Rate-Limited Token Issuance Protocol

draft-ietf-privacypass-rate-limit-tokens-06

Tommy Pauly, Chris Wood, Steven Valdez,
Scott Hendrickson, Jana Iyengar
Privacy Pass
IETF 120, July 2024, Vancouver

WGLC Feedback

There probably are better and simpler cryptographic options for achieving per-origin rate limiting

Questions around experimental status — what is the experiment?

Needs some clarifications around the roles and which party is doing what

WGLC Feedback

There probably are better and simpler cryptographic options for achieving per-origin rate limiting

> *Agreed — as one comment points out, this is a "pragmatic" approach using more available and widely understood crypto, but it gets complex to put together.*

Questions around experimental status — what is the experiment?

Needs some clarifications around the roles and which party is doing what

Ways forward

a) Fix up issues for clarity, and move to another WGLC

   i) Experimental and justify the experiment 👨‍🔬

   ii) Proposed standard ➡️

b) Put document on hold and replace crypto with another variant when that's ready ✋

c) Abandon the document 😢

Issuer → Attester Communication

Separately from the per-origin rate limiting, the mechanism in Section 5.5 that defines how Issuers communicate rate-limiting policies to Attesters is very useful

- Useful for normal type 1 and 2 tokens
- Allows an issuer to express a dynamic rate limit (across all clients, but for a particular time period) for how many tokens should be issued

Might be good to pull this part out into a separate document regardless of other decisions