PRIVACY PASS, TRUST, AND THE WEB

Martin Thomson, Privacy Pass WG, IETF 119, March 2024

WEB USE CASE

Goal: Examine the uses of Privacy Pass on the Web

Specifically, Privacy Pass as built into Web Browsers

As seen in:

- Apple’s Private Access Tokens
- Google’s Private State Tokens

Not Cloudflare’s Privacy Pass Browser Extension

AUTHORIZATION MODES

Signatures, Passkeys, etc...

Strong, unique bindings to

- Identity, key, time, context, usage, etc...

Highly linkable

- Low privacy expectations

Requires user intervention

Privacy Pass

Loose bindings only to Issuer key

- and maybe some contextual information

Tokens form anonymity set

- Provides privacy and transfer of tokens

Maybe operates without intervention

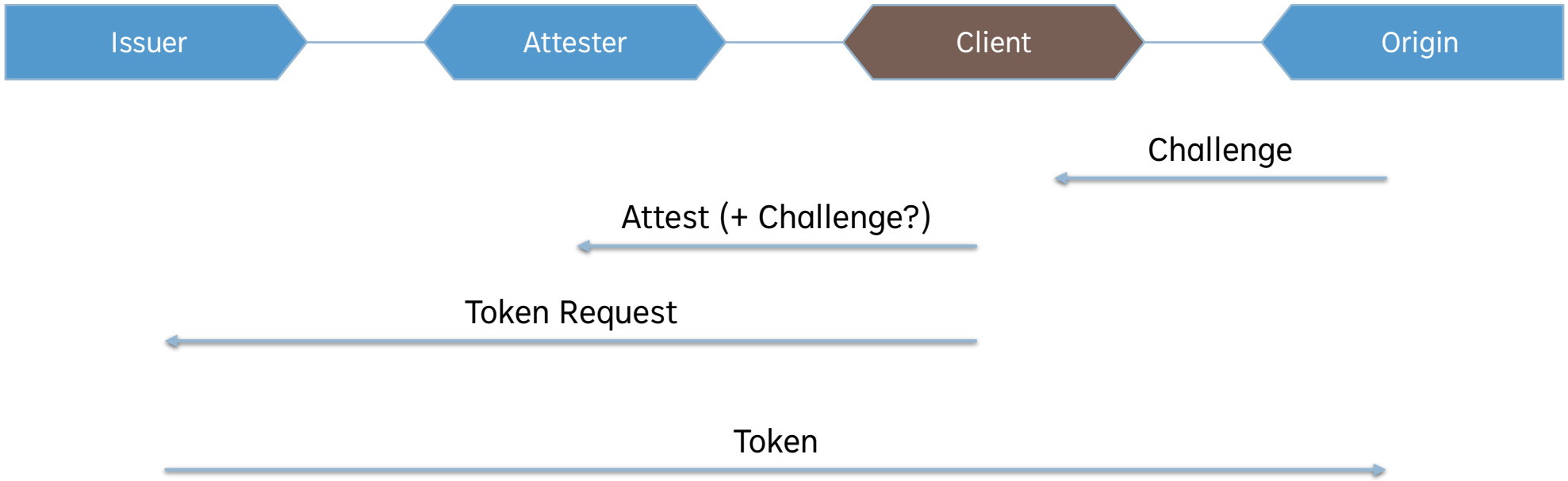
TOKEN MAGIC

Cryptography provides a means to limit information transfer

This can reduce the need for some parties to trust others

... or rather, to **reduce the ways in which other entities are trusted**

INFORMATION FLOW (RECAP)



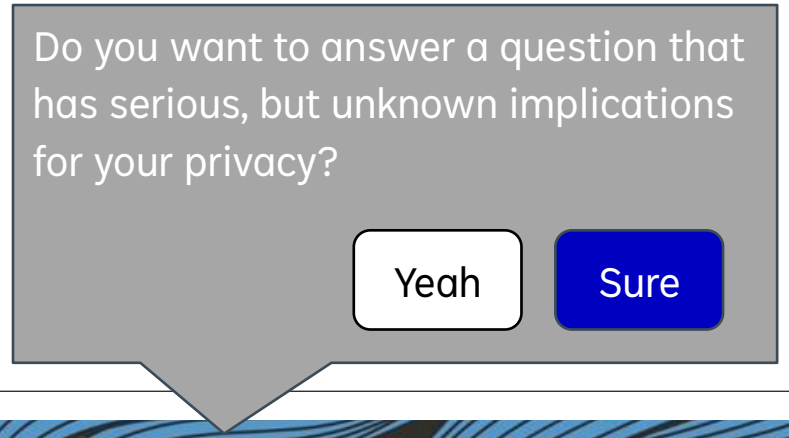
LOW STAKES AUTHORIZATION

Premise: *if privacy is good, user intervention might not be needed*

Seems useful for a bunch of Web use cases

- Fraud mitigation in particular
- Trade fidelity for availability

Maybe we don't need this:



INFORMATION TRANSFER

The presence or absence of a **token** carries information

Timing carries information

Transport **metadata** (IP address) carries information

This information might not always be useful,

... but designs need to account for leaks like these

LOOSE BINDINGS

Privacy Pass tokens are only loosely bound

- To a specific Issuer key
- Maybe to the target Origin
- Maybe to some additional contextual information

Loose bindings mean tokens are transferrable within their scope

- Scope does not include Client identity
- This means that tokens can be transferred to Clients outside of the authorized set

Additional bindings narrow the anonymity set and create privacy issues

- **Too many bindings → anonymity set is small → reduced/no privacy**

WHO TRUSTS WHOM

	Issuer	Attester	Client	Origin
Issuer		🤷	🤷	🤷
Attester	🤷		🤷	🤷
Client	🤷	🤷		🤷
Origin	🤷	🤷	🤷	

Trust relationships depend on deployment model

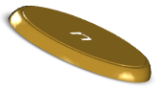
TRUST AND TOKENS

Every token carries **at least one bit**

Clients need to decide whether to pass that bit from Issuer (/Attester) to Origin

What does the bit *mean*?

TOKEN MEANING IS UNKNOWABLE



A token might mean “Person at computer”

- That is probably OK

Note: Adding metadata doesn’t change this

- The meaning of the bit is still unknowable, even if the metadata is known

Lots of other meanings that are NOT OK

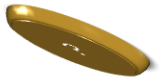
- Attesters get lots of information that they might pass to Issuers
- Tokens could mean anything

NO GUARANTEES

No guarantee that the bit means anything in particular

No guarantee that the anonymity set is large

TRUST IS ALL



Privacy Pass deployments therefore rely on trust

Clients trust that the Issuer is not passings notes to the Origin

...and that the Attester is not helping with that

The Web is not kind on solutions that rely on trust

OPTIONS TO EXPLORE

Governance structures

- See Google's attestation form or Apple's registration
- Strong desire to avoid introducing gatekeepers
- Challenging incentive structure

Sovereign identity providers

DISCUSS