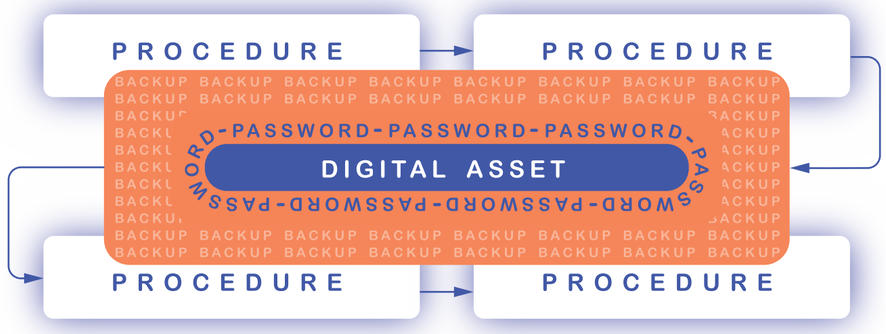


BOOST SECURITY

The more valuable the information, the higher the security level required to protect it, and the higher the cost of that protection. In consequence, any intrusion will necessitate a higher energy / asset expenditure to force access. Therefore, the questions to answer first should be:

What is the value of my information?
What level of security does the Capsule provide?
Can I improve it by additional means if necessary?

Think through the entire process of sensitive private information access. The security of any solution depends heavily on the particular implementation. The Capsule was designed to store information for backup cases; however, it is a universal tool and can be applied in various scenarios: recovery seed backup, password protection and storage, and other sensitive information storage/transfer.

How do you protect intangible assets?
Who is the keeper of my digital footprint?
Are my kids safe online?
How do I provide security for my children online?
I don't trust the centralized authorities or global companies so, how can I control what's mine?
How do I take care of my privacy in a digital world?
Can I protect my data from instances of violence?
What do my relatives need to know once I'm not around?
Is it for me? Do I even need to care about my online security?
Who can take care of me better than I can myself?
What will the damage be if my information ends up in the wrong hands?
How can I make my passwords truly safe?
What kind of digital assets can I protect?

THE MOTHER OF ALL BACKUPS

MY SECURITY AND ME

The more complex the digital environment I live in becomes, the more important it is to use a simple physical starting point that I can possess and, based on which, all of my digital wealth can be proven and accessed.

This is just a sample of some questions and thoughts one might have nowadays when thinking about digital wealth and virtual presence. Below you will see the hows and whys of storing private information with the Cryptosteel Capsule and achieving peace of mind.

ON OPERATIONAL SECURITY AND THE CRYPTOSTEEL CAPSULE

The Anatomy of the Cryptosteel Capsule

POOR PASSWORD CHOICES

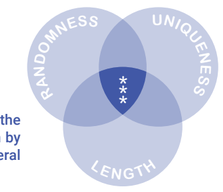
Think of your password as the magical phrase that opens the cave to all your treasures. Would you use something obvious like "open sesame" that anybody can guess? Or a long, unique phrase that's too complicated to remember so you write it down and store it somewhere close to the cave? Any security system is only as strong as its weakest part.

With a proper backup tool like the Capsule, there is no need for a trade-off between password strength and memorability.

Don't compromise on password or key length. To protect a highly valuable digital asset one needs a high-quality password (unique, long enough, and difficult to be guessed - random, using various strings like uppercase, lowercase, numbers, special characters), a safe tool to store it (Cryptosteel), and a secure procedure to handle it.

GOOD PASSWORD FEATURES

These are the requirements for creating a strong password:



UNIQUENESS
- Key/password should be used for one purpose only
- Should not be obvious or based on common words or sequences, a replacement scheme, or a single dictionary word

LENGTH
- The minimum length depends on the application of the key or password. Always follow the suggestions given by the provider of the related service or check general suggestions for the applied algorithm
- The longer the better

RANDOMNESS
- Use various types of characters (uppercase, lowercase, numbers and special characters) in a random combination
- If possible, use a password generator including a reliable source of entropy such as a true random number generator

BAD PRACTICES

- Identical passwords reused for different sites (like one PIN used for several credit cards).
- Easy to guess passwords (like Peter123 or P@ssw0rd).

GOOD PRACTICES

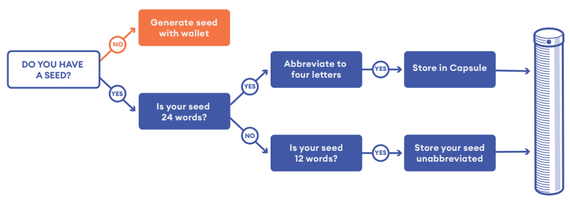
- We recommend using mnemonics (e.g. BIP39), which is the best method for human to computer interaction compared to handling raw binary or hexadecimal password representations.
- Don't share your password with anyone. Keep your secret offline. Don't take pictures of it, especially with your smartphone.
- A feature of the Capsule is that once your password is on the core, neither you nor anyone else can accidentally reveal it or take a picture of it.
With the Capsule, you are able to store 512-bit keys or even more complex codes. In combination with modern cryptographic algorithms, it provides you with state-of-the-art security for your digital assets.

MNEMONIC SEED FLOWCHART

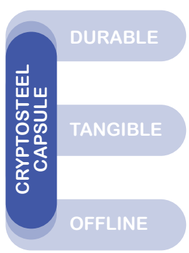
The private key to your cryptocurrency holdings stored in the BIP39 mnemonic seed format is the paramount access element and ultimate recovery tool. At the same time, misplacing access to this string of characters represents the single greatest vulnerability to your assets. To facilitate security procedures, we have boiled down the process to this simple flowchart so you can quickly identify your position on the timeline of securing assets.

Start at the beginning: Do you have a recovery seed phrase?
Step-by-step follow the instructions and proceed to secure and safe recovery backup access in a Cryptosteel Capsule for permanent storage.

Scan the QR code to download the flowchart for an easy BIP39 four-letter format adoption.



FEATURED ATTRIBUTES

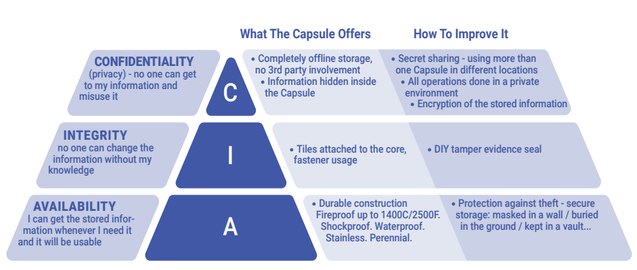


DURABLE [A] - the main purpose of the Capsule is to provide the **availability** of the stored information. No matter how long it has been stored, or what hostile conditions the tool has been kept in, the information will be available in the original form and able to be read.

TANGIBLE [I] - cannot be randomly changed, keeps the **integrity** of the form and format for a very long time, and there is more common knowledge of how to protect tangible items (e.g. gold, cash, etc.) in comparison to digital ones.

OFFLINE [C] - in order to achieve **confidentiality** of the stored information, at no moment should the full information be available in an uncontrolled environment (cloud storage, mobile app, etc.)

The Capsule fits perfectly within the AIC Triad, which is a template for information security strategy.



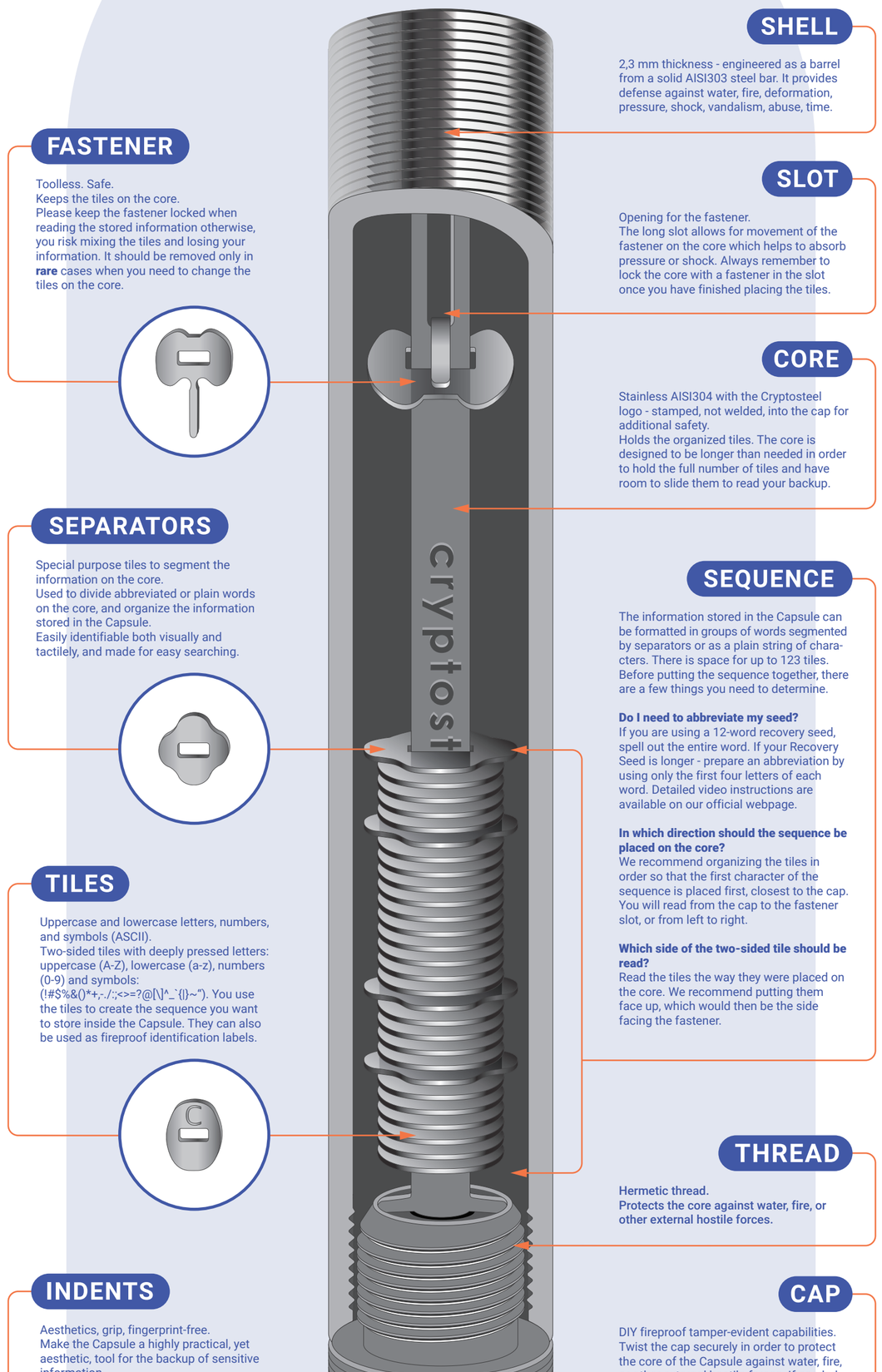
USE CASES

- Cold storage for hardware wallet recovery seed backup (BIP-39, if abbreviated - use only the first four letters of each word)
- Secret sharing (SLIP-39 Shamir backup in abbreviated form, use the first four letters of each word)
- Private keys for public-key algorithms for digital signature (ECDSA, base64 encoded)
- Secret keys for symmetric algorithms for encryption (AES, base64 encoded)
- Passphrase backup for password managers

FEATURED STANDARDS

- BIP-0039: Mnemonic code for generating deterministic keys
https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- SLIP-0039: Shamir's Secret-Sharing for Mnemonic Codes
https://github.com/satoshilabs/slips/blob/master/slip-0039.md
- BIP-0032: Hierarchical Deterministic Wallets
https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
- Base64 (RFC 3548, RFC 4648)
- NIST Special Publication 800-57: Recommendation for Key Management
http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
- FIPS PUB 186-4: Digital Signature Standard (DSS) http://dx.doi.org/10.6028/NIST.FIPS.186-4
- FIPS PUB 197: Advanced Encryption Standard (AES) https://doi.org/10.6028/NIST.FIPS.197

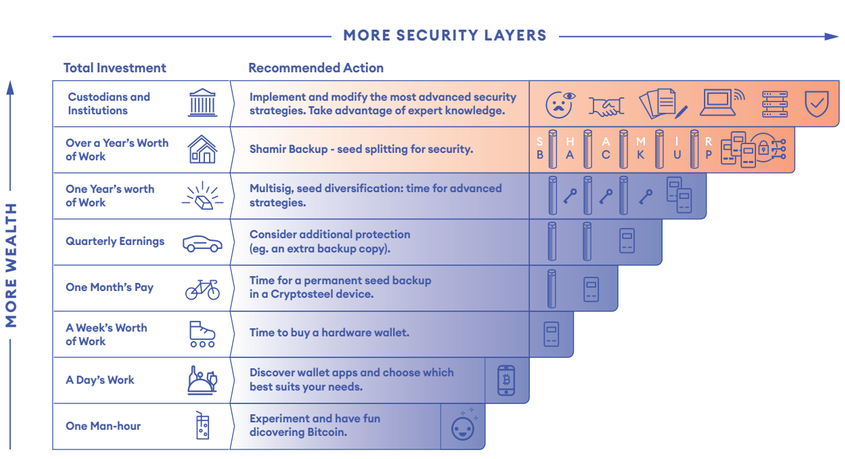
The Anatomy of the Cryptosteel Capsule



TIME FOR A HARDWARE

Adjust your security level to your investment. Take a moment to quantify your cryptocurrency holdings by applying a time-based variable, namely interpretation according to the ***time taken to generate value***.

The **graph below** shows what security measures are best paired with respect to your investment. Hence, following an initial one-hour asset value merits experimentation with free online solution, while, on the other end of the spectrum, is a robust, multilevel security system with multiple, permanent, offline Capsules ensuring that nothing could endanger the safety of your holdings.



CRYPTOSTEEL PRIVACY GUIDE

EXPLAINED BY WASABI

MY PRIVACY, BITCOIN AND ME
In the digital age, privacy is hard. Privacy is a choice about what information to share about yourself. As an open monetary network, all bitcoin transactions are publicly visible to all. Maintaining financial privacy on bitcoin can be hard, but you can protect it using the right wallet.

PRIVACY = SECURITY
You should generate your seed on a bitcoin wallet that does not leak personal information. A bitcoin wallet should be free and open source, with as many reviews from developers and users as possible. It should handle balance queries in a private way, without leaking your addresses and transaction history to third parties. Your wallet should also be integrated with an anonymity network such as Tor, which protects your IP address from being collected.

We recommend using Wasabi Wallet. It is compatible with most hardware devices and has a built-in coinjoin feature. A coinjoin is a collaborative bitcoin transaction to hide your transaction history from the public and reclaim your privacy on bitcoin.

HARDWARE WALLETS

EXPLAINED BY BITBOX

Bitcoin is electronic money, which means that it's necessary to use an electronic device to send and receive it. Computers and smartphones are incredibly powerful devices, but can easily catch viruses or be hacked by someone motivated enough.

A hardware wallet is a special device made to hold your Bitcoin. Similar to how a proper camera will take better pictures than a smartphone, a hardware wallet will do a better job of protecting your digital assets than a normal computer. Because it specialises in one core functionality, it can make it much easier to protect yourself from having your Bitcoin stolen.

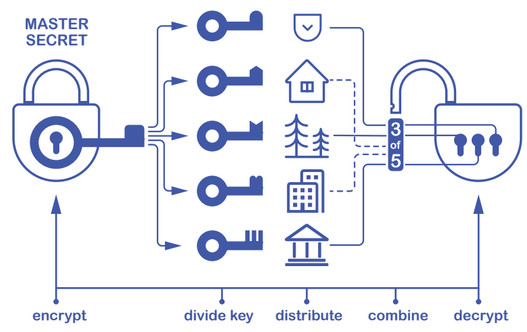
In practice, hardware wallets are small devices that can look similar to USB sticks with a display and buttons. They communicate with your computer either via USB or QR codes.

Don't be intimidated though. A good hardware wallet will guide you through the installation and use. We recommend the BitBox02, as it is highly secure and very easy to use.

SHAMIR'S SECRET SHARING

EXPLAINED BY TREZOR

Shamir's secret-sharing provides a better mechanism for backing up secrets by distributing custodianship among a number of locations or trusted parties in a manner that can prevent loss even if one or a few of those parties become compromised or lost. The scheme allows you to split your recovery seed backup into multiple independent parts called shares.
Cryptosteel Capsules have been boxed together to support the Shamir Backup secret-sharing scheme as implemented by SatoshiLabs in the SLIP-39 standard. The sets "TRIO" and "QUINTET" can be used to store a master seed using the 2-of-3 and 3-of-5 schemes, respectively, and multiple sets can be used for up to x-of-16.



MY RESPONSIBILITIES, MY POWER

GPGR = with great power comes great responsibility
You maintain full possession and control of your data. There is no way to recover your lost backup. It is up to you to protect your backup and remember to always keep the fastener on the core.

SPOF = single point of failure
In decentralized systems, there is no main authority who may revoke or restore your passwords. If you lose your key, there is no way to get it back.
If one part of a system failing causes the entire system to stop, that is known as a single point of failure. Redundant copies and Secret Sharing Schemes are the solution for this.

Socrates said "Know Thyself"
Acknowledge your limitations. The Capsule provides standardization for Offline Backup Solutions. Unless you are a tremendously skilled professional, please take our advice and avoid creating an untested or undocumented cryptosystem that could lock you or your relatives out of your own money.

ADDITIONAL SECURITY FEATURES

The Capsule is a universal backup tool, and it's up to the user to decide what level of protection they need. The main security feature provided by the Capsule is the availability of the stored information. Depending on the type of information stored, additional security features may be required.
Example: Having stored a backup copy of a private key for signature, one needs to know if an outside agent has read the key while it was stored in the Capsule, and in the case of a compromised private key, revoke the related public key.

- It's possible to put a DIY **tamper-evident seal** on the Capsule. Depending on your needs you can add paint, nail polish, sealant, a special envelope, etc. You can also weld it closed to create a fireproof barrier seal.
- You can create **fireproof identification labels** with the provided tiles. Place a wire through the cap hole, bend a tile in half with a hand tool, thread it on the wire, and clamp it tight.
- For those using a hardware wallet, most producers recommend adding a **passphrase to the seed**. Please read the manufacturer's instructions on how to add one. If you want to make a physical backup of your passphrase, do not store it next to the backup of your seed. Use another Capsule stored in a different location.

STORABILITY

The Capsule is a solid metal device that has been designed to survive extreme conditions and to last for several lifetimes. It is resistant to crushing, compression, and corrosion. It's waterproof, fireproof, and shockproof. That, along with its small size, means that its ability to be stored or hidden is only limited to your requirements and imagination.

SHARE IT!

Please share this paper copy with your friends and loved ones.
Getting hacked is no fun.

- Bitcoin User Manual Booklet
https://github.com/cryptosteel/operational-security-manual

Ver. 07082023

ADDITIONAL SERVICES

- Personalization - We provide a wide range of engraving services as well as casual packaging services. You can find them on our webpage.
- White-labelling - If you wish to launch your own line of Capsules "Powered by Cryptosteel®" do not hesitate to contact us: **cryptosteel.com**

KNOW WHAT YOU BUY

Our products are researched, designed, developed, and produced in-house. We take your security seriously - no tradeoffs or corners cut. We use only high-quality materials and top-grade production technology. Being the pioneers of the market, trusted by hundreds of thousands of users, we provide peace of mind for you and future generations.
We make white-label versions for select companies and you can always find "Powered by Cryptosteel®" on the packaging to know that it is the real deal.
Don't be scammed by cheap imitations or risk buying one made of fraudulent materials.