draft-ladd-privacypass-bbs-01

Public metadata and redaction
(with other authors Chris Wood, Vasilis Kalos, Tobias Looker)

Problem

- Privacy Pass used to encode a single bit about the user
- Close coordination between issuer and verifier about what this meant
- Public metadata changes this

Inescapable tradeoffs

- Too many bits encoded => privacy impact
- Too few => origins don’t get what they need
- Open system => origins want different data from each other

A Solution

- Issuer gives anonymous credential (CL04, BBS04)
- User Agent transforms to reveal what origin needs
- Issuer can issue on all attributes
- User Agent can enforce privacy

Challenges

- We need a way to achieve the rate limiting properties
  - Link with blind RSA somehow?
  - Clever crypto?
  - BBS/GS based?
  - Do we even need to link?
- Origins need to advertise what they want to know
- Can selectively remove unlinkability origin side to rate limit[1], but this doesn't fit some applications

[1] e.g., with pseudonyms: https://basileioskal.github.io/bbs-per-verifier-id/draft-vasilis-bbs-per-verifier-linkability.html

Alternatives

- Cut and choose SD-JWT style (but has some problems with penalties and bandwidth)
- Other malleable signature schemes
- Blind signing makes obvious solutions hard

Questions for the WG

- Is this a problem that needs solving?
- Is this a viable way to solve it?
- Should we adopt this draft?