Privacy Pass Implementation & Deployment Tests

Tommy Pauly
Privacy Pass
IETF 114, July 2022, Philadelphia

Open Source

GitHub implementations

https://github.com/cloudflare/pat-app

Client / Origin / Attester / Issuer functionality for all basic and rate-limited variants

https://github.com/raphaelrobert/privacypass

Client / Origin / Issuer functionality for basic variants

WWDC22

Replace CAPTCHAs with Private Access Tokens

Privacy pass protocol

Privacy pass standard from IETF

PrivateToken HTTP authentication

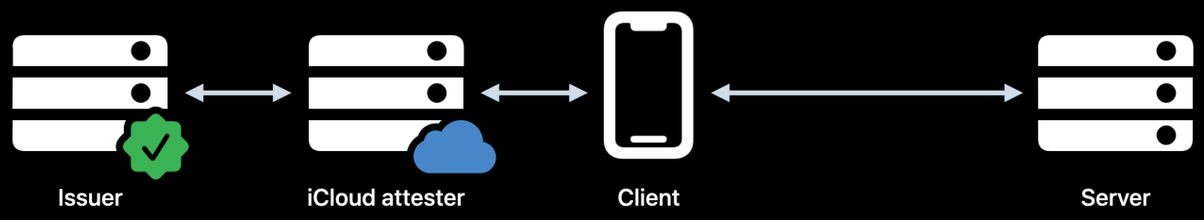
RSA blind signatures

Servers cannot track client identity

PRIVACY PASS

IETF

Privacy pass protocol



WWDC22

Aiming to increase awareness of Privacy Pass

Allowing developers of apps and websites to test out using Privacy Pass

Other issuer and attester implementations are encouraged to grow the ecosystem!

Testable deployments

Cloudflare and Fastly Issuers

- demo-pat.issuer.cloudflare.com
- demo-issuer.private-access-tokens.fastly.com

iCloud Attester

- Device + account attestation

iOS 16 and macOS Ventura system clients

Demo origins

- https://demo-pat.research.cloudflare.com/

What's supported

Type 2 (Publicly Verifiable Basic Tokens)

Split Origin, Attester, Issuer model

Supports origin-bound or cross-origin tokens

Token challenges only accepted from first-party domains in web context

Scale

Based on early betas

~35K tokens issued per day (seen by Attester)

~16K tokens redeemed per day (seen by Origins working with Cloudflare managed CAPTCHA)

Minimal latency for token issuance (~100ms)

Questions?