cryptosteel

Product specifications

Capsule dimensions: length 102mm, diameter 16mm

Solid metal construction – 100% stainless steel

Shell made of AISI 303

Core, separators, fasteners and character tiles made of AISI 304

Packaging includes all printable ASCII characters (96 different characters).

Backup type compatibility

100% coverage for:

- BIP39 (unabbreviated 12-word recovery seeds or 4-letter abbreviations of 24-word recovery seeds)
- Shamir Backup SLIP39 (4-letter abbreviations of 20-word recovery seeds)
- BIP32 root keys
- WIF private keys
- Monero mnemonic seeds (4-letter abbreviations of 25-word recovery seeds)

more than 99% coverage for:

- hexadecimal strings up to 123 characters
- random ASCII strings up to 55 characters

Coverage based on analysis of more than 3.5M samples.

HIGH FLEXIBILITY

supports all printable ASCII characters

IMPROVED SECURITY

passwords are protected, not visible at first glance

ADJUSTABLE SEPARATORS

keep your mnemonic seed in full in 123 characters

HIGH MOBILITY

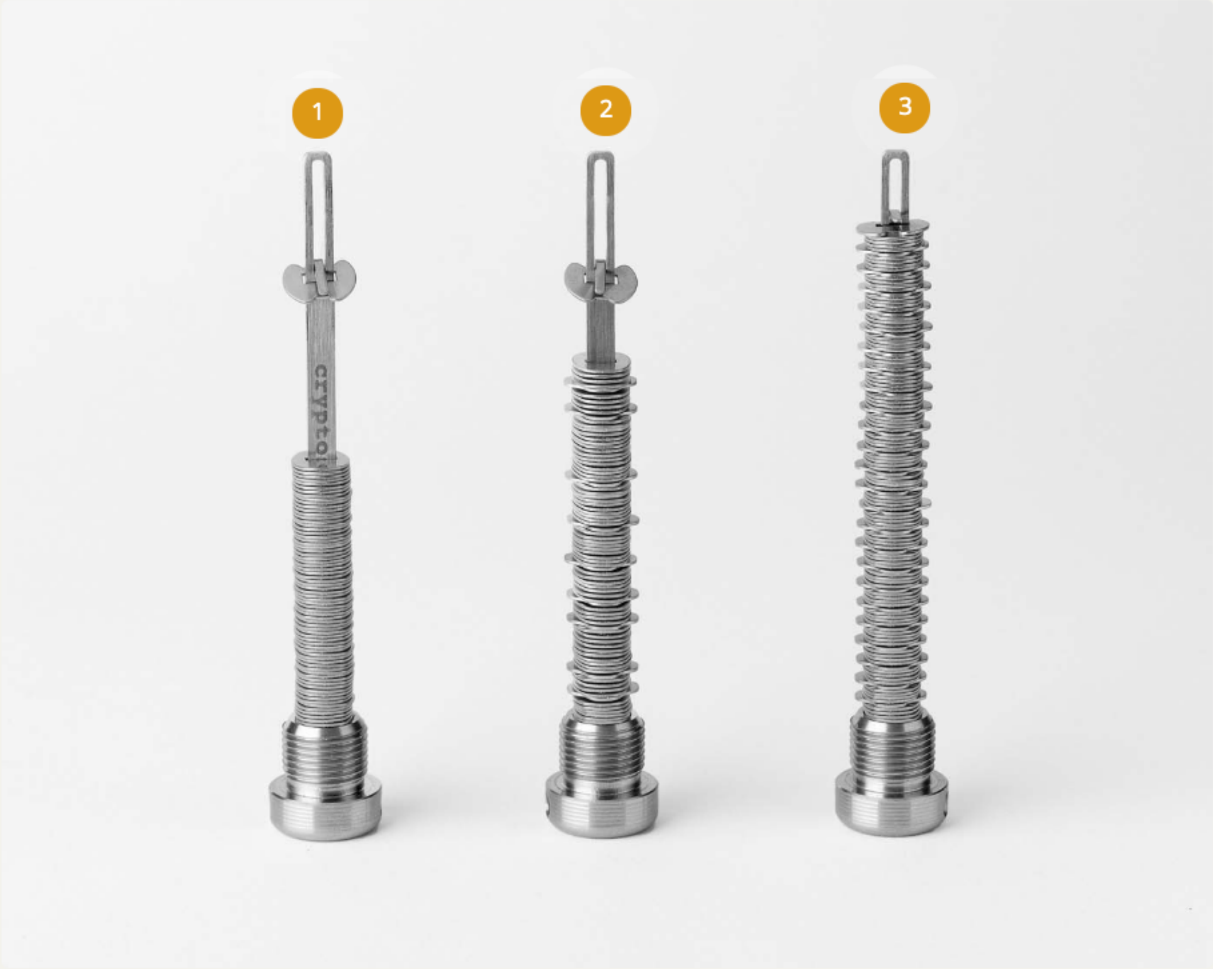
small, light, easy to hide and protect

TAMPER EVIDENCE

DIY fireproof barrier seal, capsule identification possible

EXTREMELY DURABLE

Fireproof up to 1400C/2500F. Shockproof. Waterproof. Stainless.



High Flexibility

The capsule features adjustable separators, offers more capacity – 123 instead of 96 characters most other solutions provide – and comes with a full ASCII-character-set supporting random passwords with numbers and symbols. All of the characters are deeply stamped into the tiles to provide maximum longevity.

This means that the capsule can securely store a random password without separators, an unabbreviated 12-word mnemonic seed, or the first four letters of a mnemonic seed made up of 25 word phrases.

1. The first example shows a random ASCII password stored on the core that is 55 characters long. Considering the unused space, two or more passwords can be stored, split using separators, up to 123 characters long, in total, including WIF, Hexadecimal, and Root Keys.

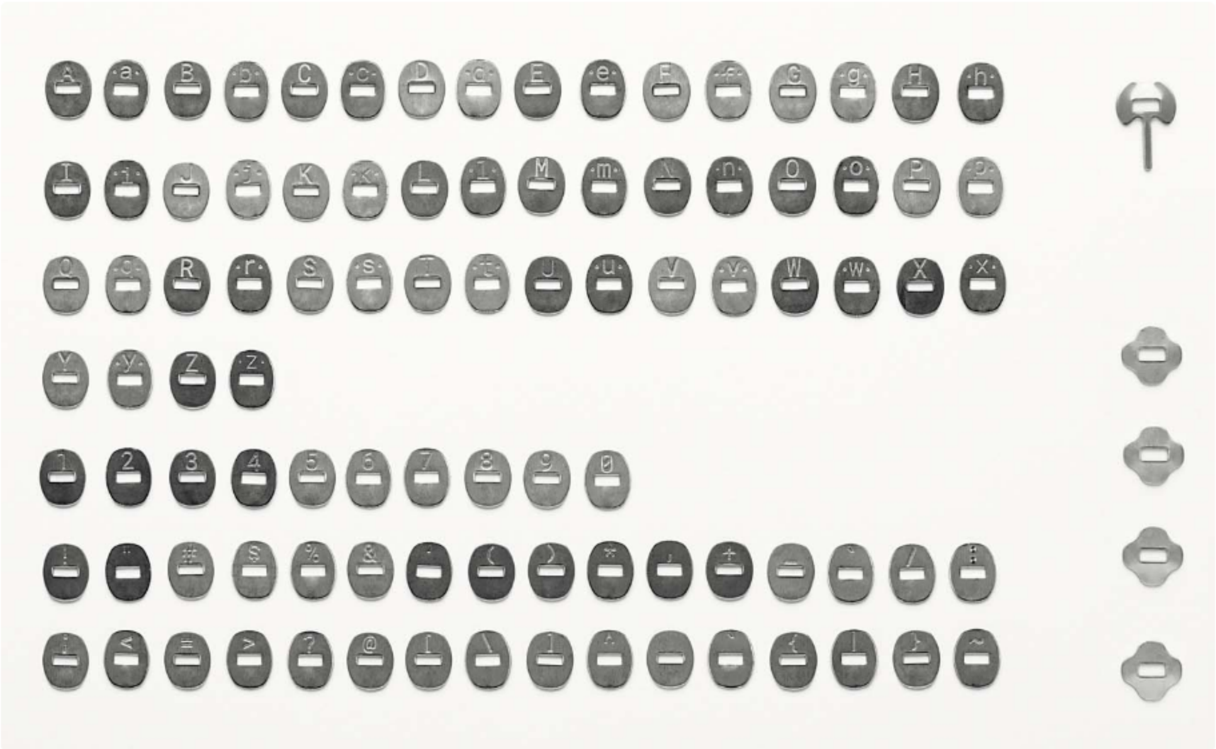
2. With the second, you can see an unabbreviated 12-word mnemonic seed. With the remaining space at the top, you can store additional data including passwords, passphrases, or random ASCII strings.

3. The third example demonstrates a 25-word abbreviated mnemonic seed. Of course, the aesthetically designed capsule is also able to store 20-word Shamir backups and 24-word recovery seeds in their abbreviated forms.

Standardised letter tiles vs hand-written solution

Our aim is to standardise the offline information protection system and provide a solution right out of the box. You don't need to think or worry about buying additional materials or special tools. You don't have to learn the hard way how painful engraving metal can be – no specific knowledge or safety equipment is needed. Simply open the pack and get started – everything you need is right there.

We use a classic, easy to read font that will be legible 10 or 100 years from now. Hand engravings will naturally differ from person to person. Over time, you (or your heirs) may not be able to retrieve the information from a hand-written backup due to style, ambiguity, or decay. Using standardised tiles, you can change, undo, or redo the data you wish to be guarded. Should you make any errors, you can easily correct them.



Packaging

We designed a sturdy box which is reusable, transparent for easy searching, ergonomic for ease of use, and made from recycled PET. We have ensured the tiles stay separate during transport and storage and that they are easy to take out of their respective compartments.

There is no need to throw away the remaining character tiles because their numbers are partially random – nothing is revealed about the characters used or unused in the device. And as a consequence, the valuable data does not get compromised, and you have all the tiles you need should you decide to change your code.

Shamir Backup Support

The usual approach to protecting digital assets is redundant backups, but when the asset itself is of significant value and high liquidity, there is a substantial risk of a backup custodian absconding with the asset.

The cryptographic secret-sharing scheme created by Adi Shamir is an ingenious way to help protect data.

How Shamir's secret sharing works?

Shamir's secret-sharing provides a better mechanism for backing up secrets by distributing custodianship among a number of trusted parties in a manner that can prevent loss even if one or a few of those parties become compromised. The scheme allows you to split your recovery seed backup into multiple independent parts called shares.

You may shield important information using Shamir Backup, which is supported by the Capsule. The master secret that you are protecting might never be compromised even in cases of aggressive acts including but not limited to theft, bribery, vandalism and violence where the knowledge of fewer than the required number of shares is discovered.

Cryptosteel Capsules have been boxed together in different packs keeping in mind the Shamir Backup secret-sharing scheme as implemented by SatoshiLabs in the SLIP39 standard. 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. Up to x-of-16.