Idea: Zero Knowledge Logins

The following document will go over the design details related to providing zero knowledge logins, as outlined in Story ticket UFC-XXX.

Motivation

- People don't trust services with their passwords.
- Servers and database can be comprised.
- As such, making it so that people can trust services by *never providing them their passwords* seems like a win-win.

Acceptance Criteria

- TODO

Prior Art

- Let's talk about PAKE – A Few Thoughts on Cryptographic Engineering
- OPAQUE protocol: https://eprint.iacr.org/2018/163.pdf
  - Supposedly a better protocol than SRP.
- Zero Knowledge Proofs: An illustrated primer – A Few...
- Secure Remote Password protocol - Wikipedia

Design Brainstorming

- TODO