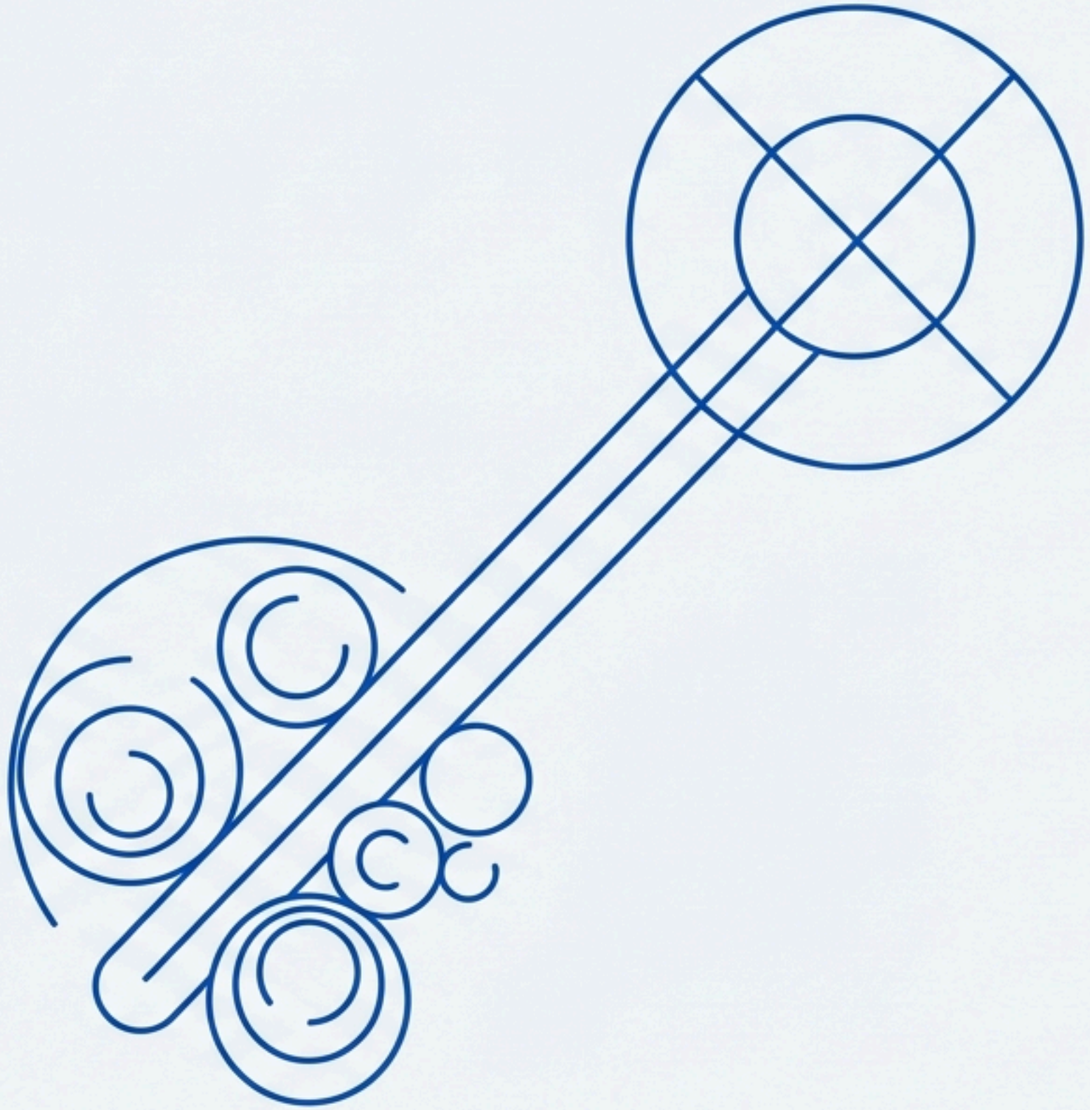
Privacy Pass: The Quest for a Private, CAPTCHA-Free Web

The story of a zero-knowledge protocol that evolved from a clever hack into a global web standard.



The Problem

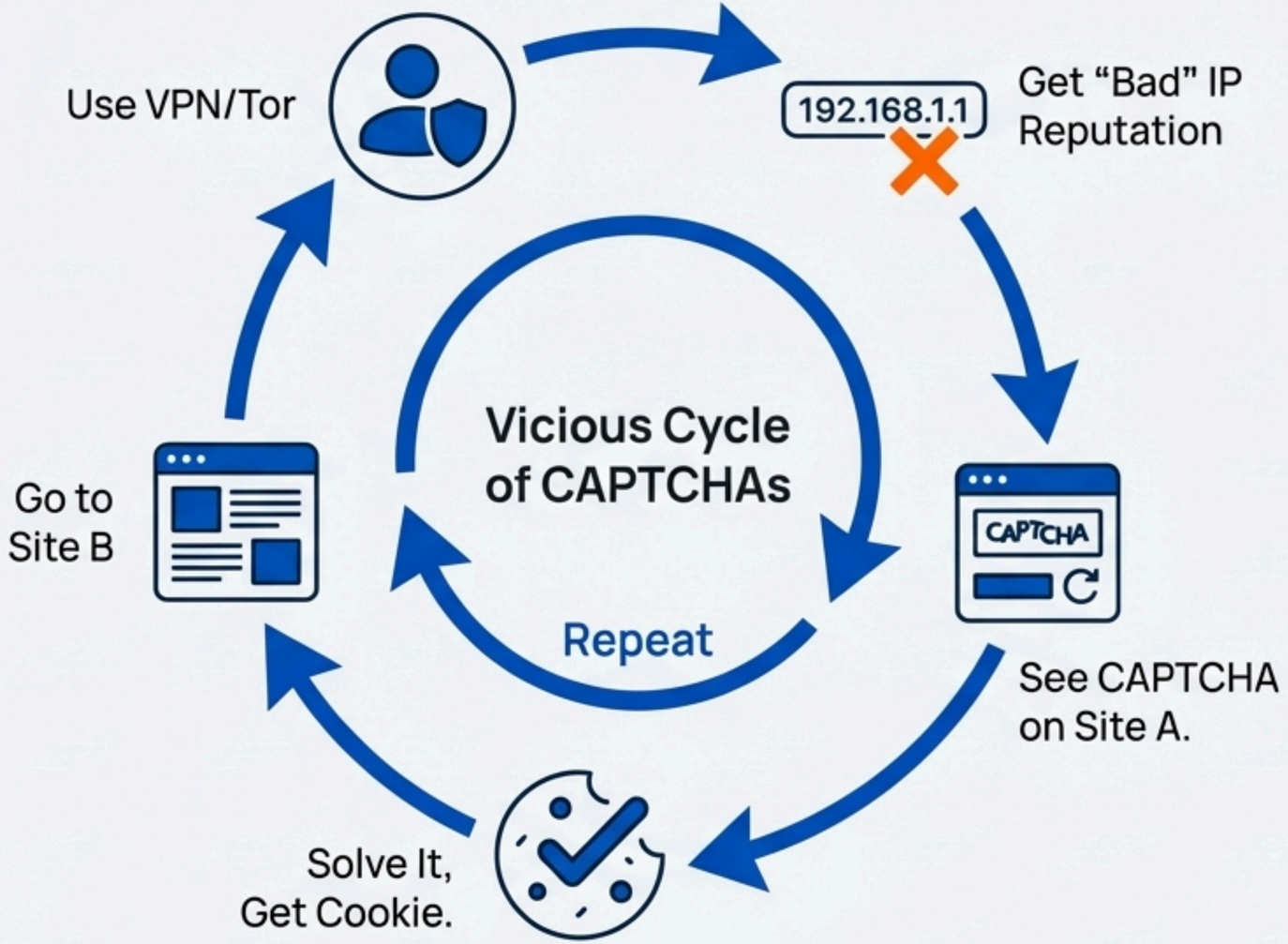
The Internet's Gatekeeper: A Trade-Off Between Security and Experience

Websites must distinguish between humans and bots to prevent abuse like spam, *credential stuffing*, and SQL injections.

For years, the primary tool has been the CAPTCHA, a *blunt* instrument that harms user *experience* and consumes a staggering amount of human time.

The Privacy Penalty: This problem disproportionately affects privacy-conscious users. Those using VPNs or anonymity services like Tor are challenged more frequently due to IP reputation systems.

One Solution, Millions of Problems



The Web Origin Policy is a core security principle preventing websites from sharing information.

This means when you solve a CAPTCHA on one site, you receive a cookie that is useless on any other site.

This creates a vicious cycle for users, especially those on VPNs, who must solve the same puzzles repeatedly across the web.

Wouldn’t it be nice to have a reusable, anonymous ‘pass’ to prove you’re human just once?

The Core Idea: Blind Signatures

The solution is inspired by David Chaum's 'e-cash' concepts from the 1980s.

The Principle: An authority can cryptographically sign a piece of data without knowing its contents. This creates a token that is both:

Authorized: Provably signed by a trusted issuer.
Unlinkable: The issuer cannot connect the token they signed to the one that is later redeemed.

1. Prepare
2. Sign
3. Redeem

Modernizing an Old Technique for the Web

The initial blinded signature schemes used RSA, which is computationally expensive and too slow for the high-traffic demands of the modern web.

The Breakthrough: The protocol combines two powerful concepts using efficient elliptic curve cryptography:

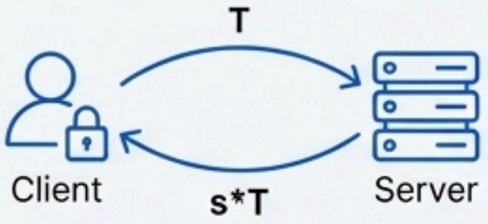
1. **Oblivious Pseudorandom Functions (OPRFs):** A server and client can compute a function where the server learns nothing about the output.
2. **Verifiable Random Functions (VRFs):** A server can prove that a function was computed with a specific private key.

The Result: A **Verifiable Oblivious PRF (VOPRF).** This construction, standardized in RFC 9497, is the fast and lightweight cryptographic engine of Privacy Pass.

Forging an Unforgeable, Unlinkable Token

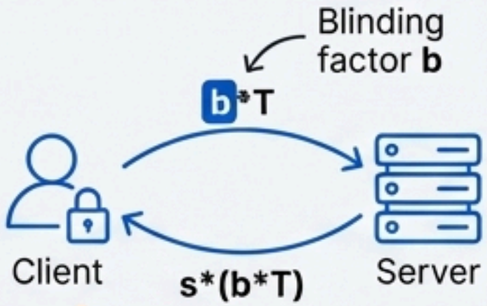
Through iterative cryptographic design, the protocol achieves security against key attacks. Each step adds a new primitive to fix a flaw in the previous one.

1. Base Protocol



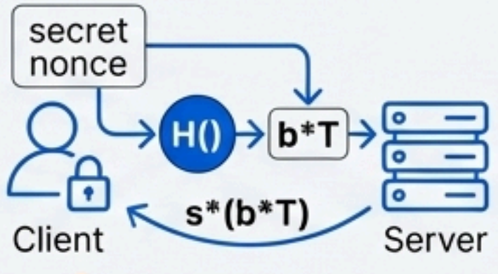
Flaw: Linkable. The server sees T at both issuance and redemption.

2. Add Blinding



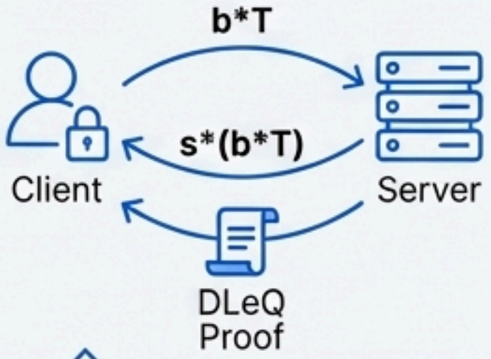
Flaw: Malleable. A user can create infinite valid tokens from one signature.

3. Add Hashing



Flaw: Redemption Hijacking. An eavesdropper could steal and use the token.

4. Add Zero-Knowledge Proof



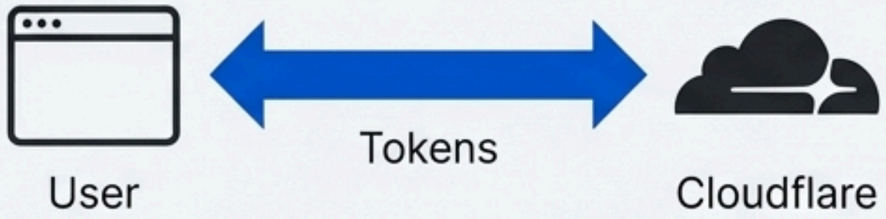
Fix: This proves the server used the same secret key **s** for everyone, preventing malicious targeting of specific users with unique keys.

The Protocol Matures: A Four-Party Ecosystem

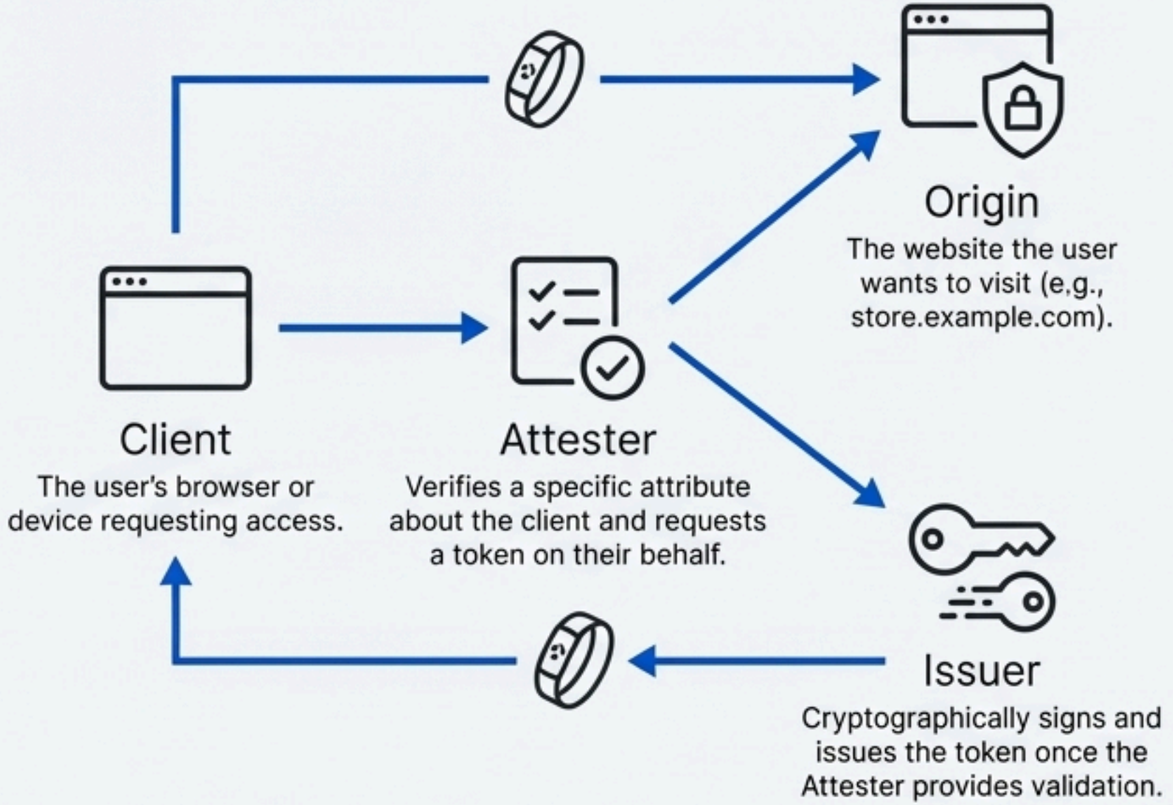
The original protocol was a direct exchange. The modern, standardized version separates duties to enhance privacy, ensuring no single party has the full picture.

Then (2017)

Monolithic Two-Party Exchange

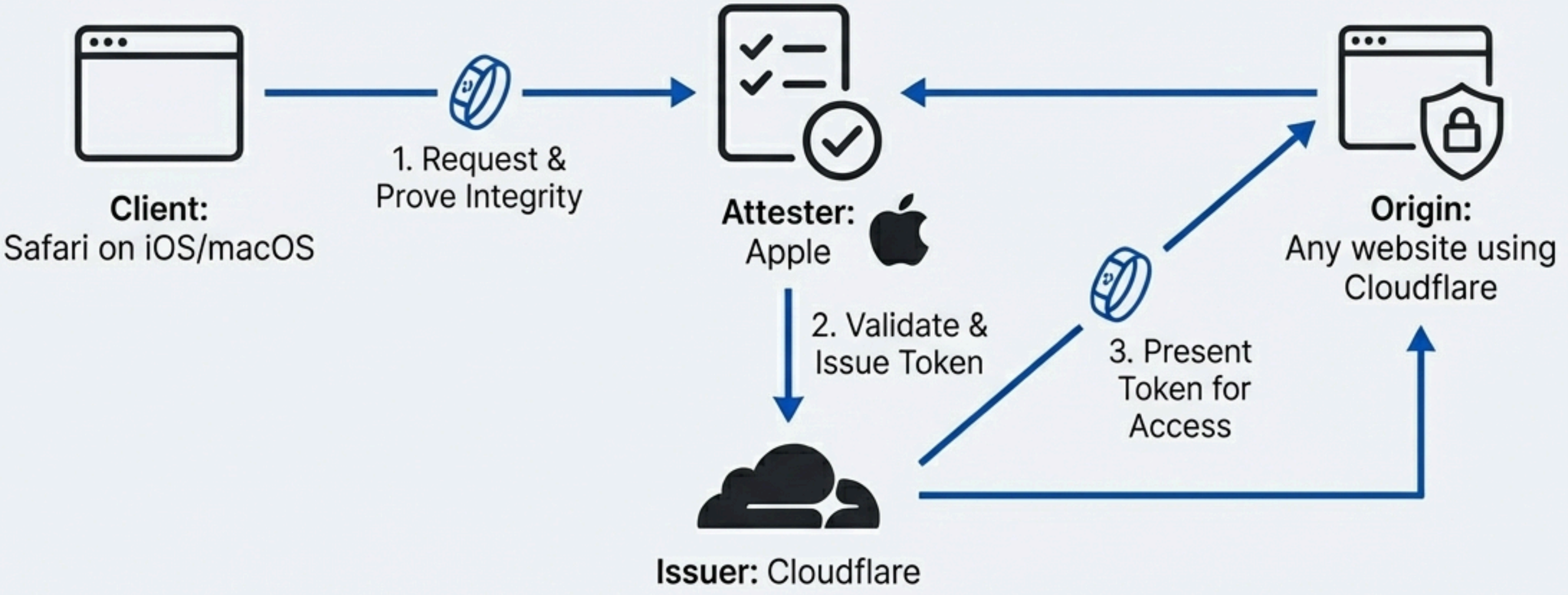


Now (2024)



Ultimate Validation: Powering Private Access on Apple Devices

- In 2022, Apple integrated Privacy Pass into iOS and macOS as ‘Private Access Tokens’ (PATs).
- This system uses the four-party model to dramatically reduce the need for CAPTCHAs on supported devices.
- The device’s secure hardware itself acts as the **Attester**, proving its own integrity to Apple without revealing sensitive device information. This allows websites to trust the device without fingerprinting it.



Verifying Without Seeing: The Privacy of Compartmentalization

Private Access Tokens allow a website to trust a user's device without ever collecting, touching, or storing the underlying device data. It is validation through cryptographic abstraction. No single party sees the full context of the user's activity.

Traditional CAPTCHA Provider	Privacy Pass (PATs) Ecosystem
Sees: Your IP Address	**Origin** (Website) ✓ Sees: Your IP Address ⊘ Website Visited ⊘ Device Info ⊘ Interaction Data
Sees: Website Visited	**Attester** (Apple) ⊘ Your IP Address ⊘ Website Visited ✓ Sees: Device Info ⊘ Interaction Data
Sees: Device Info	**Issuer** (Cloudflare) ⊘ Your IP Address ⊘ Website Visited ⊘ Device Info ⊘ Interaction Data
Sees: Interaction Data	Sees nothing about you or your device; it only signs tokens when asked by a trusted Attester.

From Protocol to Internet Standard

To ensure interoperability and provide a stable foundation for the future, the core components of Privacy Pass have been formalized and adopted as official web standards by the Internet Engineering Task Force (IETF).

This process involved collaboration across industry and academia, solidifying the cryptography and architecture for widespread use.

Verifiable Oblivious Pseudorandom Functions (vOPRFs)

RFC 9497

RSA Blind Signatures

RFC 9474

Beyond Theory: A Deployable, Open-Source Ecosystem

A full suite of open-source tools is now available to implement and experiment with the latest version of the Privacy Pass protocol.

For Users

Silk

Silk - Privacy Pass Client

Brings the benefits of Privacy Pass to any user, reducing the number of challenges they see online.

For Developers

A set of open-source templates built on Cloudflare Workers makes it easy to deploy the different roles in the ecosystem.

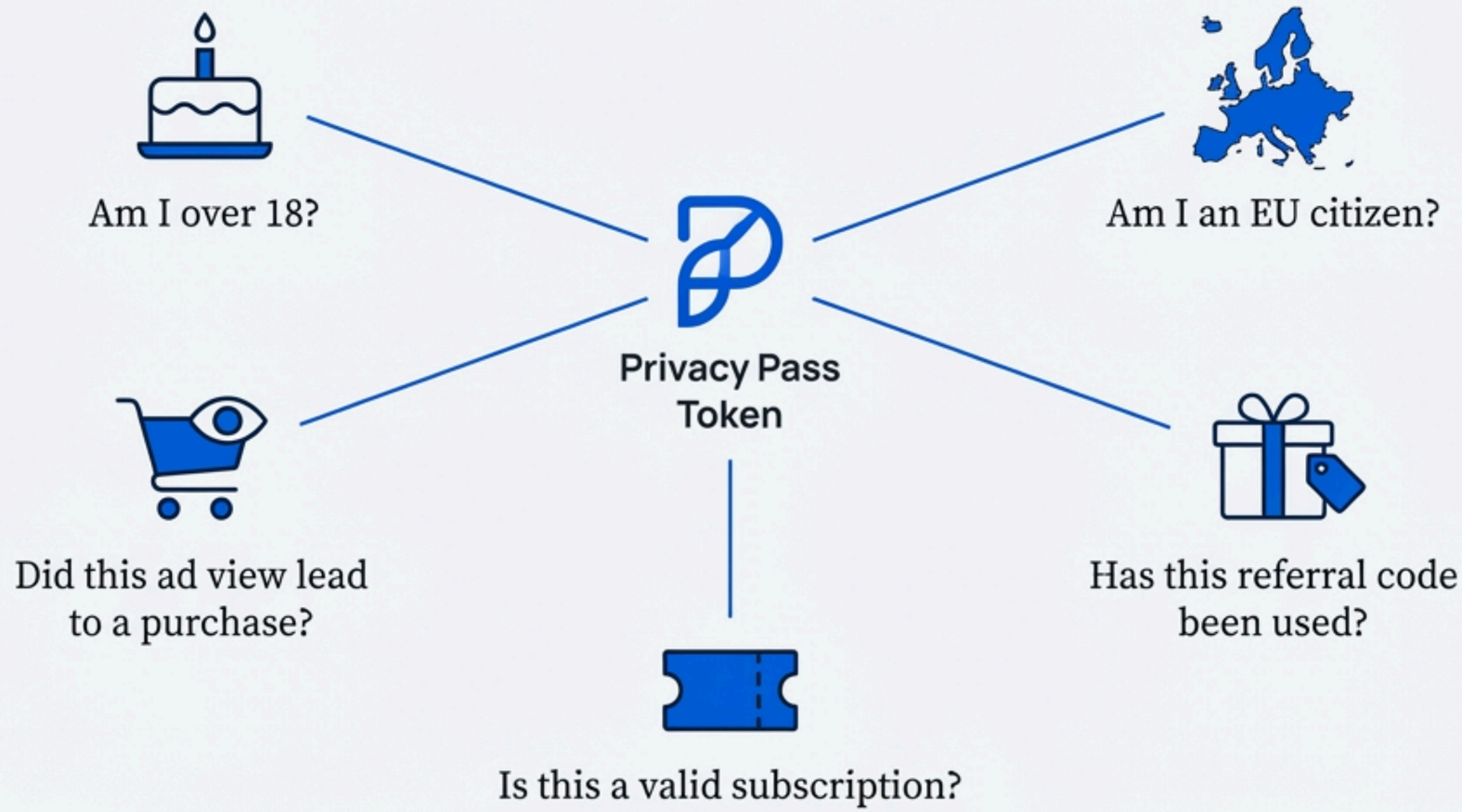
pp-origin

pp-attester

pp-issuer

The Power of a Single, Private Bit

At its core, Privacy Pass allows a user to prove– a single binary fact (“yes/no”) without revealing anything else. This cheap, zero-knowledge “bit” is a powerful primitive for a huge range of new privacy-preserving applications.

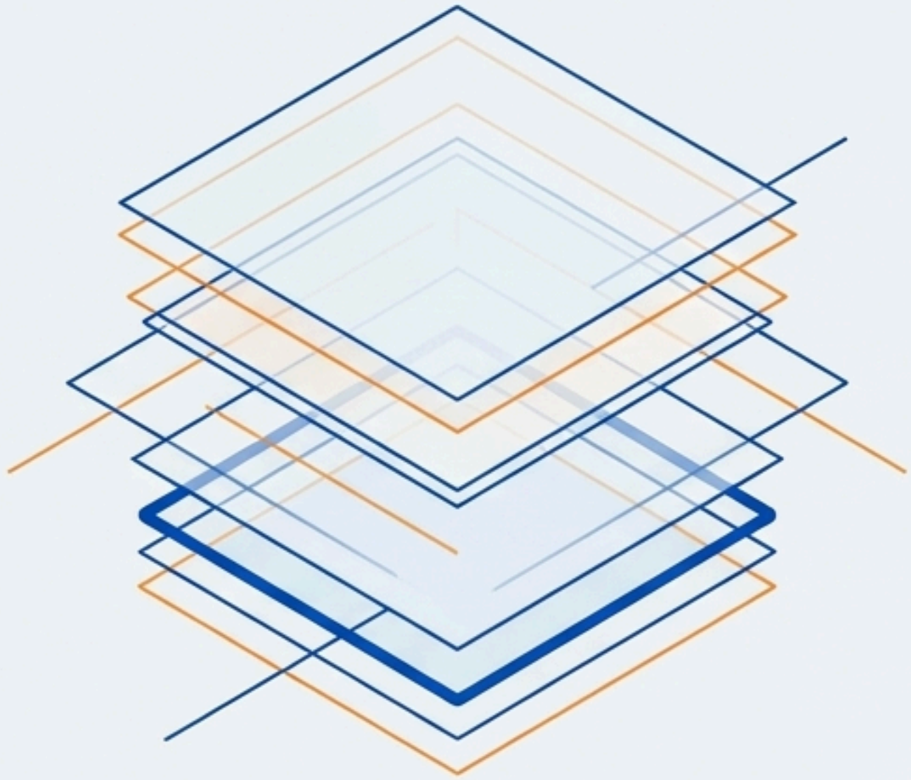


Building a Composable and Private Internet

Privacy Pass offers a new primitive for web authentication, moving beyond the crude metric of IP-based reputation.

It empowers developers to request verification while empowering users to preserve their privacy.

Ongoing work in the community includes expanding federation between providers, developing rate-limiting mechanisms, and researching post-quantum versions of the core cryptography.



Explore the open-source repositories, experiment with novel attestation methods, and help build a better, more private web.

github.com/cloudflare/pp-browser-extension

github.com/cloudflare/pp-issuer

github.com/cloudflare/pp-attester