Death Instructions

In the event of my death the following cryptosteel capsule will contain a secret that can be used (in conjunction with others) to decrypt my personal password safe.

What is this capsule?

It’s an indestructible device that when opened contains a secret. 4 capsules total exist. Only 3 of the 4 secrets are needed to decrypt a file named “mylife.txt.gpg” which will lead you all of my personal passwords.

How this works

1. I die, that sucks
2. My spouse, my mom, or my dad will reach out to you confirm my death and invoke the decryption process. They will know where the file “mylife.txt.gpg” is located (physically and digitally).
3. Open the capsule and read the secret (NOTE!!!!! Do not take the pieces off of the core! You risk losing the order of characters. Read them one-by-one with the retainer clip in place.)
4. Once you have 3 of the 4 secrets, run the following command and it will output the cleartext passphrase used to decrypt the mylife.txt.gpg file.
   1. ssss-combine -t 3
   2. Enter each secret including the prefixed number and dash. A successful output will have a readable passphrase. If your output is a random set of characters something is wrong.
5. Decrypt the gpg symmetrically encrypted file with gpg -d mylife.txt.gpg using the password from ssss-combine.
6. Further instructions on how to access my personal password safe along with the current password to it will be within this file.

Who has capsules and where can I find them:

|  |  |  |  |
| --- | --- | --- | --- |
| Capsule Number | Name | Address | Phone |
| 1 | Person 1 |  |  |
| 2 | Person 2 |  |  |
| 3 | Person 3 |  |  |
| 4 | Person 4 |  |  |

Additional info:

The file “mylife.txt.gpg” is symmetrically encrypted with a passphrase and was created using the following command:

gpg -c --no-symkey-cache mylife.txt

The gpg file uses AES-256

The shamir secrets were created with the following command:

ssss-split -t 3 -n 4

ssss version 0.5 was used