Privacy Pass

draft-ietf-privacypass-architecture
draft-ietf-privacypass-auth-scheme
draft-ietf-privacypass-protocol
Privacy Pass
Recent changes

**Architecture**
- Trust model clarifications
- Remove parameterization
- Discuss centralization considerations

**Auth scheme**
- Support multiple origin names
- TokenChallenge guidance
- Clarify double spend requirements
- Add test vectors

**Basic issuance**
- Fully specify token verification
- Advertise token validation keys in configurations
Token Type Registry
Issue #143

Auth Scheme defines a registry of token types
Basic issuance defines types 1 (private verification) and 2 (public verification)
Some types reserved for greasing

IANA questions:
Where does this go? New "Privacy Pass Parameters" page
What review policy? Specification Required
Attestation Compromise
Issue #141

What happens when attestation seems to stop working?
Attestation Compromise
Issue #141

This should be an exceptional event for carefully chosen attesters

Solution is likely deployment specific

  Maybe issuer detects lots of origins complaining about attestation failures?
  Maybe origin can present proof of attestation failure?

  ... something else?

Solution: add text describing these considerations
Questions?
WGLC?