Privacy Pass: feedback from use cases

Sofía Celi
sceli@clouflare.com
Cloudflare
IETF110

Context

- Anonymous Credentials meeting held on January along with Real World Crypto 2021.
- Big number of participation, but many questions got not-answered as there was no so much time for discussion.
- Presentations from: the Tor project, Google, Facebook, hCaptcha, Brave, IETF WG.

The points

- Public/private metadata: currently addressed by several ideas
- Hoarding attacks seem to be a problem in practice:
  - There is not much mention of this in the documents.
- Accessibility concerns: how can they be addressed?
- Practical considerations:
  - Problems with the double-spending storage mechanisms.
    - Is there much token re-use?
    - What if the double-spending storage gets down?
    - How to maintain it on a distributed architecture?
  - What is an ideal key rotation policy?
  - Do we have reliable measurements to see what/when attacks happen in practice?

Path forward

- Section around practical considerations
- Section around accessibility: is there an ideal way to address it?
- More meetings to know what the community is implementing and currently facing:
  - Feedback on what problems are they facing when implementing
  - Feedback on what attacks they see in practice
  - Feedback on what novel applications are there

Thank you!

Notes from the meeting:
https://www.sofiaceli.com/Anonymous-Credentials-Meeting/meeting-2020