Rate-Limited Token Issuance Protocol

draft-ietf-privacypass-rate-limit-tokens-03

Tommy Pauly, Chris Wood, Steven Valdez,
Scott Hendrickson, Jana Iyengar

Privacy Pass
IETF 118, November 2023, Prague

Change in -03

Align with consistency documents

- Refer to draft-group-privacypass-consistency-mirror
- Works well for Issuer-wide encapsulation key
- Trickier for per-Origin token keys...

Per-origin key consistency

Add per-Origin token keys to the defined config

- Previously, the way the Issuer sent keys to Origins was undefined

- Allows checking by mirrors

- Downside is making the configuration enumerate origins

An alternate approach would be to have the mirror check something against the origin

Thoughts?

Open issue: more flexible rate-limiting contexts

Issue #18

Currently, the rate-limited context is an Origin name (a hostname)

- Works pretty well for many cases, like websites or services on unique hosts

Theoretically could be broadened to include URL paths, etc

- Separate limits for `/foo` and `/bar`
- Useful for mitigating Sybil attacks on DAP (PPM), etc.