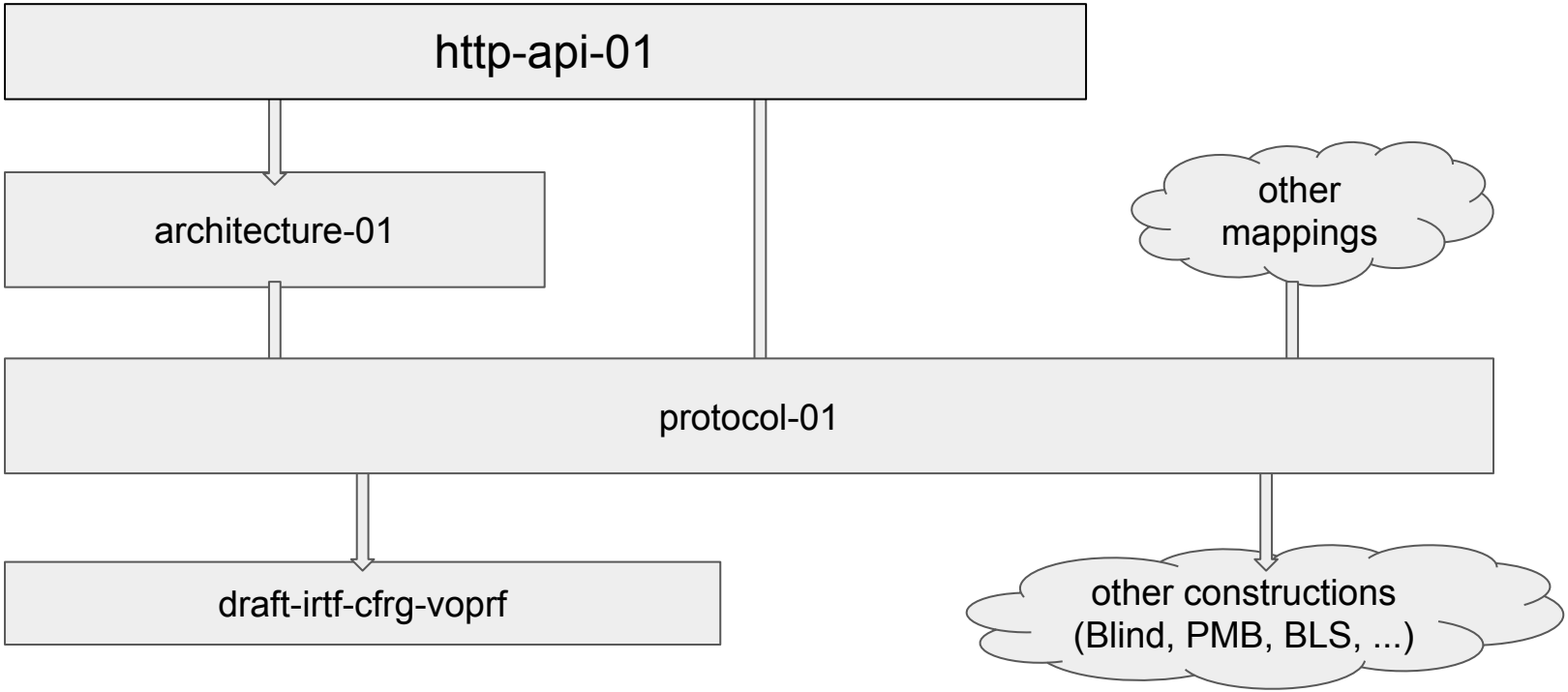
Privacy Pass Updates

IETF 111 – Virtual – 2021-07

Steven Valdez - svaldez@google.com

Privacy Pass Landscape



Closed Issues

- #66 Add Redemption Contexts
  - Follow-up from IETF 110 discussion
- #68 RFC8446 Vector Syntax
  - Update to match correct TLS syntax

Protocol Open Issues

- #67 Refactor redemption flow
  - Sync RedemptionRequest with VOPRF inputs/outputs, simplify exposed fields.

Architecture Open Issues

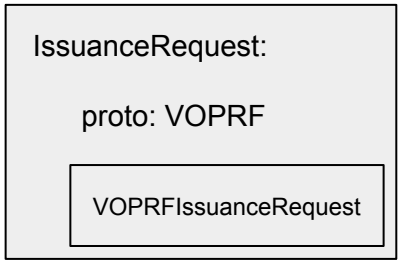
- #2 Identifying Malicious Servers
- #44 Redemption Mode in Public Config
  - Mechanism for exposing additional server config options in commitments.
- #45 Centralization Documentation
  - https://datatracker.ietf.org/doc/html/draft-mcfadden-pp-centralization-problem-00
  - Additional documentation in WG?
- #46 Exposure of token in proxied-verifier
- #65 Update privacy calculations
  - Sync privacy calculations as additional protocol/architecture changes are made.

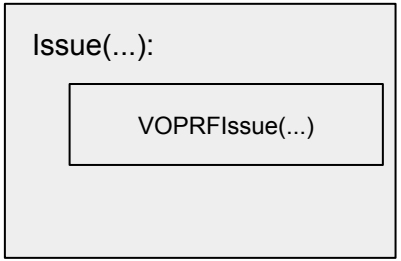
Supporting Other Constructions

- #40 Public Verifiability
  - Tokens that can be verified without the issuer’s keys.
- #42 Private Metadata Bit Variants
- #63 Client and Server Metadata
  - Supporting Metadata, followup presentation
- #77 Pin protocol messages to crypto scheme
  - Next slide.

Supporting Other Constructions (PR #79)

- Additional Abstraction Level
- Treat messages as arbitrary blobs.
- Each construction defines internal structures.
- New Constructions
  - Add a new codepoint
  - Define protocol structures (wire format)
  - Define internal construction-specific issue/redeem.





Charter Timeline

- Specification of protocol & surrounding architecture - February 2021.
- Risk assessment for centralization in Privacy Pass deployments for multiple design options - February 2021
- Specification of application-layer requirements (including HTTP integration) - June 2021.
- Specification of HTTP browser API (in coordination with W3C) - October 2021.

Potential Updated Charter Timeline

- Core protocol (with VOPRF construction) draft - November 2021
  - Updates for abstractions/metadata.
- Architecture draft - March 2022
  - Updates for deployment Issues/Centralization/metadata.
- Specification of application-layer requirements (including HTTP integration) - April 2022
  - Updates to new core protocol changes, architecture deployment changes.
- HTTP browser API (in coordination with W3C) - 2022
- Additional Constructions - ???
  - Based on WG on which constructions to focus on (public verifiability/metadata-supporting/etc)

Open Questions

- Refactor documents to abstract protocol for additional constructions?
- Updated Charter timelines?
- Metadata support in the draft? (following presentation)