Privacy Pass and W3C

IETF 117 - PRIVACYPASS - 2023-07

Steven Valdez - svaldez@google.com

Agenda

- Private State Tokens
- W3C Groups

Private State Tokens

- Explainer/Spec: https://github.com/WICG/trust-token-api
- Web API for use on different websites.
- Some origins register as “Issuers” (effectively a joint privacypass Attester/Issuer).
- On the Issuer first-parties and places they are embedded as third-parties, they can issue tokens based on first/third-party information.
- On other sites, the Issuers can redeem tokens.
- Primary use is for Antifraud/IVT (Invalid Traffic Detection)
  - CAPTCHAs
  - Embedded Botted Traffic Detection
  - …

Private State Tokens (Versioning)

- Formerly known as Trust Tokens
- Ran an Origin Trial through May 2022.
  - Limited experimental results as many IVT/AF solutions are reliant on consistent access to features.
- Launched PSTV1 in Chrome 114 in May
  - Currently ramping up to 100% Stable.
- Plans for a backwards-compatible “vStandard” version that aligns closer to existing specs
  - privacypass
  - Better structured header compatibility

PST: Existing extensions to privacypass

- Consistent way of fetching keys from the various issuers and caching the results.
  - draft-group-privacypass-k-check
- Due to latency, batched token issuance is critical.
  - draft-robert-privacypass-batched-tokens
- Public Metadata in tokens
  - Currently performed by choice of keys.
  - draft-hendrickson-privacypass-public-metadata-issuance

PST: Deltas from privacypass (Protocol/Deployment)

- Method of distributing consistent keys to clients
  - Optimization to avoid unnecessary fetches.
  - Chrome: PST currently has a component updater to distribute fetched keys.
  - Generic: Having some sort of bulk/batch distribution from a k-check style server may be useful. Use of headers for operations rather than separate requests
- Key Commitment Format
  - Expiry to allow for differing expirations between different keys.
    - privacypass Cache-Control only allows global expiry for the entire commitment.
  - Use of .well-known vs configured endpoint
    - PST requires “registering” an issuer, allowing for multiple issuers to use the same infrastructure for serving keys.

PST: Differences from privacypass (Web)

- PST attaches the payloads for PST operations (issuance/redemption) in Sec-Private-State-Token headers.
  - Generally AF/IVT collects additional information to use as part of making the issuance.
  - Using the existing application/private-token-request headers would either require request matching different requests together on the server-side or embedding the additional data as additional headers.
- PST operations are initiated by client code (fetch, XHR, iframe attributes)
  - Generally web-based issuers are making decisions as part of an interaction with a web page instead of as part of a resource load.
- Addition of a redemption record for web redemptions
  - Returned from a redemption of a token and cached on the client-side.
  - Cookie/Local Storage equivalent, can be replaced by client code to take the redemption response and store it in local storage

PST: Open issues to align with privacypass

- These are changes PST will need to make for vStandard to align.
- Token type is different from privacypass.
- Key Commitment Format
  - protocol_version -> Token-Type
- Potentially support the auth-scheme/WWW-Authenticate API in addition to the client code.

W3C Groups

- Anti Fraud CG
  - Thinking about problems with coming up with verdicts about potential bad traffic in privacy-preserving ways.
- PATCG
  - Advertising ecosystem APIs that needs some form of privacy preserving authentication.
- Privacy CG
  - General privacy APIs
- Webauthn/Web Payments
  - Attesting to properties of users without full identification.