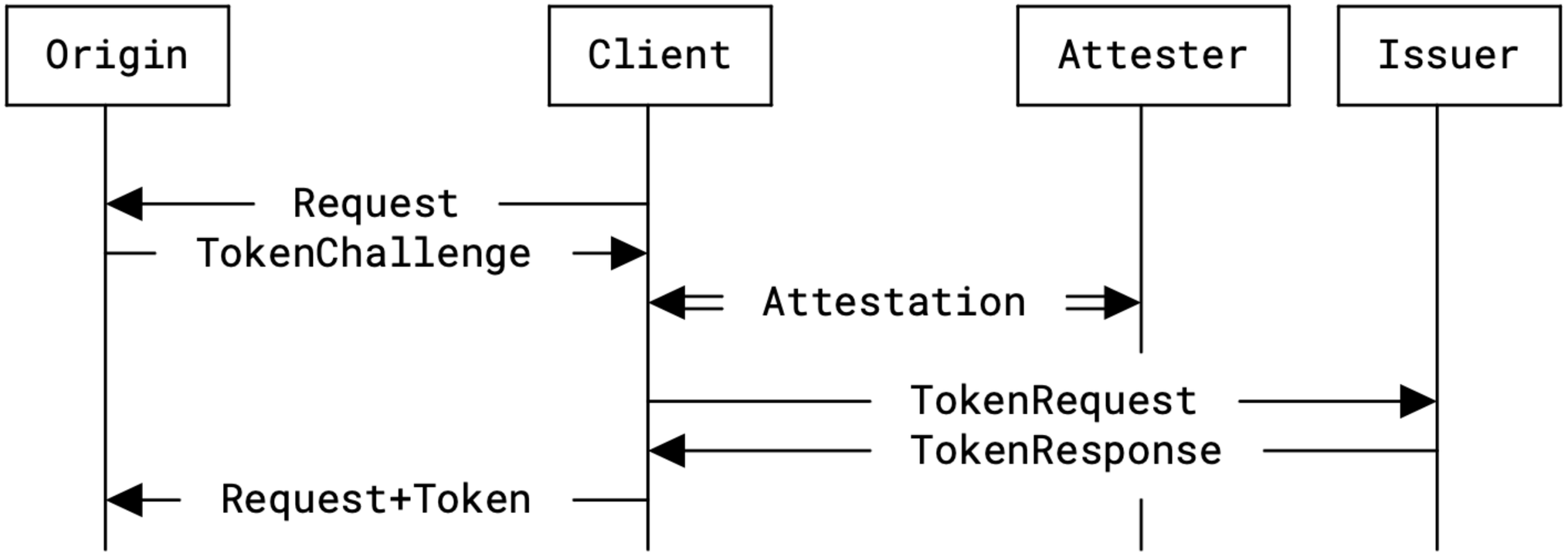
Anonymous Rate-Limited Credentials

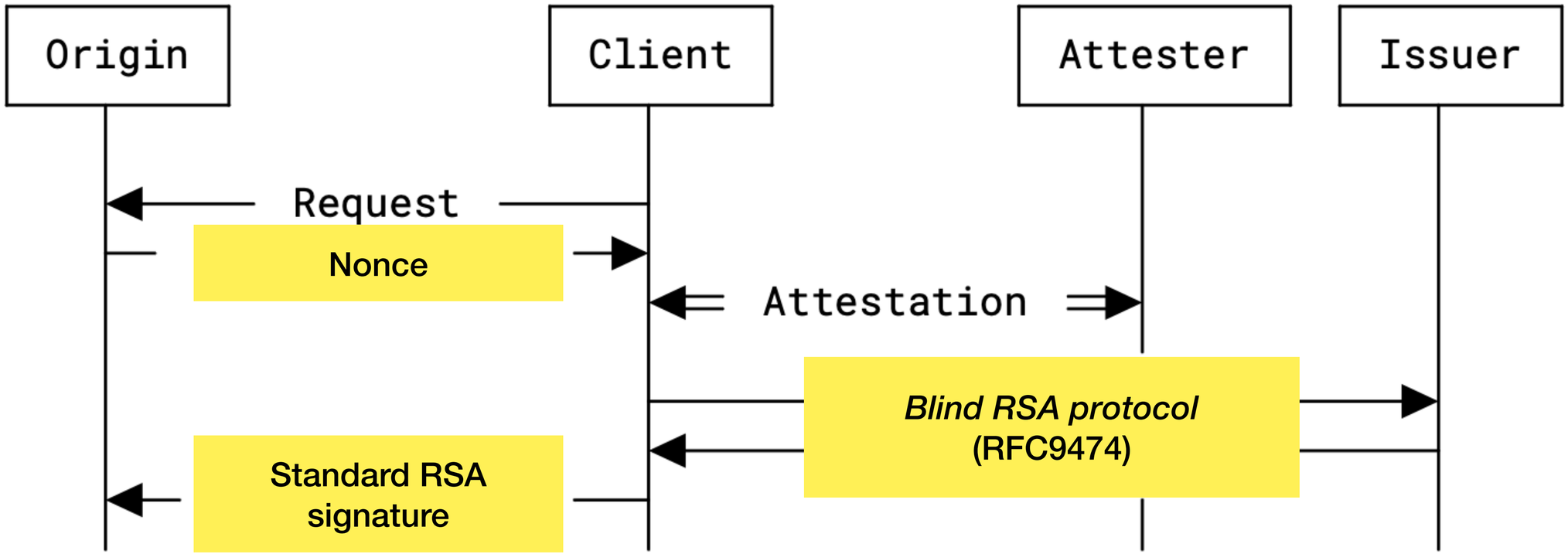
draft-yun-cfrg-arc

IETF 122 - CFRG

Privacy Pass (RFC9576)



Privacy Pass (RFC9576)



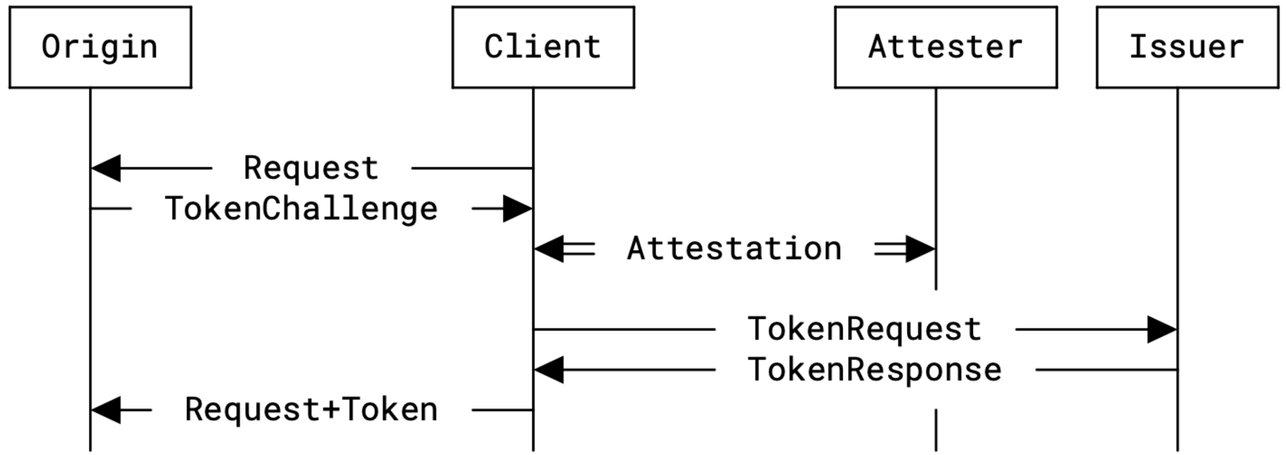
Privacy Pass (RFC9576)

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

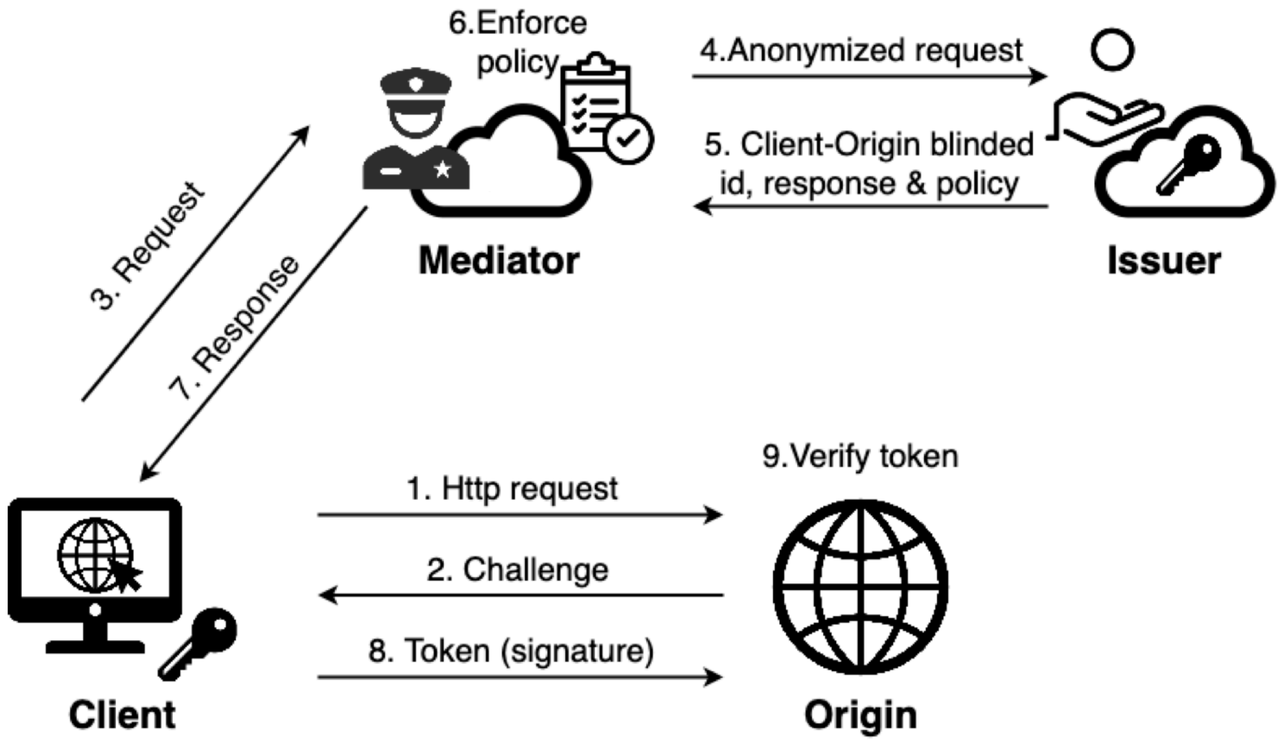
Client, Attester, and Issuer communicate for every single Token



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/

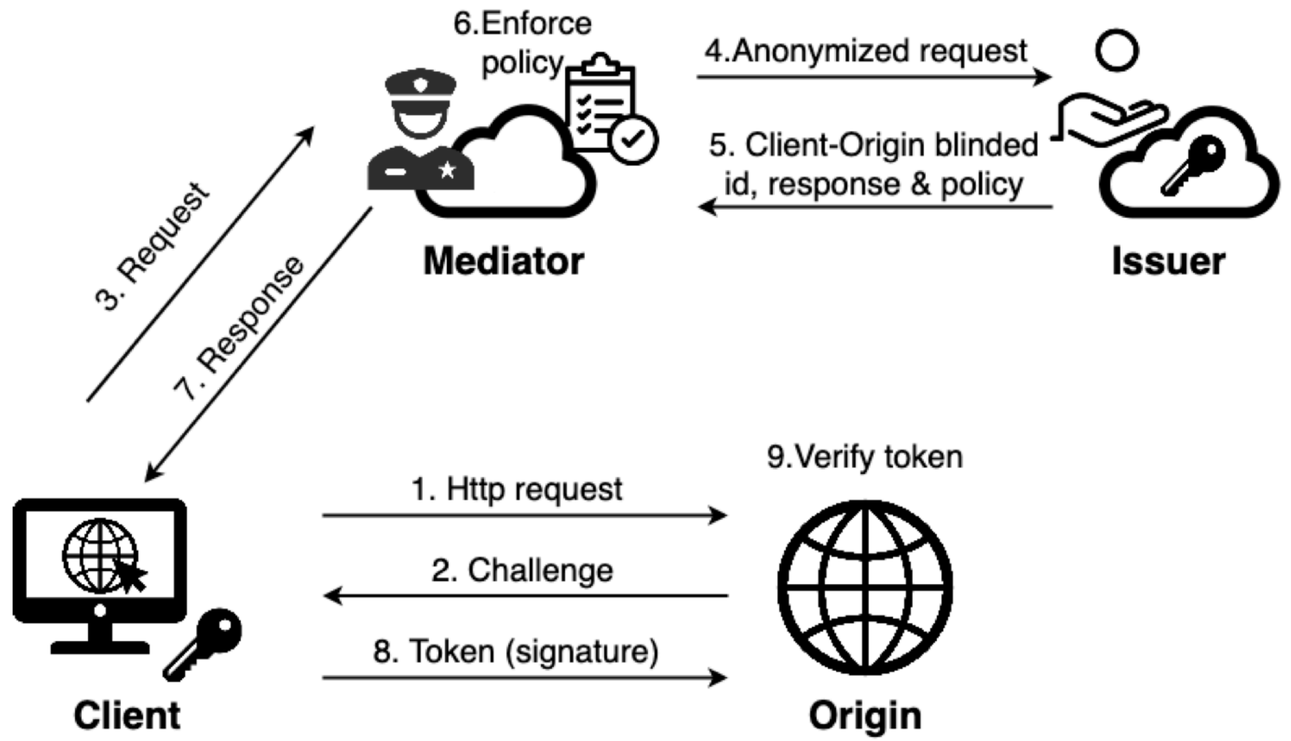
https://eprint.iacr.org/2023/1805.pdf

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

Anonymous Credentials

Anonymous credentials generally allow selective disclosure of attributes bound to a credential

Private metadata bits, pseudonyms, rate limiting, issuer-hiding

Various constructions exist: CMZ14, BBS04, etc

Publicly verifiable credentials use pairing-friendly curves, whereas privately verifiable credentials (keyed-verification) uses standard curves

ARC: Anonymous Rate-Limited Credentials

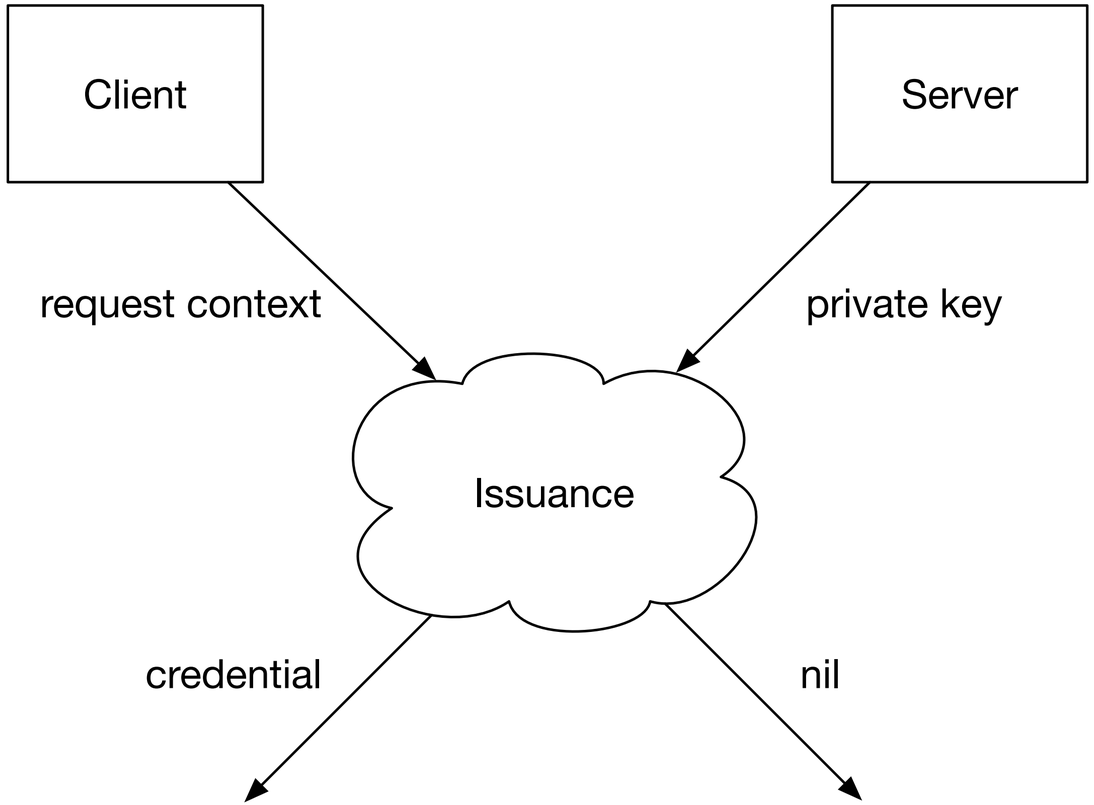
ARC was built to solve the problems of the experimental rate-limited Privacy Pass issuance protocol built on blind RSA

ARC is an opinionated instance of a keyed-verification anonymous credential built on CMZ

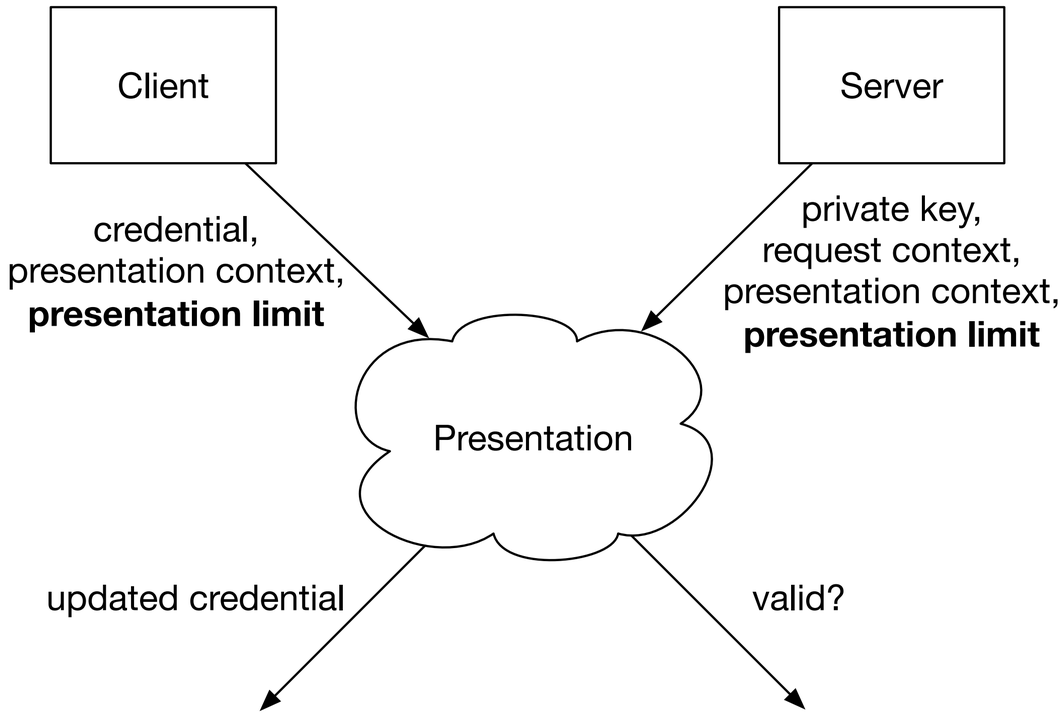
Rate-limiting is the primary (and only) attribute (or extension)

Generalizable to keyed-verification version of BBS

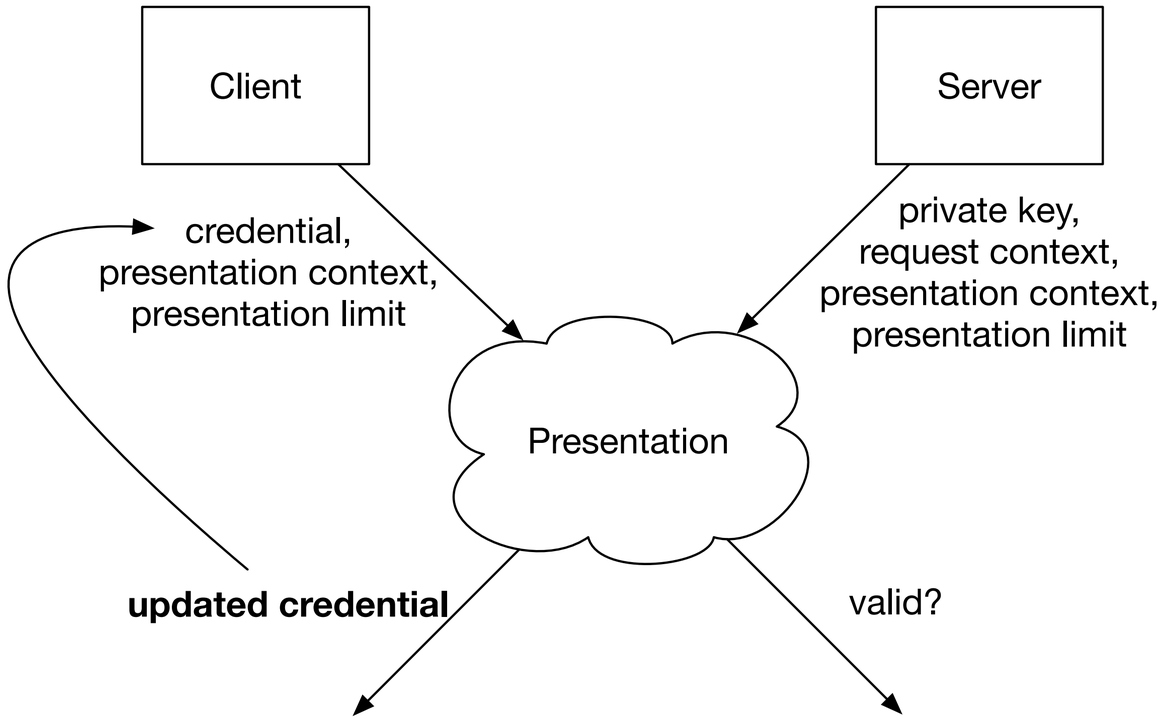
ARC Syntax - Issuance



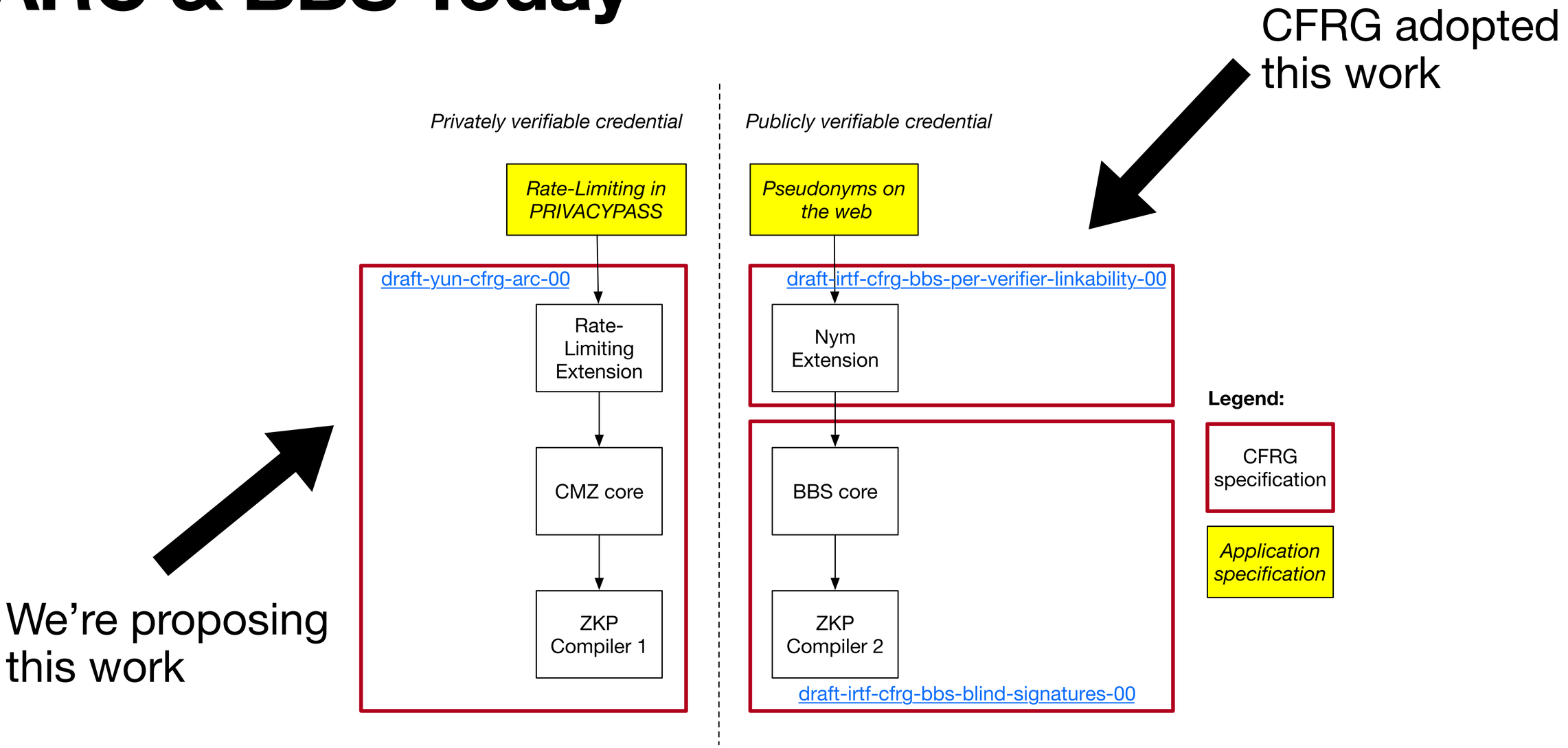
ARC Syntax - Presentation



ARC Syntax - Presentation



ARC & BBS Today



ARC Summarized

ARC is the privately-verifiable variant of CFRG's blind BBS work, which currently only supports public verifiability

ARC can be changed to use another ZKP compiler, another MAC, and even another extension mechanism

ARC satisfies a direct need for the Privacy Pass working group

Proposal

1. Produce a research document oriented around anonymous credentials (similar to research document on KEM combiners)

   Describe an architecture and framework for thinking about and using anonymous credentials in applications

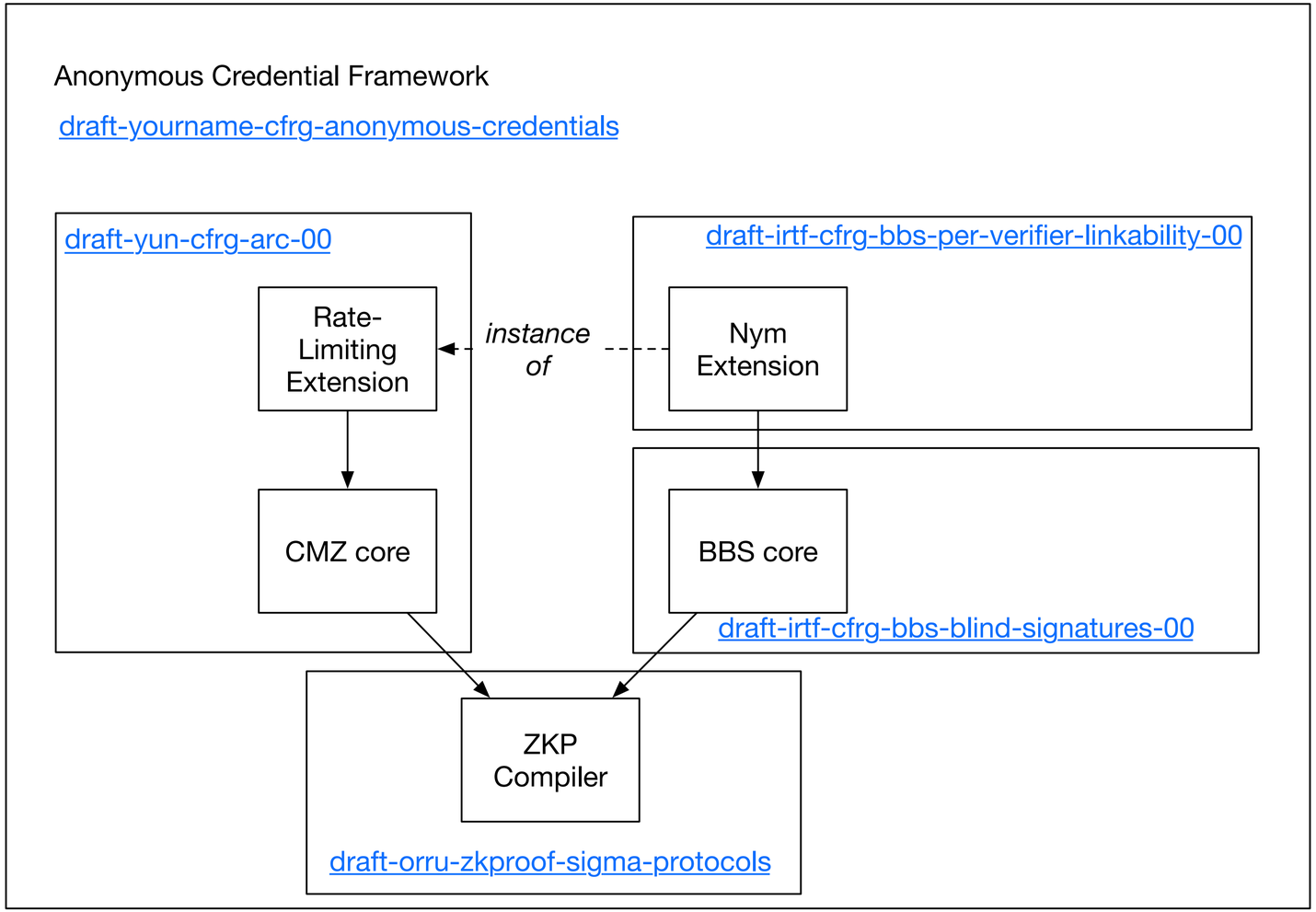
2. Produce concrete instances of anonymous credentials: BBS (publicly verifiable) and ARC (privately verifiable)

   Specify concrete anonymous credentials that can be implemented in an interoperable way

3. Factor out common pieces like the ZKP compiler to lower level specifications (similar to hash-to-curve)

   Specify essential pieces as a new interop and analysis target, simplifying the documents in (2)

A Happy Union



Questions?
Feedback on our proposal?

Anonymous Rate-Limited Credentials

draft-yun-cfrg-arc

IETF 122 - CFRG