

OPAQUE

draft-irtf-cfrg-opaque

OPAQUE is a compiler for translating an OPRF, hash function, memory hard function (MHF), and authenticated key exchange (AKE) protocol into a **strong, augmented PAKE**

OPAQUE

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

Draft status

Major:

- Add *internal* and *external* modes for AKE private key storage
- Add client enumeration mitigations during authentication, along with “fake” test vectors
- Replace application info with shared context string (matching SPAKE2+), making all protocol messages fixed-length

Minor:

- Improve security considerations around message decoding and trust boundaries
- Align with **draft-irtf-cfrg-voprf-07**
- General editorial improvements

Next steps

Towards RGLC

Help wanted!

Add more implementations (Node.js, Go, Rust, C/C++)

New Crypto Review Panel review (and revisit past PAKE competition reviews)

Ready to ship

Questions?