Alex Davidson

coela@alxdavids.xyz

@alxdavids

Privacy Pass

Problem statement and use-cases

https://datatracker.ietf.org/wg/privacypass/about/

https://privacypass.github.io

Intro

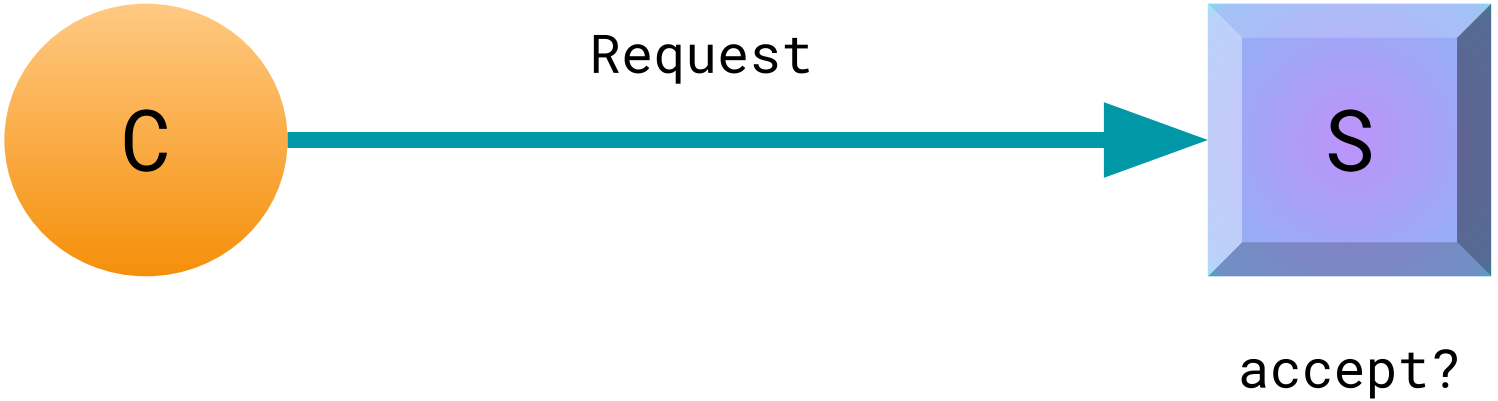
Privacy Pass is a privacy-preserving protocol for providing proofs of trust attestation

First announced in November 2017

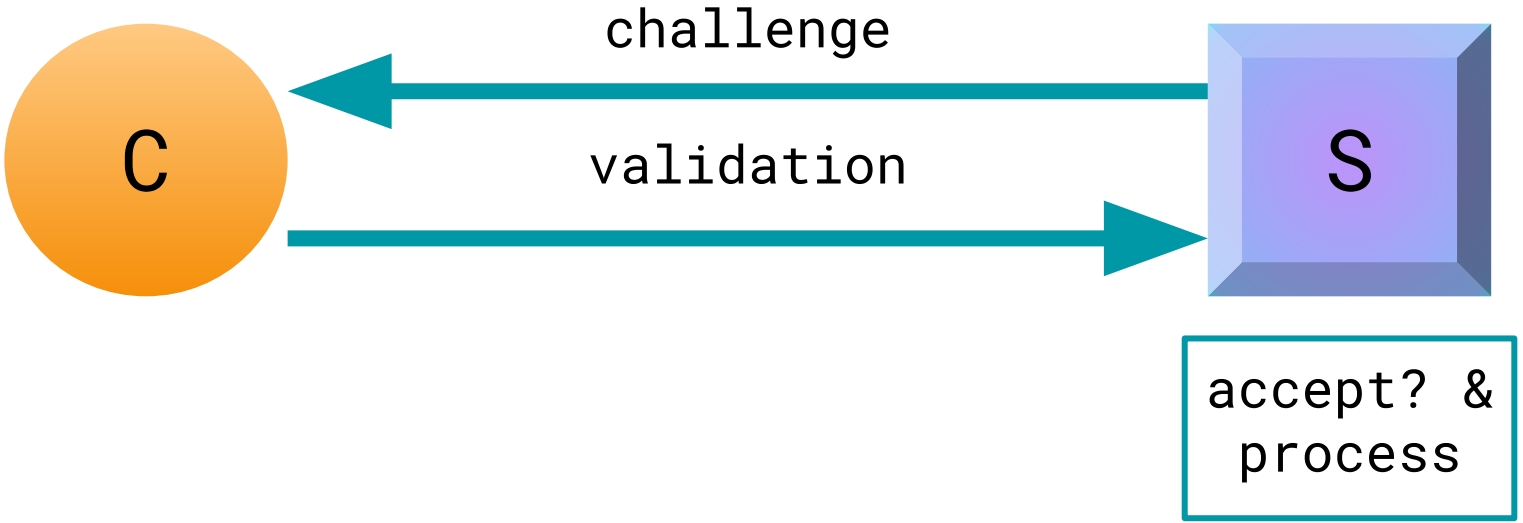
Actively used and developed by:

- Cloudflare, Chromium, Brave, Least Authority, hCaptcha, ...

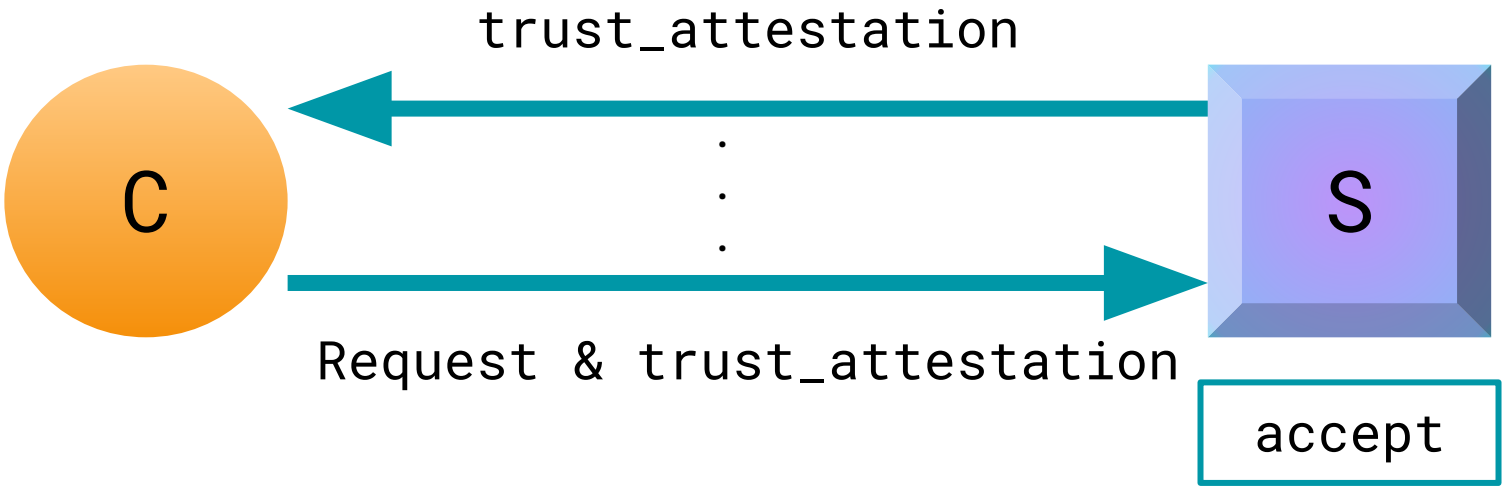
Trust



Trust



Problem: Trust propagation



Concerns

Usage of trust_attestation (e.g. as a cookie):

- limited functionality (cross-origin)
- mapping of client browsing patterns

Lack of alternatives beyond solving a challenge on each request (impractical/infeasible)

Privacy Pass

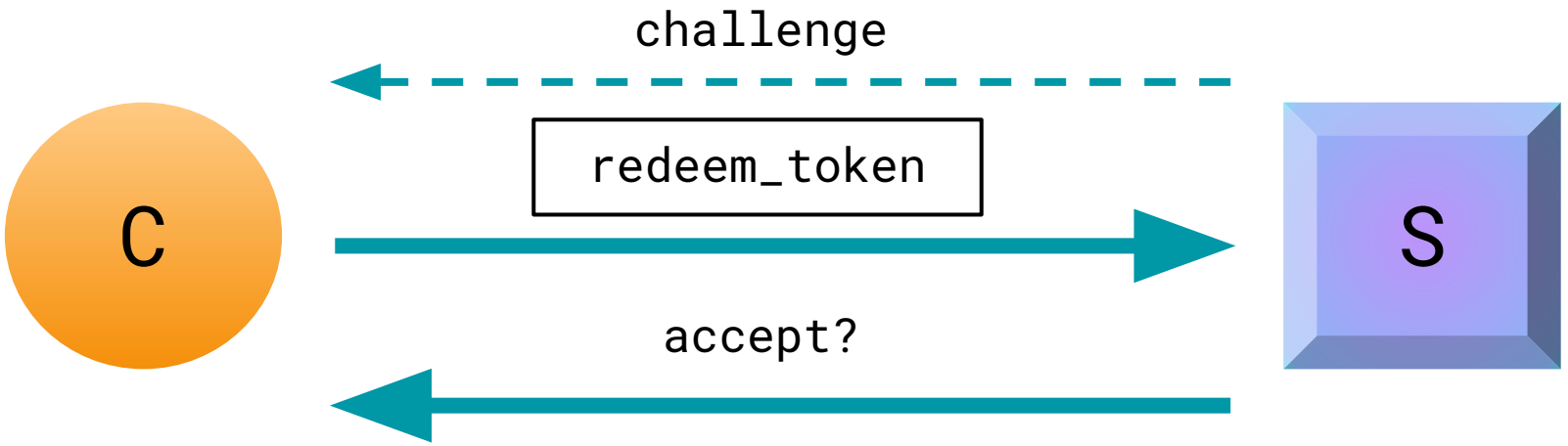
A protocol for producing unforgeable tokens that attest to some client attribute.

Tokens that are redeemed are unlinkable from those that were originally issued.

(they do not reveal how or when they were created)

Token issuance

Token redemption



How does it work?

Uses an underlying cryptographic protocol for computing a verifiable oblivious pseudorandom function (VOPRF)

Draft specification:
https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/

Costs

Additional cryptographic data in messages:

- request_tokens: ≤ **65** bytes per token
- issue_tokens: ≤ **65** bytes per token + **130** bytes
- redeem_token: ~ **64** bytes

Computation (public-key cryptography ops):

- Issue: client ~ **3** per token, server ~ **4** per token
- Redeem: client **0**, server **1**

Application: Abuse prevention

Cloudflare's CDN issues Privacy Pass tokens to clients that complete Internet CAPTCHAs

- https://privacypass.github.io

Online ad platforms can use tokens to ensure ad clicks are made by non-fraudulent actors

- https://github.com/WICG/trust-token-api
- https://engineering.fb.com/security/partially-blind-signatures/

Application: Anonymous currency

Brave clients use a variant of Privacy Pass to acquire Basic Attention Tokens (BATs)

- https://github.com/brave/brave-browser/wiki/Security-and-privacy-model-for-ad-confirmations

Anonymous receipts for prepaid services

- https://medium.com/least-authority/the-path-from-s4-to-privatestorage-ae9d4a10b2ae
- https://openprivacy.ca/assets/towards-anonymous-prepaid-services.pdf

Conclusions

Privacy Pass is a performant protocol that is already being used for providing trust-based attestation on the Internet

We hope to form a working group that will standardise the usage of the protocol and any specific implementation considerations

Alex Davidson

coela@alxdavids.xyz

@alxdavids

Privacy Pass

Problem statement and use-cases

https://datatracker.ietf.org/wg/privacypass/about/