Tahoe-LAFS—encrypted peer-to-peer storage
Brian Warner, Zooko Wilcox-O'Hearn, Daira Hopwood, and many others
Why do we do what we do?
Each component of a system should have the least authority necessary to perform its function.

The Principle of Least Authority
• end-to-end security
• open system — no “Digital Rights/Restrictions Management”
• decentralized — no “Trusted/Treacherous Third Parties”
• economically sustainable
• Free and Open Source

Requirements
Unify designation and authority.

“Programming Semantics for Multiprogrammed Computations” J.B. Dennis, E.C. VanHorn, 1966


Capabilities
Crypto-Caps in LAFS
Directories

mutable directory

maxwell.pdf

miller.pdf

notes.txt

read cap

read cap

read cap

read cap

public key (RSA), cipher key (AES)

private key (RSA), cipher key (AES)

immutable

immutable

mutable
Read-only Access to Directories
Immutable Directories

- Immutable directory
  - maxwell.pdf
  - miller.pdf
  - notes.txt

- read cap
- hash value (SHA256), cipher key (AES)
- write-only caps (public key encryption!)
- append-only caps (consensus problem?)
- revocation
- YOUR IDEA HERE

Open Problems, Future Work, HELP!
Brian Warner, Zooko Wilcox-O'Hearn, Daira Hopwood, and many others

to learn more:
  · https://Tahoe-LAFS.org
  · https://LeastAuthority.com

The Least-Authority File System