The OPAQUE Asymmetric PAKE Protocol

draft-irtf-cfrg-opaque-11

D. Bourdrez, H. Krawczyk, K. Lewi, C. A. Wood – IETF 117 – CFRG
What is OPAQUE?

OPAQUE is a compiler for translating:

- an OPRF
- A hash function,
- A memory hard function (MHF), and
- An authenticated key exchange (AKE) protocol

into a strong, augmented PAKE.

Recommended configurations for OPAQUE-3DH:

1. ristretto255-SHA512, HKDF-SHA-512, HMAC-SHA-512, SHA-512, Argon2id(...), ristretto255
2. P256-SHA256, HKDF-SHA-256, HMAC-SHA-256, SHA-256, Argon2id(...), P-256
3. P256-SHA256, HKDF-SHA-256, HMAC-SHA-256, SHA-256, scrypt(...), P-256
Overview

Two protocol phases:

- Offline registration: Clients use password to register public key credentials with the server
- Online login: Clients use their password to recover public key credentials from the server and complete an AKE

This document specifies OPAQUE-3DH with accommodations for future AKE instantiations (TLS 1.3, SIGMA-I/R, HMQV, etc.)
Updates since IETF 111 (July 2021)

**Major:**
- Added configurability for OPRF group vs. AKE group
- Added test vector support for AKE group curve25519
- Removed “internal” and “external” EnvelopeMode configurability
  - We now default to internal mode, and applications which want to bring in an external AKE private key can be supported with future extensions to this draft

**Minor:**
- Aligning with draft-irtf-cfrg-voprf-21
- General editorial improvements
Next Steps

- We believe the document is ready for RGLC

You can leave feedback as an issue on Github: https://github.com/cfrg/draft-irtf-cfrg-opaque/issues

Thank you! Questions?