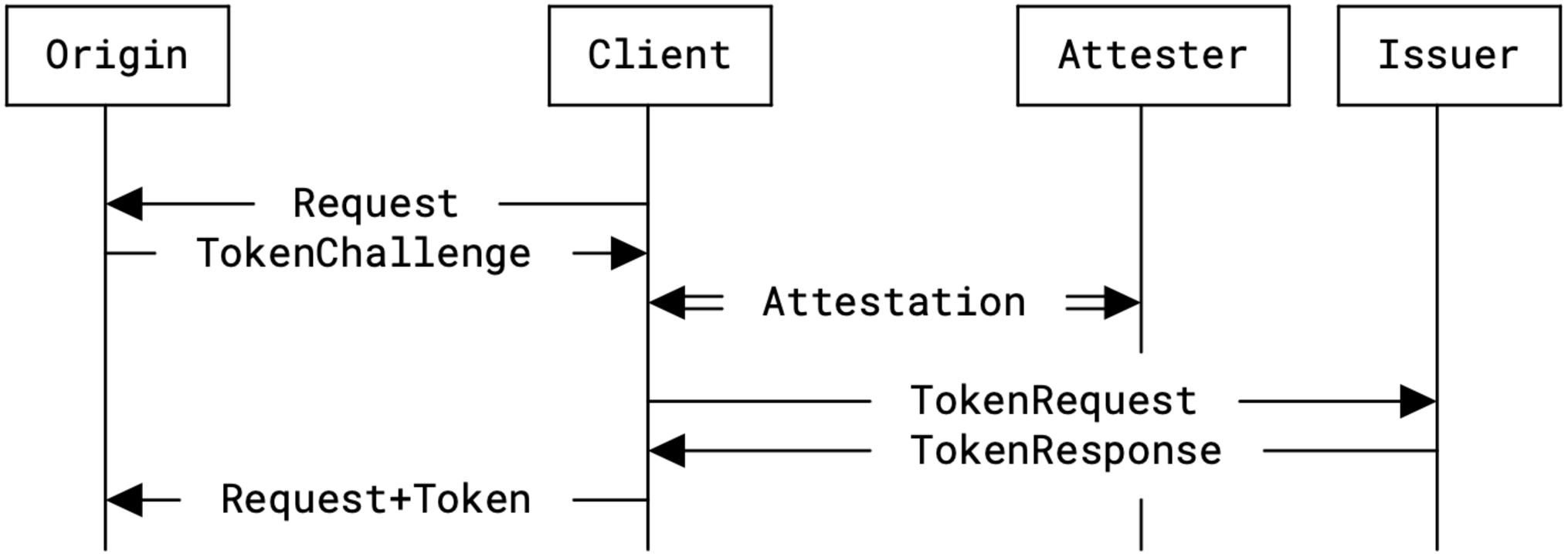
Privacy Pass Issuance Protocol for Anonymous Rate-Limited Credentials

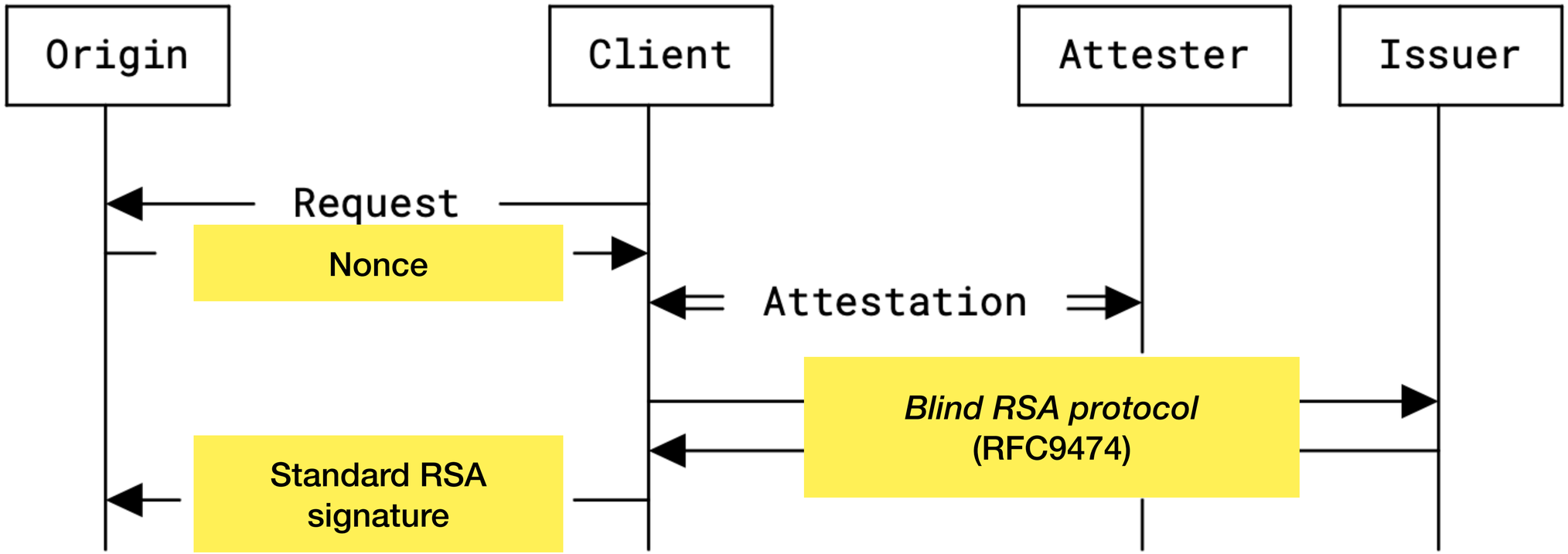
draft-yun-privacypass-arc

IETF 122 - Privacy Pass

Privacy Pass (RFC9576)



Privacy Pass (RFC9576)



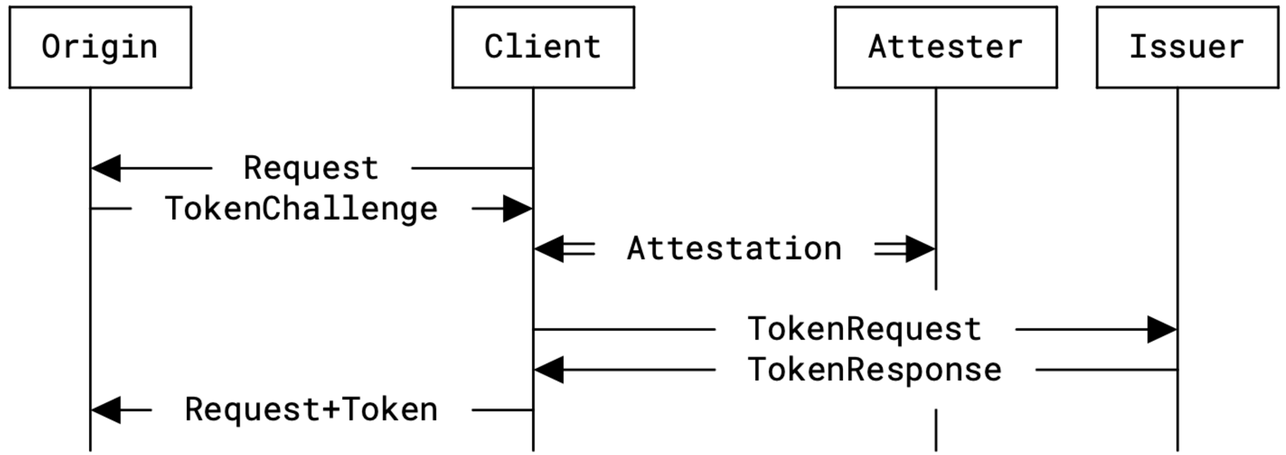
Privacy Pass (RFC9576)

Client Tokens are unlinkable from other Tokens and TokenRequests

Cannot distinguish between N tokens that come from the same Client, and N tokens that come from N different Clients

One TokenChallenge yields at most one Token

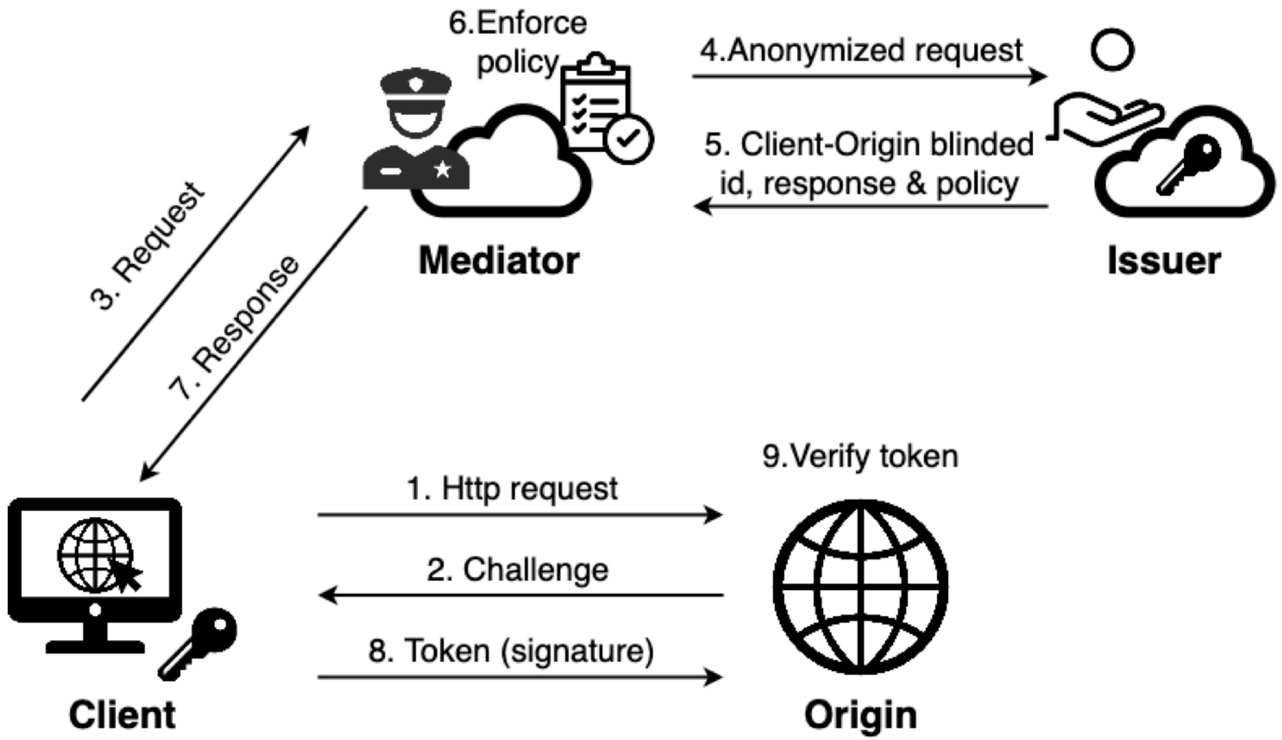
Client, Attester, and Issuer communicate for every single Token



Privacy Pass Limitations

Pros	***Cons***
Built on simple, widely deployed cryptographic protocols	No per-client rate limiting
	1:1 issue:token

Rate-Limited Privacy Pass



https://datatracker.ietf.org/doc/draft-ietf-privacypass-rate-limit-tokens/

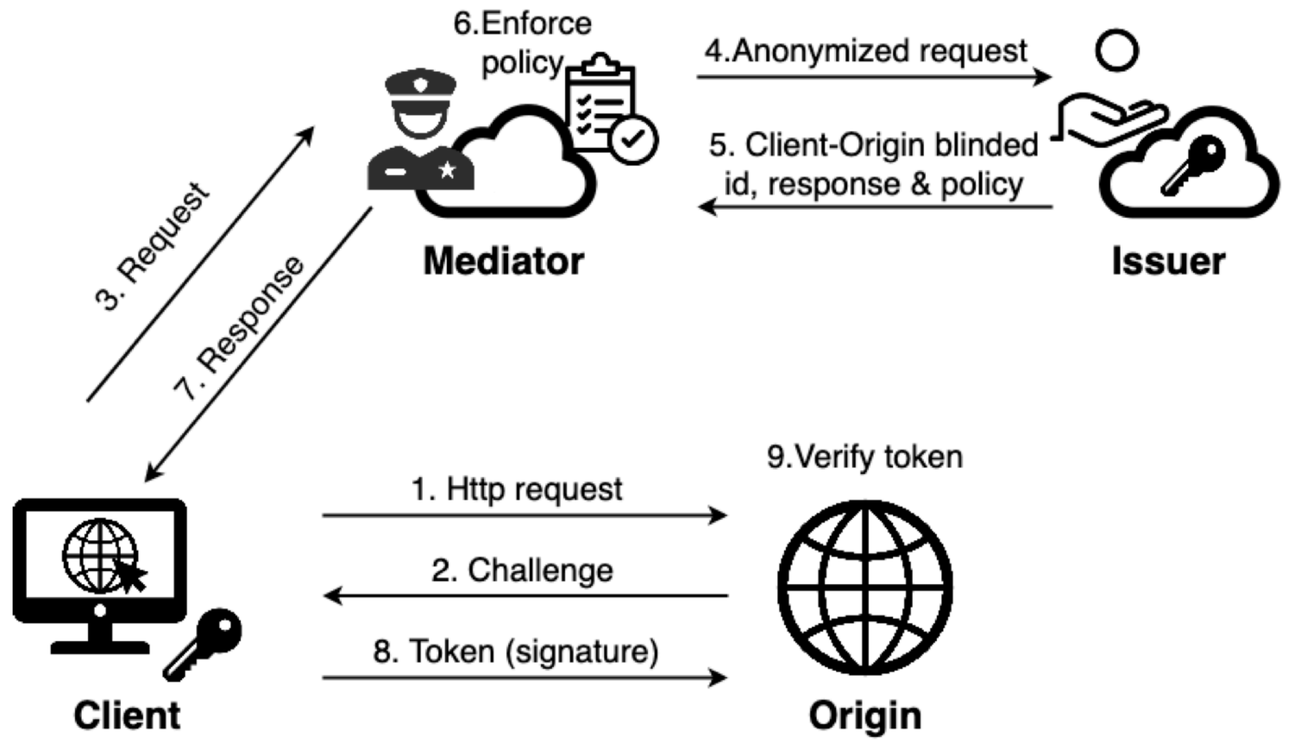
https://eprint.iacr.org/2023/1805.pdf

Rate-Limited Privacy Pass

Non-collusion requirement between Attester, Issuer, and Origin for privacy

Controlled privacy leakage to Attester (Mediator) required to enforce the rate limiting policy

Does not solve 1:1 issue:token cost



https://datatracker.ietf.org/doc/draft-ietf-privacypass-rate-limit-tokens/

https://eprint.iacr.org/2023/1805.pdf

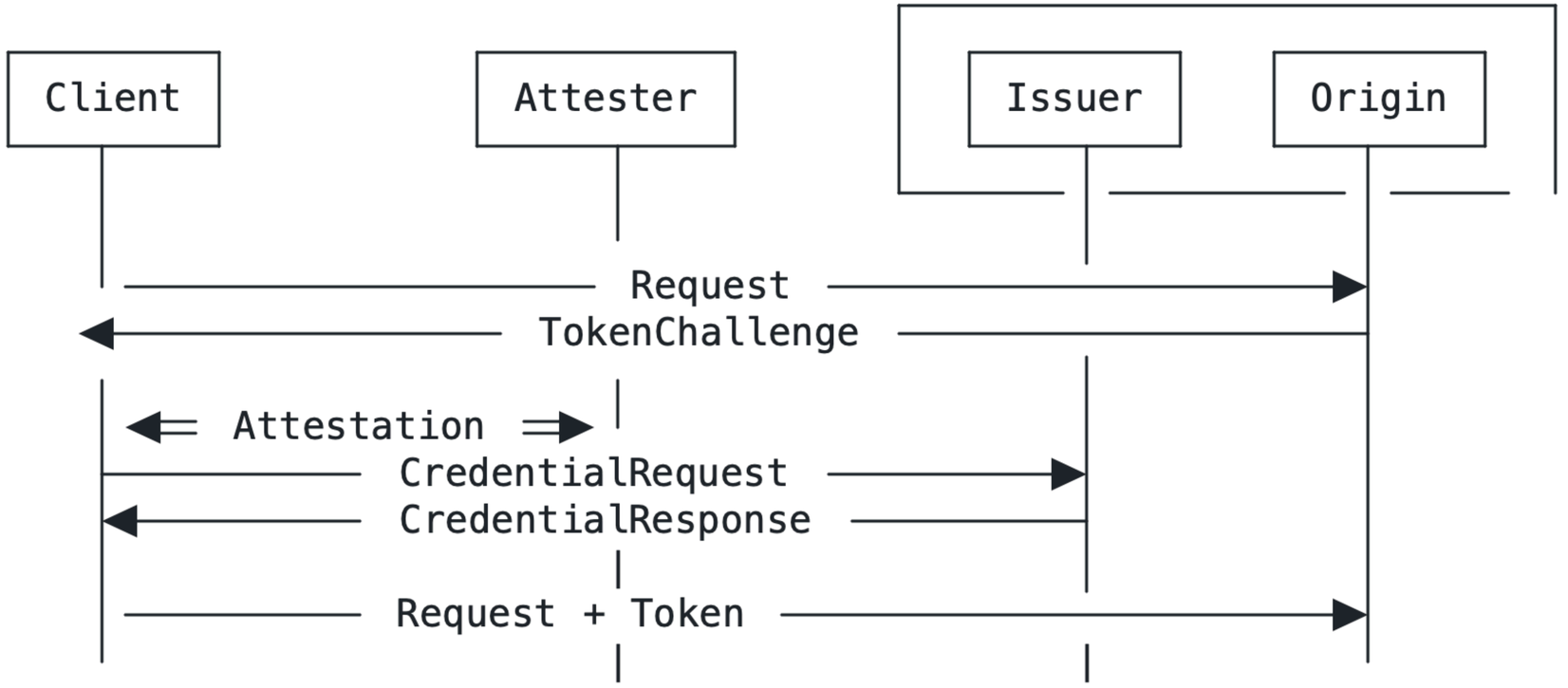
ARC: Anonymous Rate-Limited Credentials

ARC was built to solve the problems of the experimental rate-limited Privacy Pass issuance protocol built on blind RSA

Rate-limiting is a built-in feature

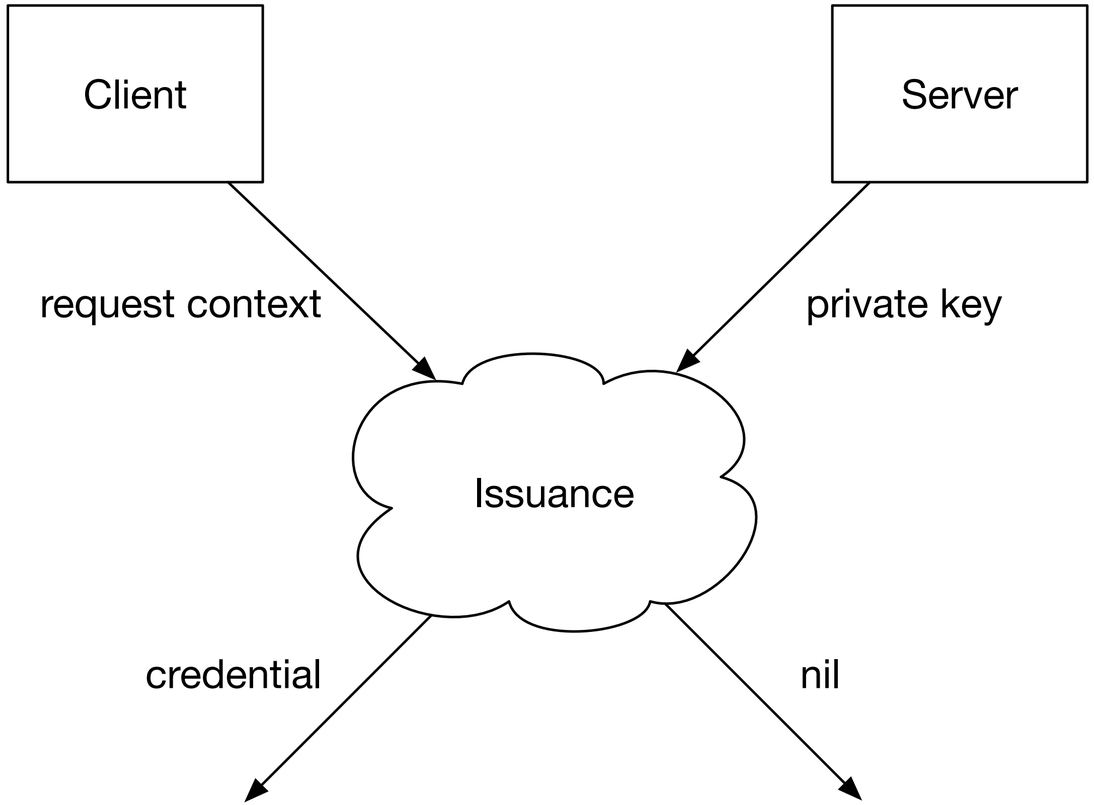
ARC solves the 1:1 token:issue cost problem by allowing tokens to be *derived* from a single credential (up to the rate limit)

ARC Overview



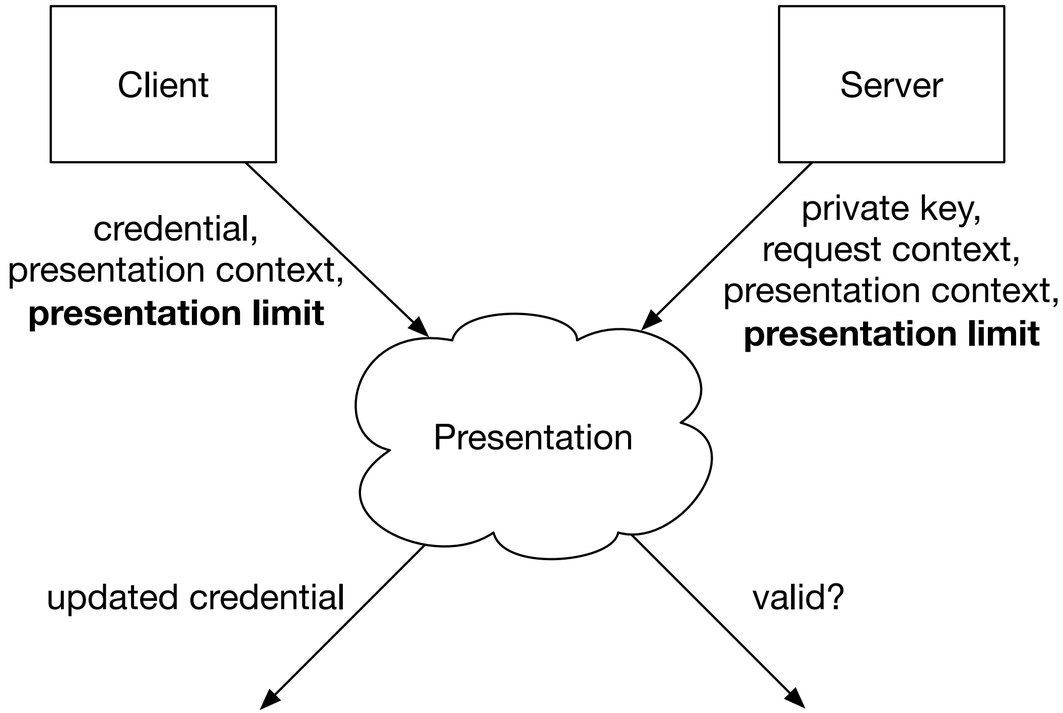
ARC Syntax

Issuance



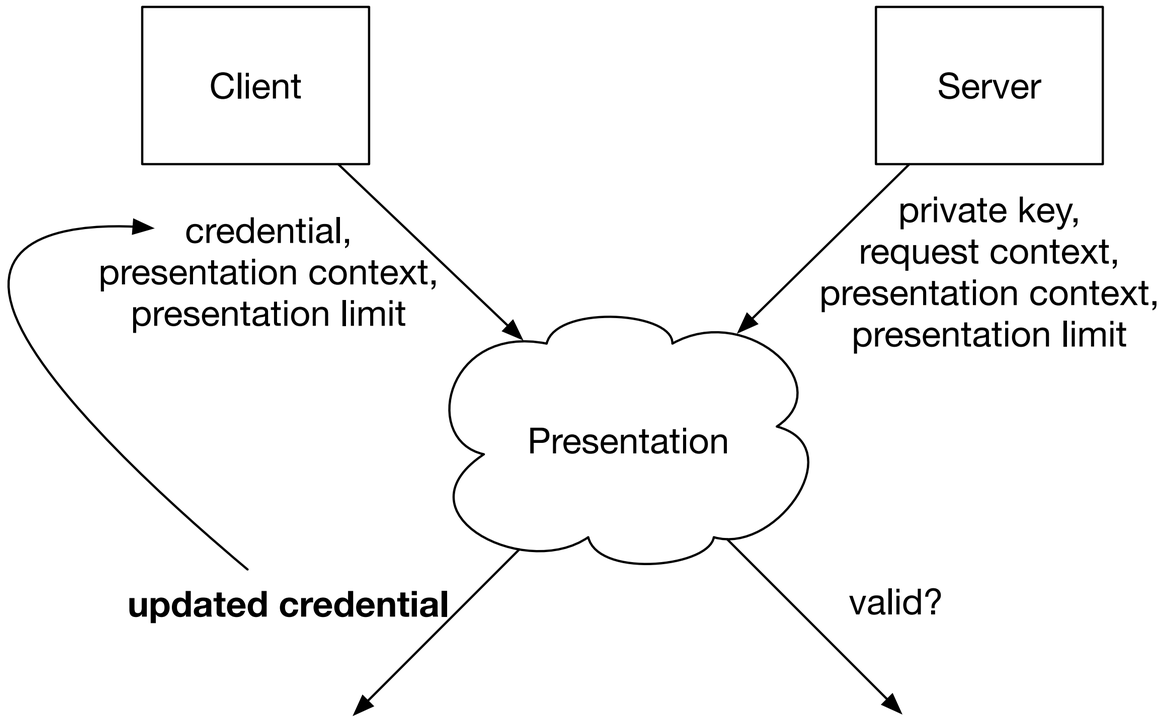
ARC Syntax

Presentation



ARC Syntax

Presentation



ARC Summary

ARC is the privately-verifiable variant of CFRG's blind BBS work, which currently only supports public verifiability (see draft-ladd-privacypass-bbs)

ARC allows multiple tokens to be produced from a single credential (skipping issuance), while rate limiting tokens produced from a single credential

ARC supports rate limiting, allowing us to deprecate and replace draft-ietf-privacypass-rate-limit-tokens

Interest in adoption?

Privacy Pass Issuance Protocol for Anonymous Rate-Limited Credentials

draft-yun-privacypass-arc

IETF 122 - Privacy Pass