# draft-josefsson-scrypt-kdf

Rich Salz
(for Simon Josefsson)

# Scrypt KDF

- Password-based key derivation function
- Widely used:
  - Facebook
  - Android (previously pkbdf2)
  - Litecoin (can now find scrypt-miners)
- To appear in OpenSSL 1.1

# Current draft

- Pseudo-code (Python)
- Includes test vectors
- Used to drive implementations (TAO)

# Goals

- Seeking CFRG input and review
- To be published as informational RFC
  - So that other IETF RFC's can use it