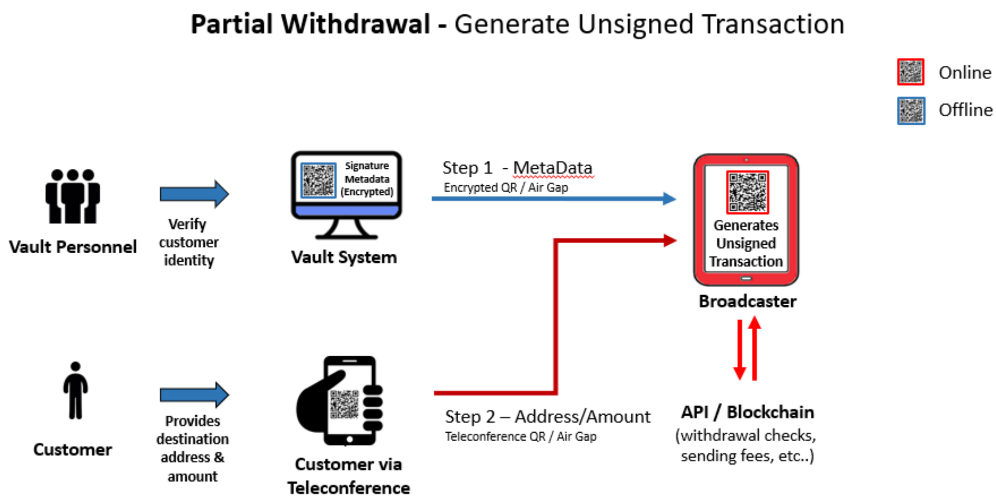
- Crypto balance, type and valuation in USD or SGD
- Crypto balance locked as collateral for P2P loans

- Unpaid storage fees
- Card ID
- Customer Details

The vault personnel will then request 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 withdrawal 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 the cryptocurrency used, add the appropriate transaction fee to ensure timely delivery.

The Broadcaster 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 displayed on the Broadcaster screen.




### *3.5.4.2. Sign and Broadcast Transaction*

The unsigned transaction will be signed as follows:

Step 1 – Vault personnel use the offline Verifier device to scan the encrypted unsigned transaction QR code from the Broadcast device which initiates the signing process.

Step 2 – Vault personnel scan 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 scan the Customer Encrypted Private Key Card to decrypt the private key which is needed to sign the transaction.

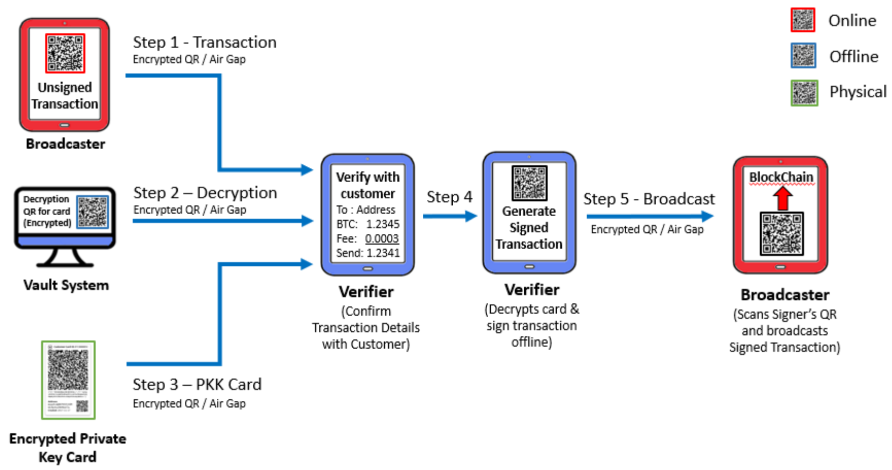
Once the card is successfully scanned, the Verifier will provide a transaction summary. Note that using the wrong private key card causes the decryption process to fail. In case of a video conference the vault personnel will use this summary to reconfirm with the customer:

- The destination address
- The 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 code from the Verifier. Once scanned, the Broadcaster will broadcast the transaction to 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 the 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 effectively impossible to reproduce. A good random private key is almost mathematically impossible to reproduce and therefore very safe from external attackers trying to guess a private key.

We utilize the crypto library RNGCryptoServiceProvider in an offline setting, which meets FIPS 140-2 certification of the Security Requirements for Cryptographic Modules, to ensure high entropy keys are generated. After encryption and etching, we erase the private keys from memory. This process is open source and will be available on GitHub 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, immediate key encryption and subsequent deletion of the private keys, it is practically impossible for an attacker to obtain access to these private keys remotely.

### 3.6.3. Customer Encrypted Key Card

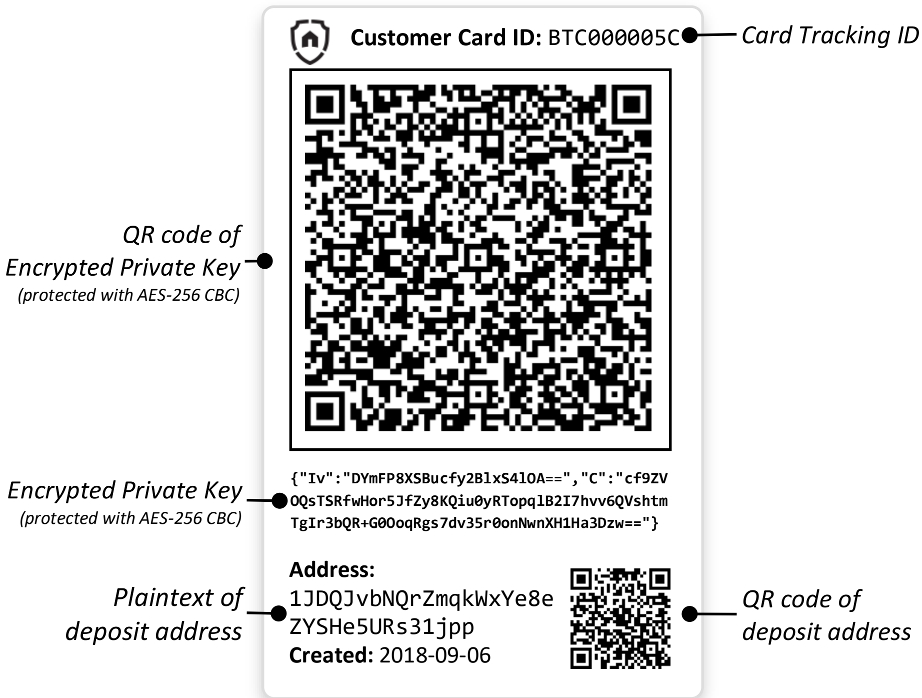
For security reasons, private keys are not stored digitally in any format. Instead, an ultraviolet laser is used to irreversibly etch the customer's encrypted private key onto a highly durable polycarbonate card. The encrypted private key (PKR) is written in alphanumerical format as well as a QR code for easy scanning.

The customer private key is encrypted at the top section of the card using AES-256 in cipher block chaining mode, or CBC, 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 card itself is useless without the database encryption key which is retrieved only upon following the Crypto Withdrawal procedure previously detailed in this whitepaper.

The encryption ensures internal security and makes the theft of the card itself useless, as only the Verifier tablet can decrypt it. Stealing a Verifier tablet plus a customer card will also serve no purpose as the decryption key for a given card is provided by 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. The card also includes the date of etching and an internal card tracking code.

This card will then be physically slotted into a Minibox or Multibox 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 Multibox for long-term storage. The box is then sealed with a one-way numbered seal which provides proof of box integrity.

The Minibox or Multibox 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*

*Sealed boxes are then stored within a class II vault*

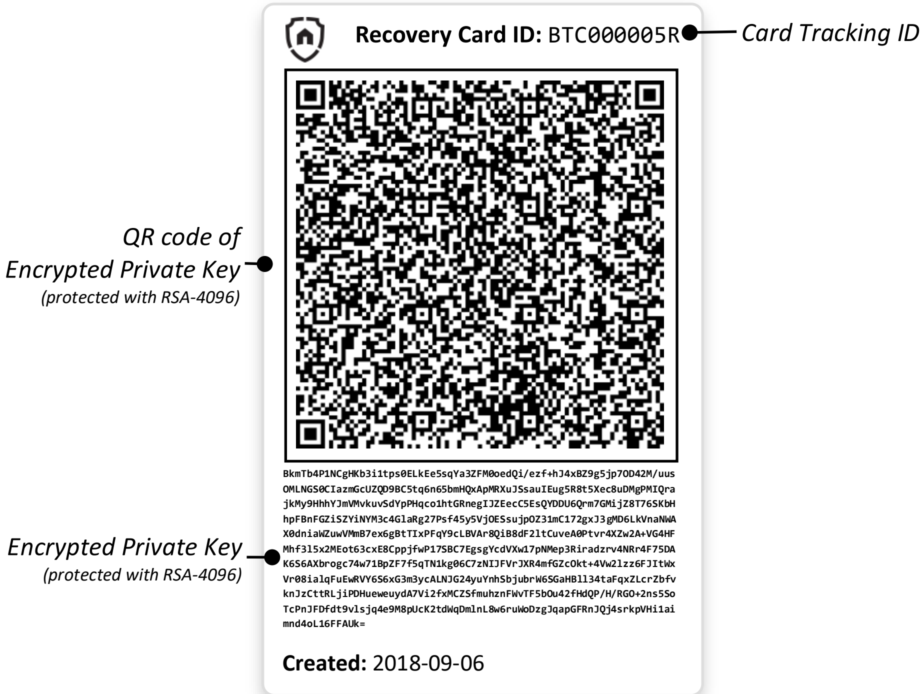
### 3.6.5. Recovery Encrypted Key Card

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

REPKCs utilize a different encryption process (RSA-4096) thereby generating a different encrypted alphanumerical string and QR code. Asymmetric encryption means that data can be encrypted using a public key and does not require access to a private key during encryption. This is important as, for security and reliability purposes, the recovery key is not stored within the storage facility, therefore REPKCs cannot be decrypted at the storage facility.

This encryption procedure means that neither a potential thief nor vault personnel can decrypt a REPKC. Instead, a specialized recovery process would be initiated in the very unlikely event of the loss of the CEPKC (see Section 3.6.6. “Recovery Process” for more information).

For reliability purposes, REPKCs are securely stored offsite in an armored “recovery box” custom built with a slit that allows the one-way insertion of the REPKCs. The REPKC has a similar layout and functionality as the CEPKC 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 (REPKC) are stored in our strong room in the headquarters of the contracted Singapore auxiliary police force (Certis Cisco) where our primary office is located about three kilometers from the vault. Off-site storage of the REPKCs increases reliability in case of fire or other potential disasters at the vault location.

Recovery cards are stored inside an armoured cabinet with a one-way slot where recovery cards are inserted for long term storage. This is akin to check deposit boxes used by banks. The cabinet is locked and sealed via numbered imprint, and kept 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 RSA-4096 Encrypted Recovery Card(s) to be recovered
- The Recovery Decryption Clearance Cards
- The Verifier Device

**Recovery Card Retrieval:** During a recovery, the armoured cabinet is opened by at least two vault operators and one director. The relevant REPKC would be retrieved based on its card ID or address. The cabinet would then be re-sealed with a new numbered seal.

**Recovery Decryption Key Retrieval:** The RSA-4096 private key required to decrypt the REPKCs is itself encrypted with an AES-256 private key which is sharded onto five separate cards using Shamir's Secret Sharing algorithm. Any three of the five cards are required to decrypt the recovery key. Recovery key shards are stored in safety deposit boxes and safes.

A Verifier device is required for the recovery process. Should no Verifier be available, a new Verifier can be configured by Little Bit.

Once all items are retrieved, the Verifier tablet scans 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 Verifier and/or Broadcaster 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 (CEPKC) and lists the public key and associated address that have been generated.

The document also lists the safe deposit box number where the CEPKC is secured. This document is verified by three individuals and requires at least one from both the Secure

Logistics group and the Vault Operations group. This document will be scanned, uploaded to 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.

### 3.6.8. Crypto Withdrawal Confirmation Document

This document is generated and printed by the Blue System upon creation of Withdraw Notify Ticket, is signed during release clearance and later scanned and sent to the customer as part of the Withdraw Closure Ticket by the Secure Logistics group.

The document confirms the numbered seal that was broken, account closure and withdrawal of the private key. The document contains three signatures, one from each functional group.

### 3.6.9. Communication Options:

High Security Authentication Options for Crypto Withdrawal

- Encrypted Video Call with verification (see Section 3.6.10. “Customer Video Verification” for more information)
- Customer appears in person

Secured transmission for Address Confirmation and 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
- Encrypted Messenger Apps

### 3.6.10. Customer Video Verification

When a video call with the customer is established, the customer is identified visually by comparing their 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 verifications can be requested during the video call to further ascertain the customer's identity:

- Request customer or authorized representative(s) to present their passport or ID document
- Call the customer on the phone number on record while during the video call
- Send a verification code via SMS to the phone number on record
- Any additional procedures specified in the customer's Authorization Mandate

### 3.6.11. Clearance Group Representatives

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

- For cryptocurrency withdrawal and private key release
    - 1 x Secure Logistics + 1 x Vault Ops + 1 x Security, or
    - 1 x Secure Logistics + 2 x Vault Ops
- For a recovery decryption
    - 1 x Secure Logistics + 2 x Vault Ops

### 3.6.12. Multi-signature Addresses

Multi-signature addresses are addresses which require X of 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.

For example, a customer could use the public key (sent via the Crypto Address Confirmation Document) along with his own private key(s) to create a multi-signature address(es). For example:

A 2/2 address would increase security against unauthorized withdrawals as neither the private key stored in the vault nor the customer's private key would be sufficient to release bitcoins. The downside is that reliability suffers, as a loss of either private key would result in the bitcoins becoming permanently inaccessible.

A 2/3 address could make sense if two separate customers want to maintain what would effectively be a joint account using the using the vault to store a backup.

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 utilizing this powerful capability.**

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

# 4. Threat Scenarios

## 4.1. DIY Mishandling

By outsourcing the private key storage, customers need not concern themselves with securing their own private keys.

## 4.2. Counterparty Risk

Defined as the risk that something goes wrong within the vaulting storage provider, counterparty risks include collusion, default, theft, and incompetence.

### 4.2.1. Collusion

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

Collusion is nearly impossible when the Gregersen-Gono Standard is fully implemented because all private keys are encrypted and plaintext private keys are never accessible by vault personnel. The encrypted private key card is useless without a Verifier device. The Verifier 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 the Vault Management System requires passwords from Security, Vault Operations and Secure Logistics personnel.

Note that the customer can elect to use multi-signature addresses to further increase protection against any form of unauthorized withdrawal (see Section 3.6.12. "Multi-signature Addresses" for more information).

### 4.2.2. Default

Default or bankruptcy involves a counterparty declaring insolvency and refusing to return the cryptocurrency assets stored on behalf of customers. (Recall the Mt. Gox case referenced earlier).

Under the Gregersen-Gono Standard, the vault operator simply acts as an agent to store private keys for customers; cryptocurrencies 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 or silver holdings would be released.

### 4.2.3. Theft

The counterparty, or a portion of its staff, transfers out, washes the bitcoins (a process called "tumbling" or "mixing") 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 members, including security (auxiliary police), to act in unison without detection by other staff.

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

Vault staff are subject to stringent security procedures, are long term residents of Singapore or Singaporean citizens, many of whom are also shareholders in the vaulting company, and are extremely unlikely to collude.

Note that that customers can elect to use multi-signature addresses to further increase protection against any form of unauthorized withdrawal (see Section 3.6.12. "Multi-signature Addresses" for more information).

### 4.2.4. Incompetence

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 and balances 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 are addressed:

- **Laser etching error causing non-readable keys**. This is addressed by:
    - A card verification procedure occurs immediately after etching to ensure the card has been written properly.
    - 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 is only valid for the specific card in question. If the scanned card is the incorrect card the decryption process will fail.
- **Loss or 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 cryptocurrency best practices. For transparency purposes the code for key processes will be open source.
- **Release to the wrong customer.** This is addressed by:
  - The six-eye withdrawal principle (at least three individuals) and the video call requirement makes it very unlikely that a release to the incorrect customer would occur.
- **Typos and other input errors.** This is addressed by:
  - The Gregersen-Gono Standard eliminates or automates most critical user input that might contain typos. The sensitive withdrawal process for example consists only of QR code scans and all documents are confirmed by multiple functional groups as well as by the customer. The only text input is the amount to be withdrawn in case of partial withdrawals.
  - The vault operating system is designed to eliminate errors by requiring multiple functional groups to confirm each other's input.

## 4.3. Hacking

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

Physical crypto storage is essentially immune to traditional hacking attempts because the private keys are not stored in digital format. The only use of computers 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 then destroyed. The key is never written onto permanent storage. The opportunity for attack is virtually nonexistent (see Section 3.6.12. "Private Key Security" for more information).
- **Physical Etched Key Verification.** This occurs on an offline Verifier device which verifies that the encrypted text is readable on the laser etched polycarbonate card. No sensitive data is stored on the Verifier.
- **Private Key Release.** This occurs during the video call with the customer upon positive identification. The private key will only be read and decrypted from

the physical card at the last moment upon transmission of the transaction and will then be immediately erased from memory. 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.

This system ensures highly effective and reliable protection against all known technical exploits. Physical storage is virtually hack-proof.

### 4.3.2. Impersonating the Customer

In practice, customer impersonation might be the greatest security threat to the cryptocurrency storage industry. An attacker gains access to a customer's smartphone, for example. This would typically allow the attacker to gain control over the customer's e-mail and phone number which in turn bypass most online security.

In such a scenario, most common two-factor authentication implementations 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 via a video call or physical presence.

The identification is based on a six-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 two-factor authentication of his phone live over the video connection.

The video call 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 operating hours, reducing convenience.

### 4.3.3. Impersonating the Counterparty

The Safe House (TSH) vault has a minimal online presence, storing sensitive data offline on its Blue System. The primary concern is that of a third party attempting to impersonate TSH staff by sending a forged e-mail or 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 deposit addresses controlled by the attacker. The attacker would also need to intercept any communications from TSH to the customer. At the least, this would require that the attacker already had full control over the customer's e-mail account(s).

The best defense against such attacks is for the customer to reconfirm the deposit address with TSH.

#### 4.3.4. Intercepting Communications

To avoid a man-in-the-middle attack (MITM), The Safe House encrypts or password protects sensitive information.

## 4.4. Private Key Loss Risk

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

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

In the case of The Safe House, the encrypted private keys are stored within Miniboxes or Multiboxes. These boxes are in turn 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 (30 cm). The Class II vault is located within a much larger Class I vault located in Singapore secured by a Singapore auxiliary police force.

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

#### 4.4.2. Degradation of the storage medium

Physical storage implies long-term storage of cryptocurrency, requiring a storage medium that can reliably store a private key for many decades without degradation regardless of conditions. Loss of the private key would be disastrous for cryptocurrency storage.

Digital storage such as hard disks and flash drives, for example, are sensitive to magnets and could even be wiped clear by strong solar flares. These types of storage media, along with tapes, CDs and DVDs also degrade over time and have an unacceptable risk of data loss when storage for periods greater than 5 years is required.

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

The Gregersen-Gono Standard utilizes an ultraviolet laser to etch encrypted private keys with precision onto polycarbonate cards. The encrypted key is written twice, once in alphanumeric format and once as a QR Code to provide both redundancy and easy scanning.

The UV laser physically changes the physical properties of the polycarbonate in an extremely precise manner and does not use ink which could decay or smear. The polycarbonate material is a durable plastic (also used in the manufacturing of bulletproof panels) which is further protected in the Miniboxes or Multiboxes within the vault, giving it an expected lifespan of centuries.

# 5. Conclusion & Notes

As of September 21st 2018, the standard is nearly implemented. 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.daenerys.co/cryptocurrency-storage and Daenerys Pte Ltd will soon be the first company to offer this service to customers.

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 solution 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 blockchain know-how was critical to development

Brian Hankey whose contribution in the final release version was invaluable

The Safe House SG Pte Ltd staff for assisting in the development of this standard

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

# 6. Legal



For **commercial use** of the Gregersen-Gono Standard, please contact Little Bit Pte Ltd:

- Gregor Gregersen: gregor@littlebit.sg
- Clint Gono: clint@littlebit.sg