

FOKS and other stuff I like

Boulder Linux Users Group - Lightning talk

2025-07-10

Neal McBurnett

QR code for this talk (also on the last page):



Neal McBurnett

- Consultant on Big Data, Election Integrity, Voting Methods
- Computer Scientist, Ex-Bell Labs
- Technology serving Community via Boulder Community Network etc. since 1994
 - Free Software, Linux, Ubuntu, ...
- Working on election audits and integrity since 2003
- Pioneered RLAs for Boulder (2010) and Colorado's current state-wide audit
- LWV rep to Colorado's **Bipartisan Election Advisory Commission**
- **nealmcb@keybase**

Overview

- FOKS - Federated Open Key Service
- Other stuff if I have time

FOKS - Federated Open Key Service

Any **Keybase** lovers here?

... who **wanted the server side to be open source #24105?**

=> **Federated Open Key Service (FOKS)**

- Fully open source (client and server), federated, post-quantum key management security infrastructure, as a follow-on to Keybase by some of the original developers.
- End-to-End Post-Quantum Encrypted Git Hosting
- End-to-End Post-Quantum Encrypted Key-Value Store
- Federated and Generalized Team Management with teams-of-teams, delegation etc.

FOKS crypto

- Device Management with Full YubiKey Support
 - You can revoke access to a device if it is lost or stolen. Revoking triggers a cascading key-rotation across all teams you are members of, whether local or federated. This keeps data secure going forward.
- NACL, Curve25519, post-quantum via NIST-standardized Module-Lattice Key Encapsulation Mechanism (ML-KEM aka Kyber)

FOKS aims currently to provide the best possible security for long-lived data, like persistent file storage (Git) and persistent key-value storage.

FOKS Privacy

Despite its ethos of forcing servers to immutably and publicly commit to cryptographic data, FOKS hides personal information behind one-way commitments as much as possible. Details like user names, team names, device names, team memberships and leaf locations remain obscured unless users are granted explicit permission to access these data. Thus, users on the same server can feel confident that their personal metadata are safe, even as the server commits to the global state of all its data.

FOKS business model

FOKS initiator Max Krohn:

We know that a lot of projects start as open-source, but later rug-pull their users due to the economics of their funding models. The creators behind FOKS have not taken on any outside funding, and are pursuing its creation as a passion project. We think there might be a good business in being a default hosting provider for FOKS, which might provide the funding for the team to continue development of the project indefinitely.

FOKS vs Keybase

- Small application feature space so far:
 - key-value store
 - very secure Git hosting
- Many applications can be built on that, client-side

Wanted:

- General-purpose signatures and encryption to public public key (vs via DNS?)
- I want Keybase-like proofs of a person's email address, website, github, online postings, social media identities, etc
 - See e.g. <https://keybase.io/nealmcb>
 - More complicated in FOKS than Keybase due to federation, and signature chains often being host-specific or private
- Nice to have? SSO, user-to-user connections, secure messaging, verifiable randomness (play poker online), secure timestamps?, secure money transfers, ...

Other stuff I could riff on

- Help me help Colorado Clerks better secure paper ballots via ballot image provenance: tiny Rust Windows app
- AI: Importance of open source for freedom, replication: (OSAID and/or MOF): Open Reasoning work, OLMo
 - DeepSeek open model: a good start, see also MiniMax-M1
- Check out Rubin observatory: extraordinary new era in astronomy: petabytes of open full-sky "video" for dynamics of the universe
- Explore [Waterways of the world](#) and public [Mapillary](#) street view data: contribute via [OpenStreetMap](#)

Questions?

This talk:

