Privacy Pass and W3C

IETF 115 - 2022-11

Steven Valdez - svaldez@google.com

Relevant Work

- Private Access Tokens
- Private State Tokens (fka Trust Tokens)
- Device Attestation
- Other Uses?

Private Access Tokens

- Recent version of type 2 (Blind RSA) and rate-limited tokens (undergoing adoption).
- Minimal deltas from privacypass protocol
- fetch API changes to standardize how to hook into fetching resources/interpreting responses containing PAT operations.
- Some sort of policy to delegate use of the API
- Potentially in WICG (Web Incubation CG) or Antifraud CG

Aside: W3C Groups

- Interest Groups - Place for exchange of ideas.
- Community Groups / Business Groups - Place for discussions/development.
  - WICG (Web Platform Incubation Community Group) - Lightweight place to discuss new features.
- Working Groups - Place for standardization process and specific deliverables
- TAG (Technical Architecture Group) - Group for architecture/principles on the web.
- AB (Advisory Board) - Guidance on legal/policy/conflict resolution

Private Access Tokens

- Token issuance is via a trusted attester (platform).
- Each origin is able to redeem tokens (primarily bound to that origin) and picks specific issuers they work with.
- Rate Limiting by the Issuer to N tokens per origin.

Private State Tokens

- Earlier version of type 1 (VOPRF) and type ? (PMBTokens) from earlier privacypass revision
  - Planned to update to RFC version.
  - TBD about getting PMBTokens in an IETF draft for CFRG review
- Currently in WICG (Incubation Community Group)
  - Interest in migrating to the Antifraud CG

Private State Tokens

- Token issuance is via various first-party and third-party sites (eg Antifraud SaaS/CAPTCHA).
- Each origin is able to redeem tokens from particular issuers (limited to small number).
- On redemption, a redemption record is stored locally (sharded by top-level origin to avoid cross-site tracking) to avoid needing to spend a token for every request from that origin.

Private State Tokens Deltas

- "Database Discovery" model for getting key commitments.
  - draft-ietf-privacypass-key-consistency may be a good way to standardize on a method.
- Protocol via additional headers vs application/private-token-request POSTs
  - Updates to RFC version could adopt the POST method*
    - There are some potential use cases where having the protocol be its own request rather than attached to an existing request could have complexity issues.
- Triggered via JS fetch parameters rather than HTTP-Authentication
  - JS Fetch defined as a W3C spec.
  - Add support for HTTP Authentication triggered issuance/redemption to PST.
- Redemption Records - Cached redemption results per top-level.
  - Avoids needing to send token to non-issuance endpoint (mitigate token hoarding)
  - Improved latency for repeated requests on same site.

(Device) Attestation

- Antifraud CG looking into providing attestations about client to websites
- Device Attestation - Attesting to the device/client.
- … Attestation - Other potential client-based attestations.
- Looking for an anonymous credential-style system
  - Unlinkable
  - Verifiable
- Certain types of privacypass may be useful.

Other Uses?

- PATCG
  - Aggregate Reporting API
- Privacy CG
- Webauthn/Web Payments
  - Tokens issued by banks/instrument providers