Zero Knowledge Communication
joind.in/talk/49bad
@bendechrai

Ziel: komplett verschüsselte Datentransfer vom Client bis zum Backend-Backend
Beispiel: Kontoumsatzliste, Kategorisierung :)

verschlüsselte Nachrichten (Whatsapp) könnten auch Plaintext geschickt werden, TLS ist nur noch für Endpoint-Ident
Private Key gehört nicht in die Cloud (Token auch nicht)
Passwort sollte schon im Browser gehasht werden (z.B. mit bcryptjs)
Decrypt vom verschlüsselten Nutzerprofil erfolgt im Browser mit seinem Passwort (als Private Key)
kann transparent zum bestehenden Login-Prozess bestehen - ist ja nur ein anderes Passwort

Homomorphic Encryption
Kategorisierung (z.B.) wird mit verschlüsselten Strings durchgeführt
funktioniert nicht mit komplexen Datentypen

es gibt einen Commitstrip :)

(es gibt ein Zsh? Theme wo der Prompt die Zeit zeigt seit Shell-Start)

Problem des Ansatzes: Private Key steht tatsächlich in der Datenbank, aber ist per Passwort geschützt

Super Konzept für Passwort-Manager!