Including Privacy Pass Tokens in TLS Handshakes

draft-pauly-privacypass-for-tls-00

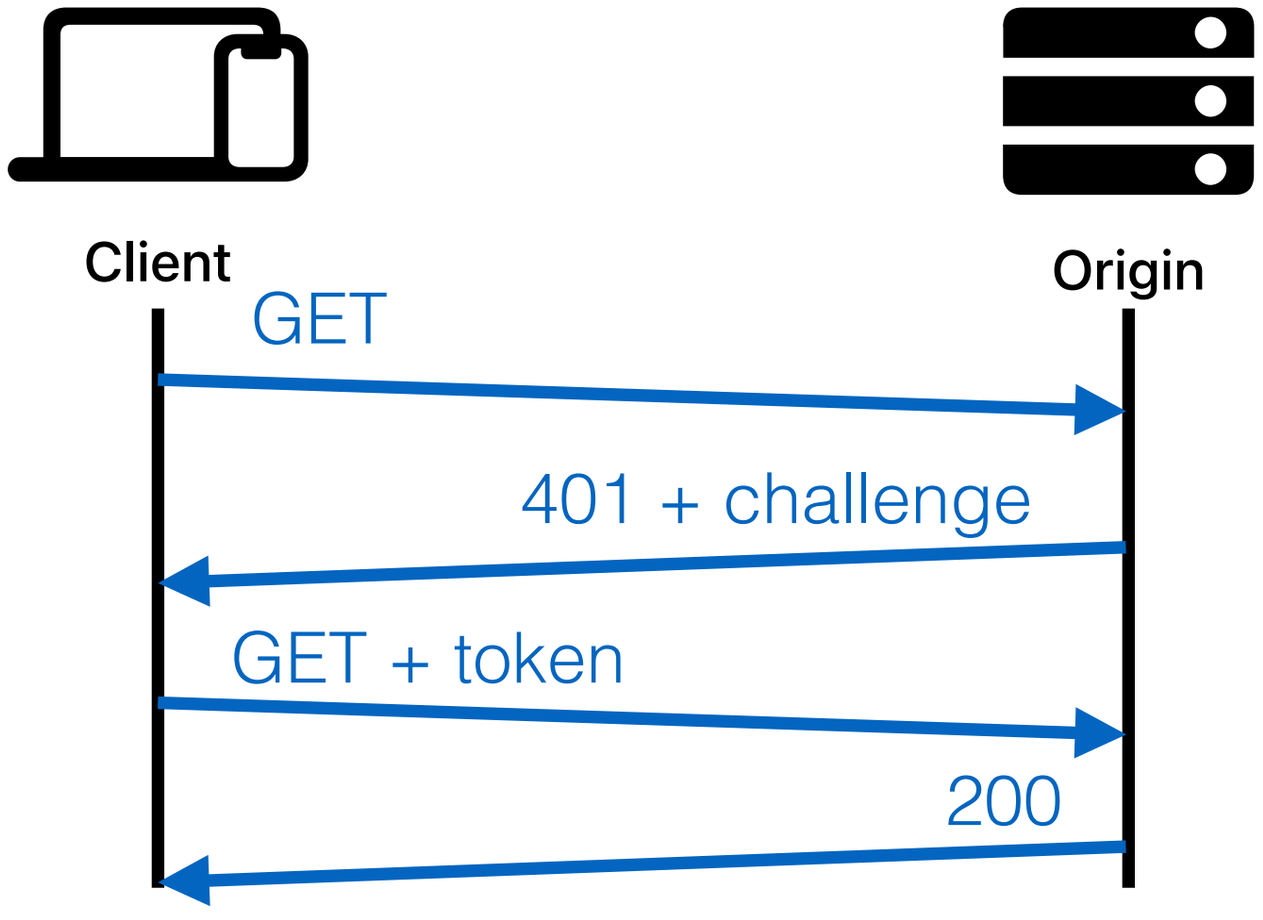
Tommy Pauly & Scott Hendrickson
Privacy Pass
IETF 122, March 2025, Bangkok

Privacy Pass as HTTP Auth

RFC 9577

The current standard transport for Privacy Pass tokens is HTTP authentication fields

```
Authorization: PrivateToken token="abc..."
```



Is HTTP Auth enough?

HTTP auth is generally a great place for privacy pass

There are use cases for other mechanisms, still!

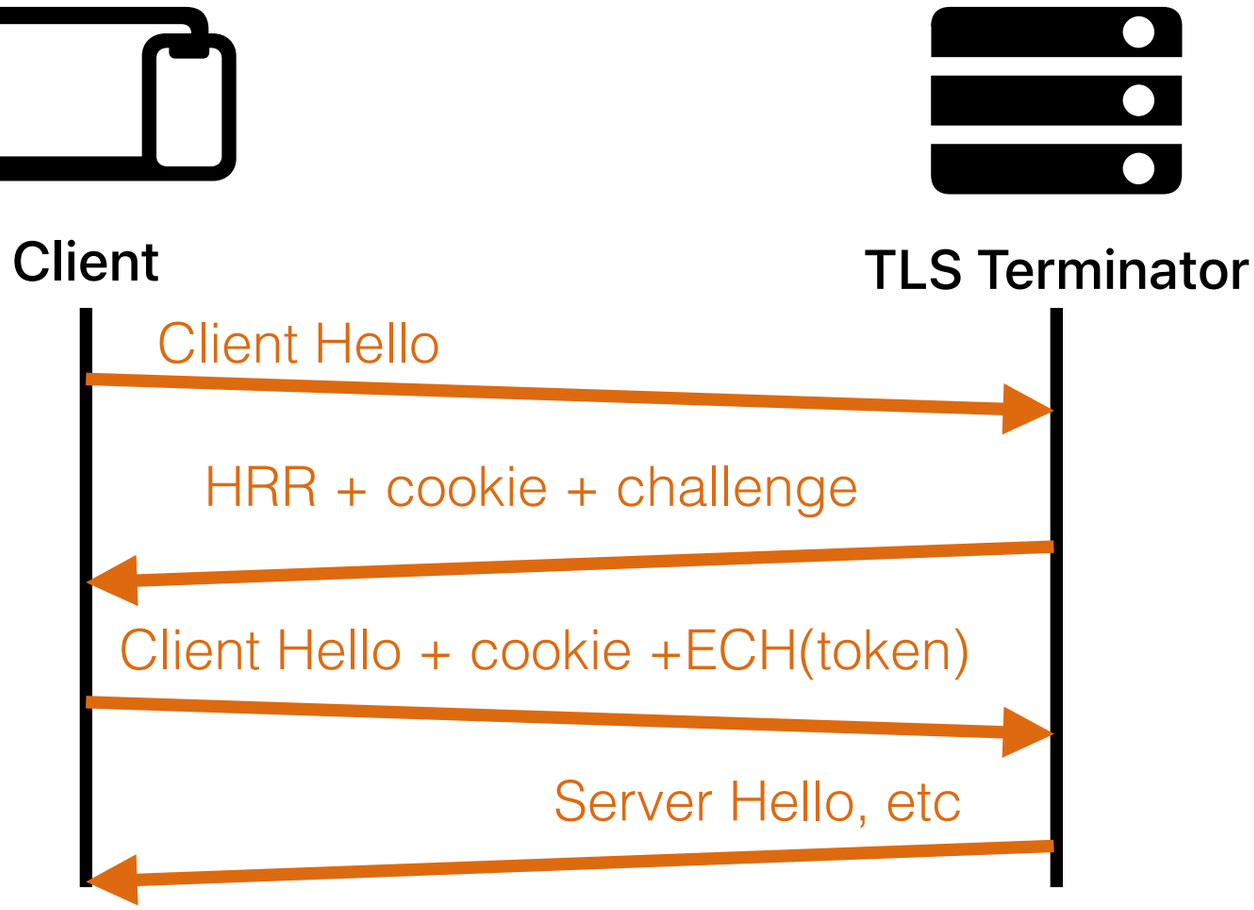
- EAP + Privacy Pass already being defined
- SIP could transport with fields like HTTP
- ... these are usually at application layers

TLS terminators can enforce their own rate limits

- Particularly impacts users sharing IP addresses in privacy proxy deployments
- Can block or degrade traffic before it reaches HTTP servers that will handle Privacy Pass tokens
- Can speed up challenge flow when TLS terminator is close to client, and far from application server

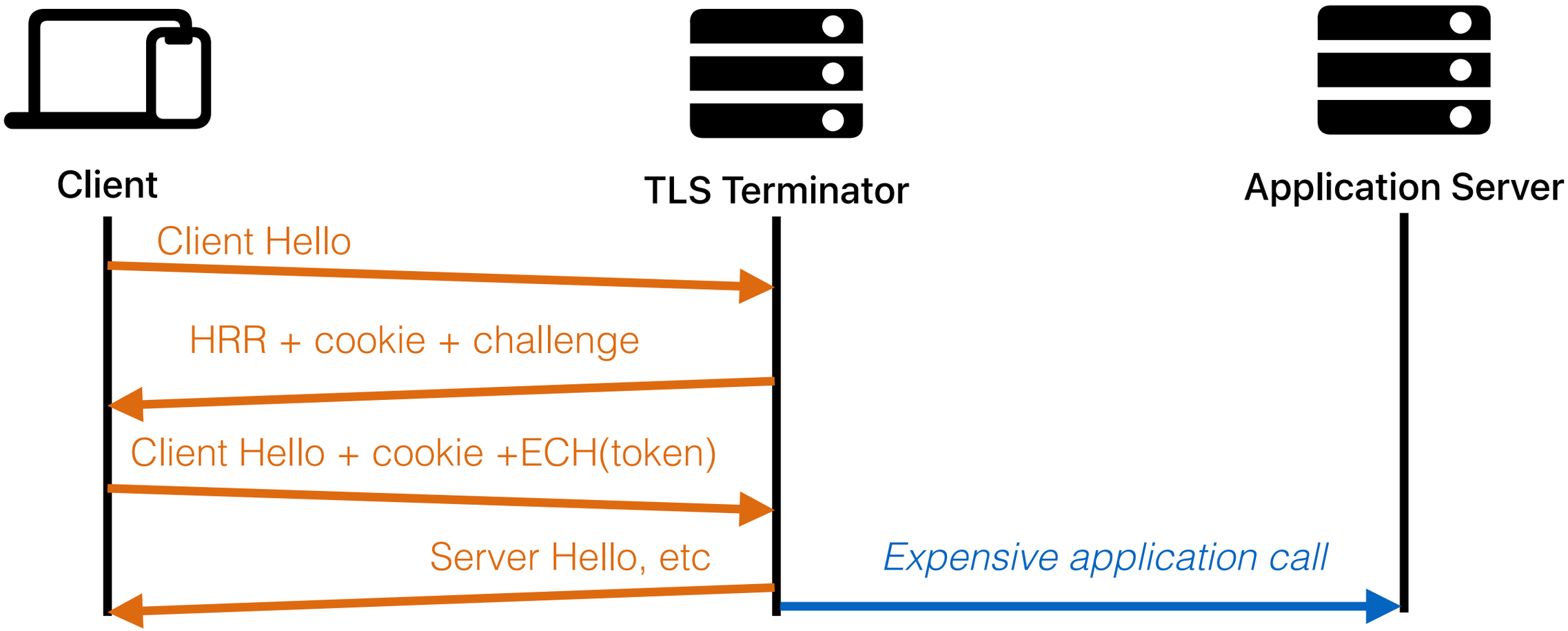
Privacy Pass as TLS Cookie

This draft takes the same challenge and tokens, and uses them during the TLS handshake



Privacy Pass as TLS Cookie

This draft takes the same challenge and tokens, and uses them during the TLS handshake



Protocol Overview

- Uses any existing or new token type
  - New types like ARC or BBS will be better for being able to generate new presentations without talking to attesters/issuers again
- Servers send challenges in HRR (along with a cookie)
  - Cookies used as redemption context, to prevent token reuse
- Clients send tokens in Encrypted Client Hello
  - ECH prevents others from seeing and replaying tokens

Questions

Are people interested in working on this direction?

Should we adopt here? Coordinate with TLSWG?