Rate-Limited Issuance

draft-ietf-privacypass-rate-limit-tokens-01

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

Recent Changes

- Penalization of Issuers and Clients
  - Attesters that detect collisions in buckets will "penalize" Issuers or Clients and stop trusting them if they have a pattern of collisions
- Include Issuer Name in Anonymous Origin ID calculation
  - Client secret is per-Origin as well as per-Issuer
- Explain selection of first-party origin name
  - If multiple names are in the challenge, client can pick
  - Clients SHOULD use first-party webpage context when applicable

Rate limits are per attester

Issue #9

Rate-limited state is stored on attesters

- Thus, the rate-limit is per attester

Specific issuer instances should choose a set of attesters that are mutually exclusive

- I.e., use a set of all device-based attesters for one issuer name, and use a set of email-account-based attesters for the other

Improve Anonymous Origin ID terminology

Issue #13

"Anonymous Origin ID" and "Anonymous Issuer Origin ID" are confusing!

Anonymous Origin ID:

> "The ID the client came up with for the origin+issuer"

Anonymous Issuer Origin ID:

> "The ID the issuer derived for the origin+issuer+client"

Are there better terms for these concepts?

Key consistency strategy

Issue #14

We should reference the key consistency document, and suggest approaches to apply

We need consistency for the Issuer configuration:

- Issuer encapsulation key
  - One per Issuer, seen by Origin / Client / Attester
- Token key
  - One per Origin+Issuer, seen by Origin / Client

Next Steps

Revise document for issues

Tracking CFRG dependency (draft-irtf-cfrg-signature-key-blinding)

- Analysis has been done, requesting to advance in CFRG

Questions?