OPAQUE

draft-irtf-cfrg-opaque
Editor's Copy, Individual Draft

CFRG @ IETF 109 (Virtual)

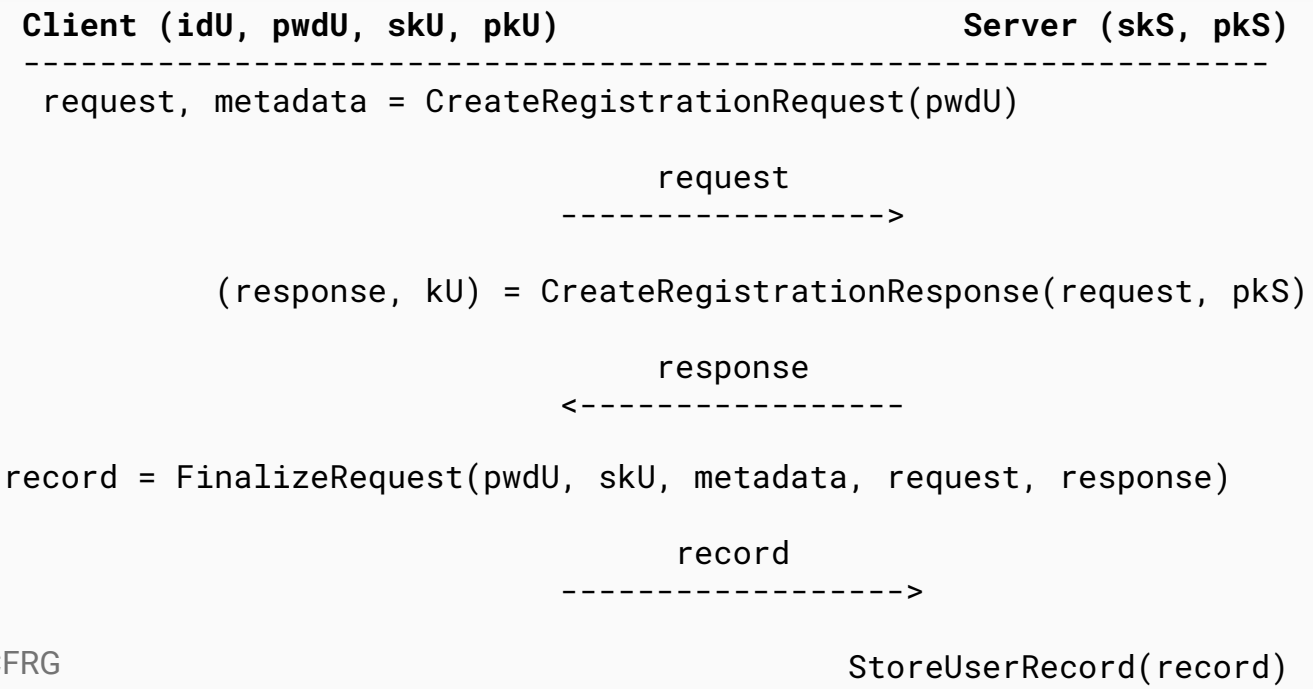
OPAQUE is a compiler for translating an **OPRF**, **hash function**, **memory hard function** (MHF), and **authenticated key exchange** (AKE) protocol into a strong, augmented PAKE

Overview

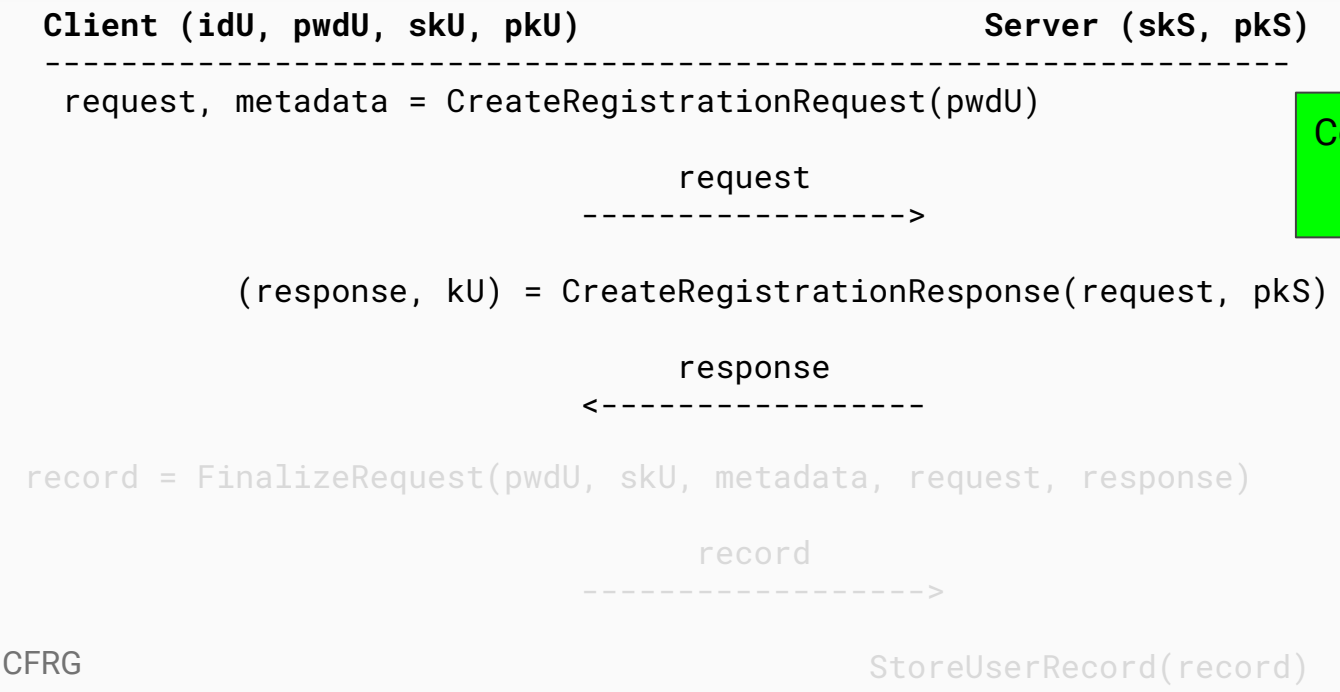
OPAQUE consists of two phases:

1. **Registration**: Clients use password to register public key credentials with the server
2. **Authentication**: Clients use their password to recover public key credentials from the server and complete an AKE

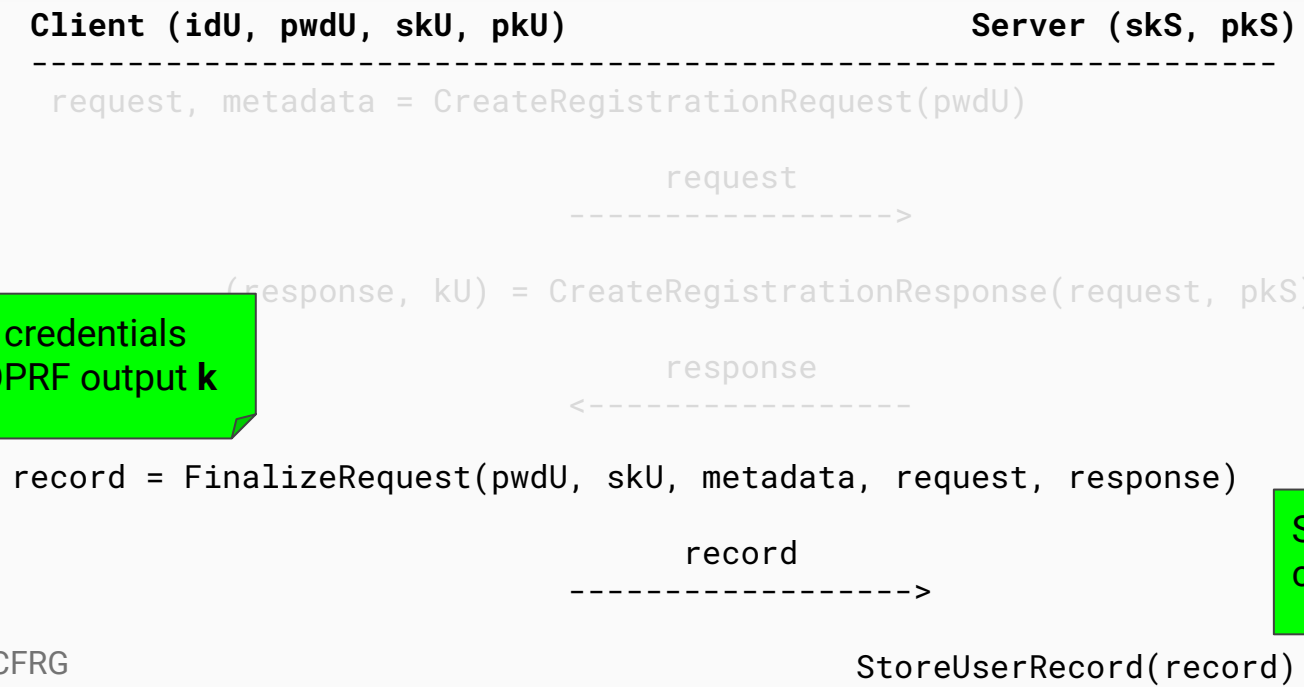
Registration Flow



Registration Flow



Registration Flow



Protect credentials under OPRF output **k**

Store protected credentials (envelope)

Registration Credentials

Client credentials are protected under a secret derived from **F(kU, pwdU)**

Per-client OPRF key

Client password

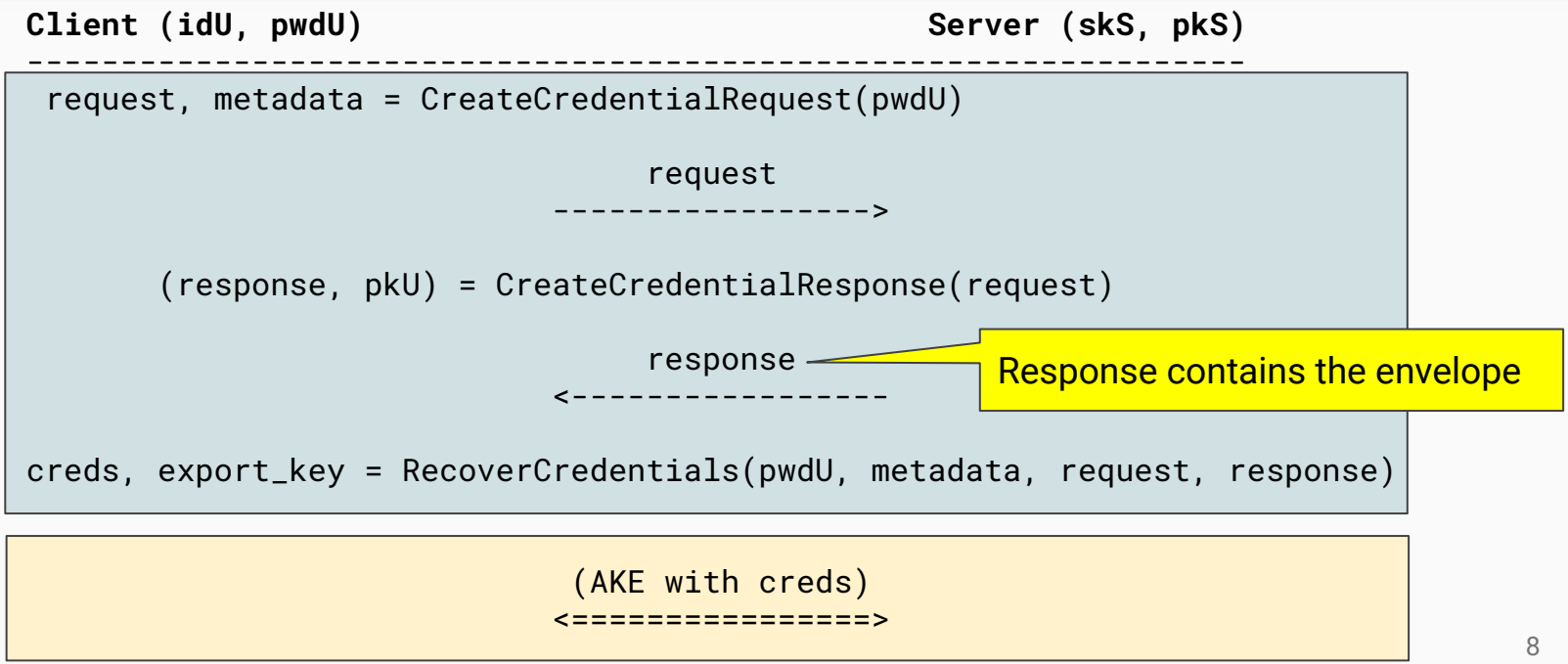
Credentials consists of **secret** values and **authenticated** types

```
enum {
  skU(1),
  pkU(2),
  pkS(3),
  idU(4),
  idS(5),
  (255)
} CredentialType;
```

skU(1) → Encrypted in the envelope, used to authenticate client

pkS(3) → Authenticated in the envelope, used to authenticate server

Authentication Flow



AKE Integration

The AKE is run inline with the core OPAQUE protocol such that the AKE transcript includes all OPAQUE messages

AKE Integration

The AKE is run inline with the core OPAQUE protocol such that the AKE transcript includes all OPAQUE messages

OPAQUE-3DH

```
C->S = credential_request, nonceU, info1, idU, epkU

S->C = credential_response, nonceS, info2, epkS, Einfo2, MAC(Km2; transcript2)

C->S = info3, Einfo3, MAC(Km3; transcript3)
```

Configurations

OPAQUE configurations specify a (OPRF, Hash, MHF, AKE) tuple

Examples:

OPRF(ristretto255, SHA-512), SHA-512, Argon2id, 3DH

OPRF(P-256, SHA-256), SHA-256, scrypt, TLS 1.3

Application Integration

Applications configure the following OPAQUE parameters:

- Configuration
- Credential structure
- *Export key usage

Open Issues

Document review requested!

#77: AKE specificity

#69: MHF parameter specification

#22: User enumeration concerns

#82: Land test vectors

Implementation Status

Reference implementation: OPRF(ristretto255, SHA-512), SHA-512, scrypt, 3DH

Novi (Rust): OPRF(ristretto255, SHA-512), SHA-512, scrypt, 3DH

Cloudflare (Go): OPRF(P-256, SHA-256), SHA-256, Argon2id, TLS 1.3

OPAQUE

draft-irtf-cfrg-opaque
Editor's Copy, Individual Draft

CFRG @ IETF 109 (Virtual)