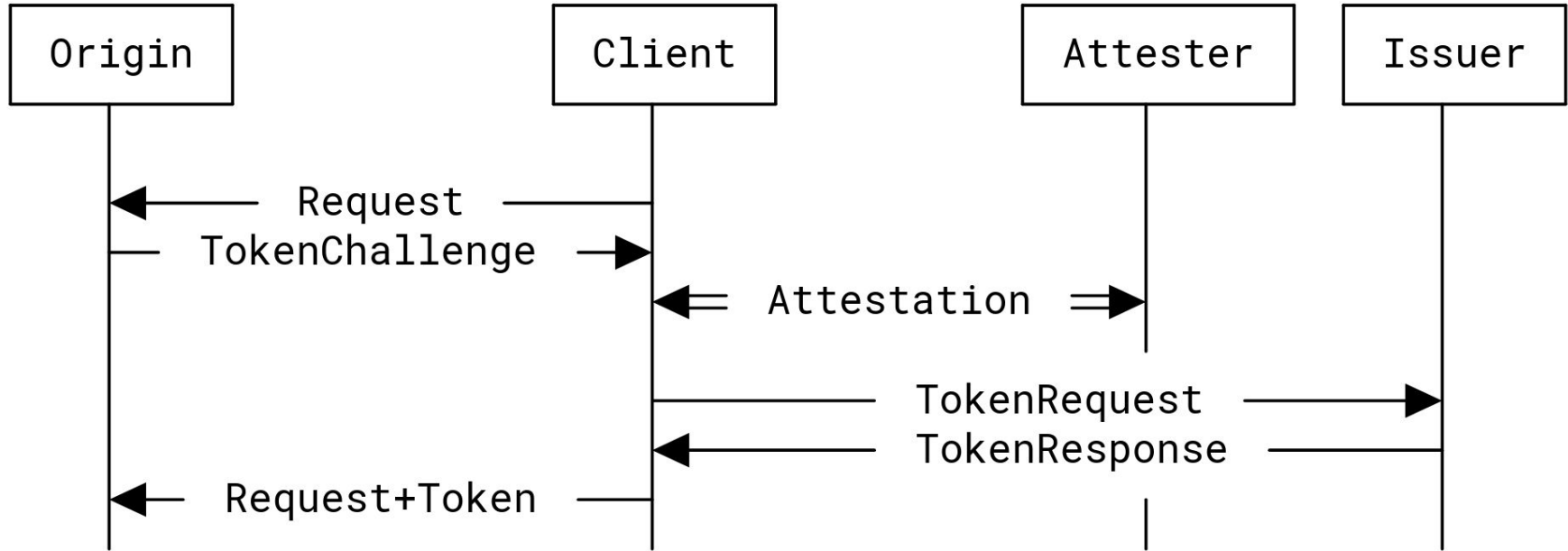


Composing tokens

Privacy Pass

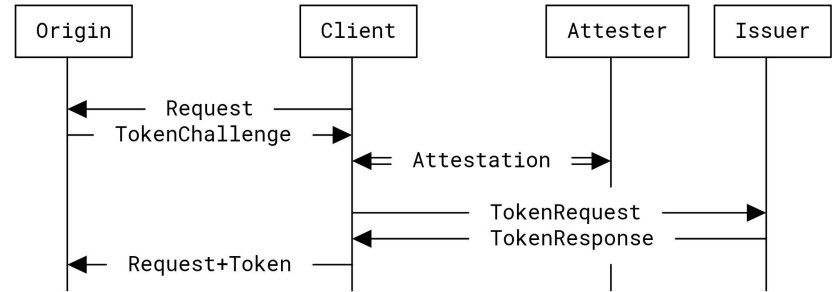
Lena Heimberger - Thibault Meunier (Cloudflare)
IETF 124, November 2025, Montreal

Privacy Pass Architecture - RFC 9576



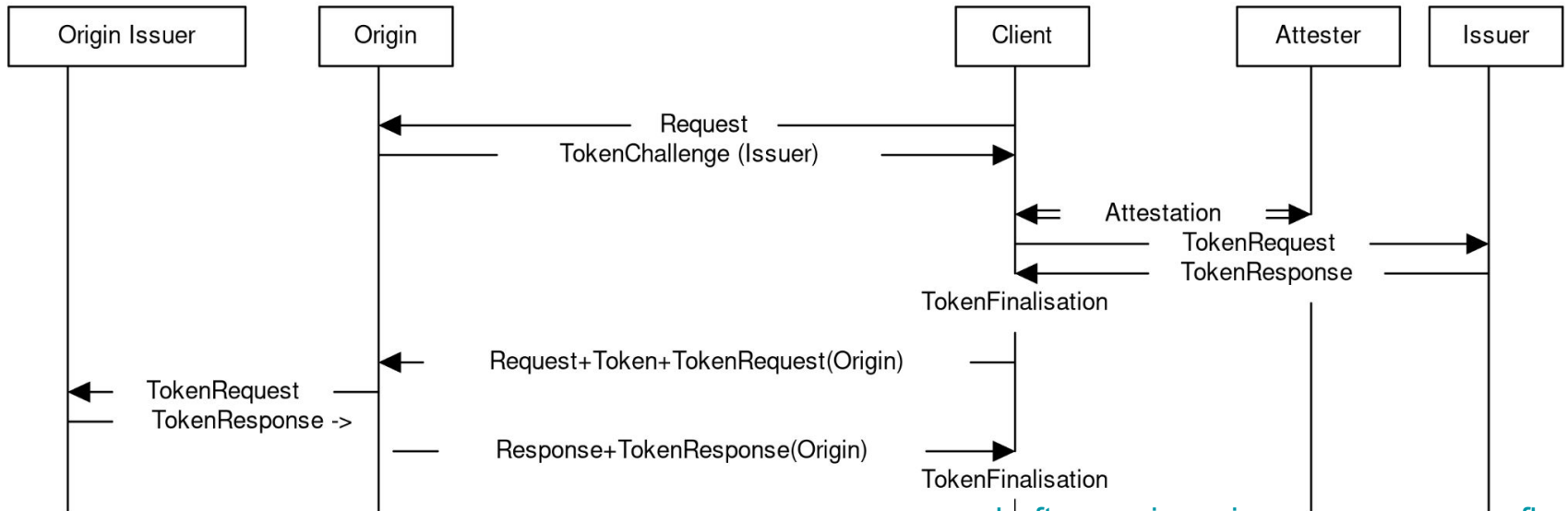
RFC 9576 - Limitations

1. Issuance communication: Number of redemption is proportional to the number of issuance
2. Late-binding: When the number of presentation is unknown, setting an upper limit can be inefficient and bound to the maximum user usage
3. Revocation: Once given, access cannot be revoked



Reverse Flow

The draft takes the same architecture, and deploys it twice



[draft-meunier-privacypass-reverse-flow-02](#)

New token types

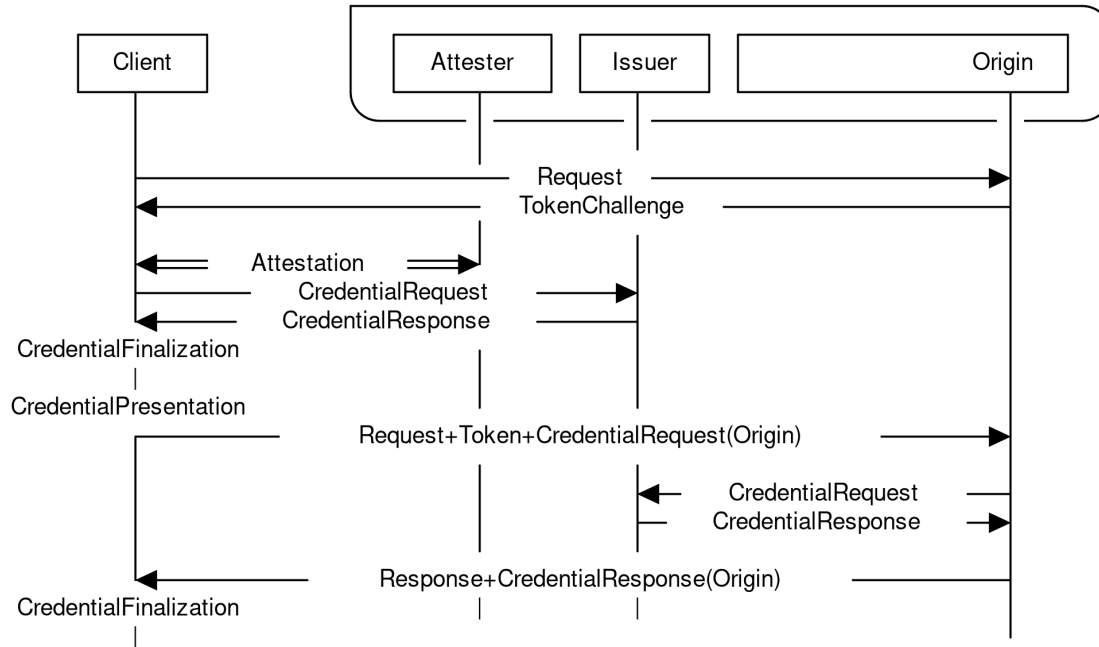
ARC

1. Great for parallel use
2. Sublinear communication, enables per-origin redemption (late-origin binding)
3. Cannot be revoked

ACT

1. Built-in revocation (refuse to re-issue)
2. Stateful policy (e.g. taxing suspicious requests)
3. Sequential redemption

For Anonymous Credentials - Joint deployment mode



ARC + ACT for Stateful, Per-Origin Revocation

Enable smarter revocation based on behavior patterns over time.

Issuance

1. Client is issued an ARC with a presentation limit of $N=1$.

ARC + ACT for Stateful, Per-Origin Revocation

Enable smarter revocation based on behavior patterns over time.

Issuance

1. Client is issued an ARC with a presentation limit of $N=1$.

First Presentation (Per Origin)

1. Client presents its $N=1$ ARC.
2. Server validates and issues an ACT credential with an initial state (e.g., credits = 100).

ARC + ACT for Stateful, Per-Origin Revocation

Enable smarter revocation based on behavior patterns over time.

Issuance

1. Client is issued an ARC with a presentation limit of $N=1$.

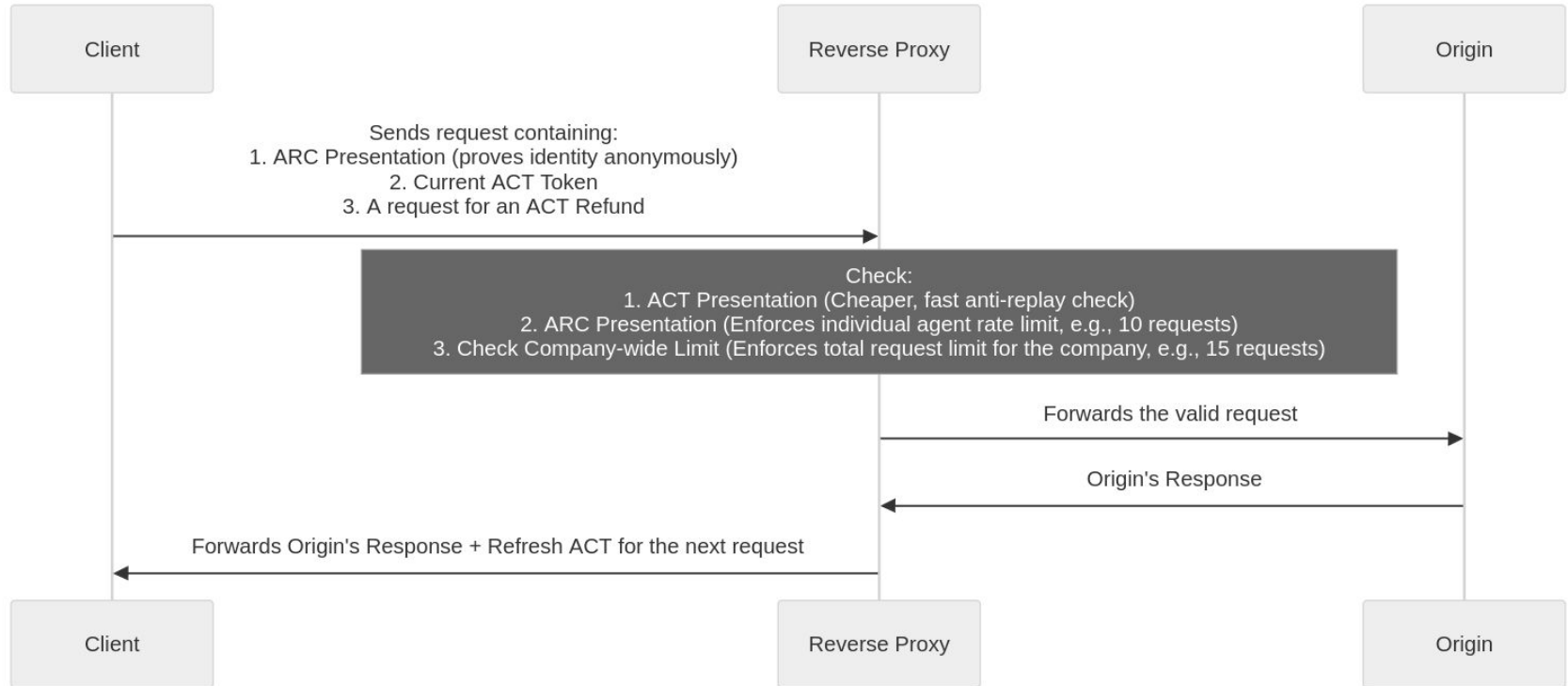
First Presentation (Per Origin)

1. Client presents its $N=1$ ARC.
2. Server validates and issues an ACT credential with an initial state (e.g., credits = 100).

Subsequent Presentations (Per Origin)

1. Client presents its ACT credential.
2. The origin has two choices:
 - a. Revoke (don't reissue)
 - b. Update (issue with a new state)

ARC+ACT combiner



Use Cases

1. WAF rate limit for websites
2. Media-over-QUIC stream budget
3. Antifraud
4. Rate limiting agents behind agentic origins

Discussion

Backup

Early measurements - BlindRSA, VOPRF

Blind RSA RFC9474 (RSA-2048+SHA384)		1 Token	
		Time	Message Size
Issuance	Client (Blind)	63 μ s	256 B
	Server (Evaluate)	2.69 ms	256 B
	Client (Finalize)	37 μ s	256 B
Redemption	Client	–	300 B
	Server	37 μ s	–

VOPRF RFC9497 (Ristretto255+SHA512)		1 Token		1000 Amortized issuances	
		Time	Message Size	Time (per token)	Message Size (per token)
Issuance	Client (Blind)	54 μ s	32 B	54 μ s	32 B
	Server (Evaluate)	260 μ s	96 B	99 μ s	32.064 B
	Client (Finalize)	376 μ s	64 B	173 μ s	64 B
Redemption	Client	–	96 B	–	
	Server	57 μ s	–		

Early measurements - ARC/ACT

Issuance Credential Generation	ARC		ACT	
	Time	Message Size	Time	Message Size
Client (Request)	323 μ s	224 B	64 μ s	141 B
Server (Response)	1349 μ s	448 B	251 μ s	176 B
Client (Finalize)	1293 μ s	128 B	204 μ s	176 B
Redemption Credential Presentation	ARC		ACT	
	Time	Message Size	Time	Message Size
Client (Present)	735 μ s	288 B	1740 μ s	1867 B
Server (Verify/Refund)	740 μ s	–	1785 μ s	141 B
Client (Update)	–	–	508 μ s	176 B