Privacy Pass at the IETF

Chairs: Ben Schwartz, Joe Salowey
For the Anonymous Credentials Meeting @ Real World Crypto 2021

A brief history of Privacy Pass

- 2015-6: Increasing CAPTCHA load for Tor users on Cloudflare sites
  - Conflict: The Trouble with Tor vs. The Trouble with Cloudflare
- 2016-7: Cloudflare et. al. propose a solution using Blind RSA
  - Called the “Challenge Bypass Protocol”
- 2017-8: Switched to Elliptic Curve VOPRF, implemented as Privacy Pass 1.0
  - 2019: Version 2.0 added key commitment verification, preventing tiny anonymity sets
- 2019: Chrome announces Privacy Sandbox, pitches “Trust Token” at WICG
  - Trust Token is a standardized web integration around the Privacy Pass crypto
- 2020: WICG adopts Trust Token, Chrome deploys an origin trial
  - Added a Trust Token variant based on PMBTokens instead of VOPRF
- 2019-20: IETF 106 (secdispatch), 107 (BoF), 108 (first session)

IETF Privacy Pass Charter Highlights

1. ... specify an extensible protocol for creating and redeeming anonymous and transferrable tokens
2. ... describe and develop protocol use cases and properties thereof [e.g.]
    a. ... use cases and interfaces ...
    b. ... privacy goals ...
    c. ... recommended parameterization(s) ... that control the size of the anonymity set ..
    d. ... prevent Issuers from ... deanonymiz[ing] clients.
    e. ... including small amounts of metadata with Issued tokens [and] associated impacts on privacy.
    f. Describing the risk and possible ramifications of Issuer centralization, and exploring possible mechanisms to mitigate these risks.
3. ... specify a HTTP-layer API for the protocol.

Current Working Group Status

- Drafts from Privacy Pass and Trust Token authors are now adopted
- Please come join us! We need more input on
  - How to model client linkability (e.g. imperfect IP privacy)
  - Cryptographic considerations
  - Implementation reports
  - New use cases
  - The tradeoffs between metadata inclusion, anonymity set size, Issuer consolidation pressure, and public key commitment approaches
  - Emergent properties of the resulting ecosystems