OPAQUE with TLS 1.3

Sofía Celi
Cloudflare
IETF110

Context

- OPAQUE is a mutual authentication method that enables the establishment of **an authenticated cryptographic key** between a client and server based on **a user's password**, without ever revealing the password to servers or other entities other than the client machine.
- OPAQUE is being standardized in draft-irtf-cfrg-opaque
- Consists of 2 phases:
  - Registration: register password and store encrypted credentials
  - Authentication: obtain and decrypt credentials, and use them in an AKE.
- Goal: Combine password-based authentication with traditional PKI-based authentication

The ideas

- After registration, the user (through a client machine) and server run the AKE stage of the OPAQUE protocol: a concurrent OPRF and key exchange flow.
- Combine OPAQUE as:
  - Part of the handshake itself: authenticate (mutual) a TLS handshake with a password alone. It cannot be used conjunction with certificate-based (m-)authentication. It can be used with Exported Authenticators for post-handshake: **OPAQUE-Sign**
  - Part of the handshake with a shared secret: the secret is fed into the key schedule for the handshake, which uses certificate-based authentication and establishes the shared key using Diffie-Hellman. There is no unilateral authentication, mutual authentication is demonstrated explicitly through the finished messages: **OPAQUE-KEX**

Security/Privacy considerations

- It does not provide identity hiding for the client, except when used with Exported Authenticators or Encrypted Client Hello.

- The draft location: https://github.com/grittygrease/draft-sullivan-tls-opaque

Thank you!