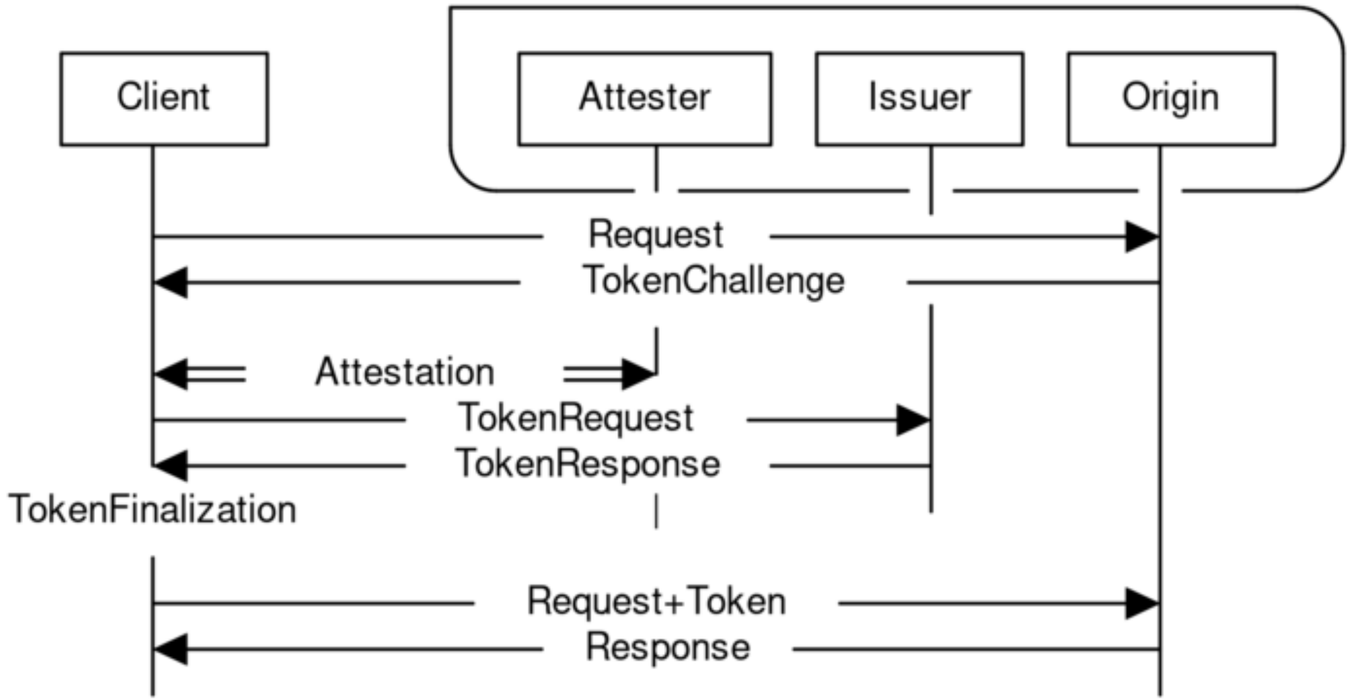
Anonymous Rate-limited Credentials (ARC)

draft-yun-privacypass-arc

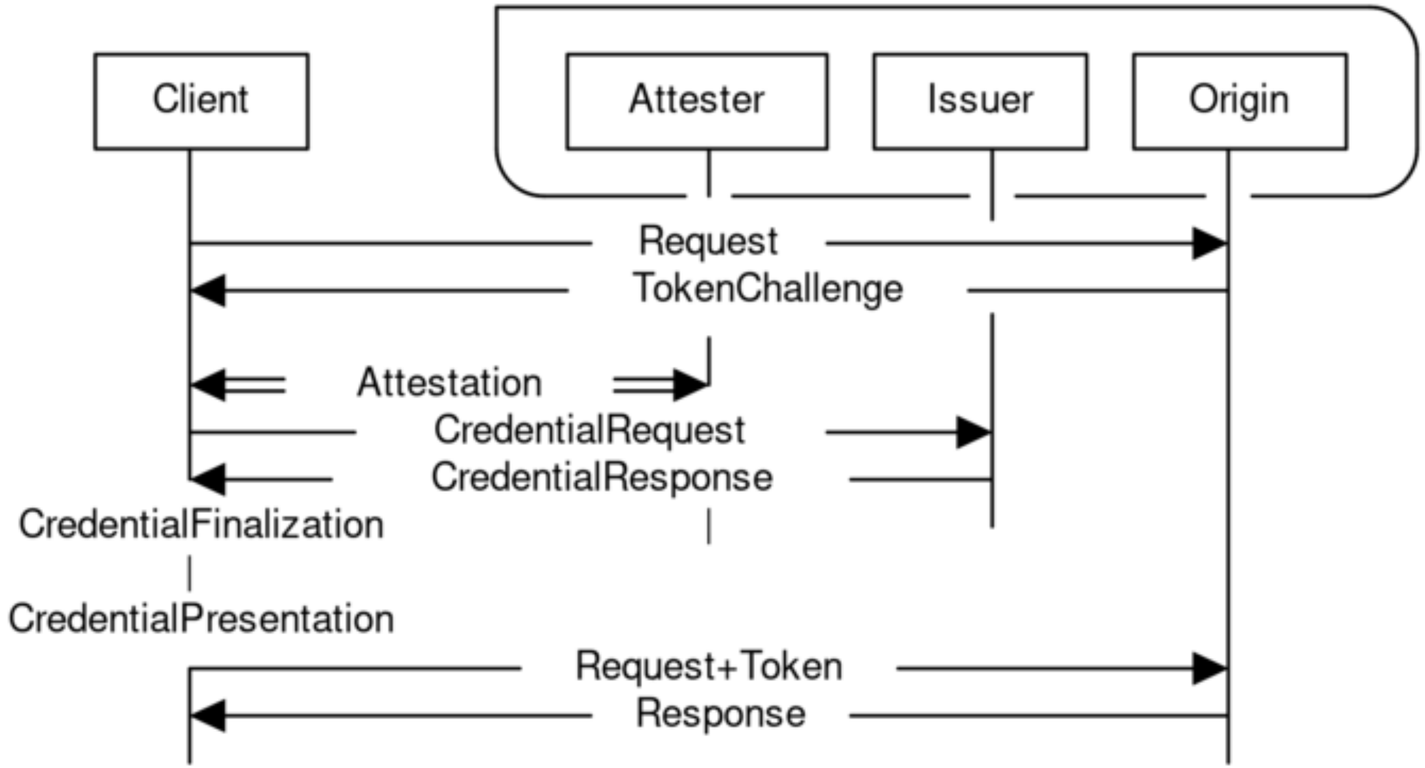
draft-yun-privacypass-crypto-arc

IETF 124 - Privacy Pass
Cathie Yun

Privacy Pass (RFC9576) workflow



Anonymous credentials workflow



ARC: Anonymous Rate-limited Credentials

A better approach to rate-limited tokens

1. Supports per-client rate limiting
    - This is built-in, as each client's credential inherently rate limits that client
2. Many tokens can be created from one issuance
    - One issuance allows for creation of one credential
    - Tokens can be derived from that credential, up to the rate limit
    - With rate limiting per origin and/or epoch ("late origin-binding")

Updates since IETF123

1. Calls for adoption
2. Nonce hiding (range proofs)
3. ZKPs using Sigma Protocol / Fiat-Shamir specs

Calls for adoption

- Calls for adoption in Privacy Pass
  - `draft-yun-privacypass-arc`
  - `draft-yun-cfrg-arc` → `draft-yun-privacypass-crypto-arc`
    - Agreement between Privacy Pass and CFRG chairs:
      Privacy Pass will solicit a Crypto Panel review prior to WGLC
- Conclusion: both drafts adopted by Privacy Pass!

Nonce hiding (range proofs)

Hide the nonce, for more robust privacy properties

- Solution: add a range proof with arbitrary `rateLimit`
  - Power-of-2 range proof: bit decomposition, prove each bit is 0 or 1
  - Modification for arbitrary `rateLimit`: decomposition base choices
  - Modification for avoiding “OR” proofs (higher complexity): instead, use “AND” statements to prove each bit is 0 or 1
- Caveat: will change performance (increase presentation creation & verification)

Nonce hiding (range proofs)

Hide the nonce, for more robust privacy properties

- Status: specification complete, reference implementation in progress
- Note: this is also useful for VDAF FLP proofs (see CFRG VDAF talk)
- Thanks: Chris P, Lena, Michele, Jonathan, Sam, Watson, and Ian!

Zero-knowledge proofs

- Update: CFRG adopted zero-knowledge proof “building block” specs `draft-irtf-cfrg-sigma-protocols` & `draft-irtf-cfrg-fiat-shamir`
- ARC moving to use the Sigma Protocol & Fiat-Shamir specs
  - Will replace ARC spec `Section 5.1: Schnorr Compiler`
  - ARC adoption has informed Sigma/F-S API and spec changes
- Status: specification complete, reference implementation in progress
  - Sigma/F-S reference uses an opinionated EC group implementation (more details in CFRG talk tomorrow)

Next steps

- Analysis of ARC in relation to other Privacy Pass token types:
  - RSA blind signatures, VOPRFs, batched-issuance VOPRFs
  - and other anonymous credential schemes: ACT, ATHM*, ?
- Reference implementation with nonce hiding, use of Sigma/F-S specs
- Investigate post-quantum / “everlasting anonymity” alternatives

*Anonymous Tokens with Hidden Metadata (ATHM):
https://datatracker.ietf.org/doc/draft-yun-privacypass-athm/
https://datatracker.ietf.org/doc/draft-yun-cfrg-athm/