“testamento” “digitale”

hackmeeting 0x19 - panda

premessa

- ho solo che delle domande

casi

- per qualche motivo sono impossibilitat* a gestire i miei “segreti”, permanentemente:
  - roba/accessi che il/la mi* compagn* di vita deve avere
  - accessi di/per servizi condivisi con altr* compagn*

Come?

- con un quorum di **x** persone su **n**, che tramite..
  - con le chiavi GPG che gia' usiamo ogni giorno? (https://git.lattuga.net/panda/gpg-quorum)
  - Shamir's secret sharing (https://secrets.dyne.org/about) ?
- ..possa:
  - recuperare una chiave di cifratura simmetrica
  - aprire direttamente un file cifrato con GPG
- dove:
  - file cifrato ma pubblicamente disponibile
  - file cifrato su un qualche supporto di memorizzazione

cosa contiene il file

- Le istruzioni per recuperare I dati?
- Il proprio password manager aggiornato?
- Un testamento di qualche tipo (olografo e/o biologico)? Ha valore? (io non ne ho idea)

robe collegate

- Progetto di long-term-storage

Note emerse durante il talk:

- NB: esiste anche 2FA/OTP oltre al pwmanager, o viene salvato il codice di configurazione dei codici o serve il device con 2FA/OTP
- Esecuzione automatica codice post-mortem (bypass parziale della fiducia)
- Obsolescenza degli script usati (gpg un giorno non sara' piu' compatibile con le versioni di oggi, soluzione hw, altro?)
- Per quanto riguarda gpg-quorum (gpg cipolla):
  - Revoca di una persona
  - Disponiblita' del file (online da qualche parte? Fisica in casa? Notaio? Persona ulteriore ai "fiduciati"?)

Note emerse durante il talk 2:

- Alcuni servizi hanno una policy di inattivita’ (o lo fanno con cert di morte): replicabile su servizi autogestiti? (tipo delete after 1y incative)
- Differenziare cosa-va-a-chi (ES: alcune cose vorrei che andassero alla mia comapgna, altre cose no perche’ mi sono state affidate da altri)
- Come essere sicuri che certa roba vada distrutta?