Chair of Connected Mobility
School of Computation, Information and Technology
Technical University of Munich

Third-Party Tokens for QUIC Address Validation

Benedikt Spies, Nico Greger, Jonathan Kaleve, and Justus Fries

QUIC

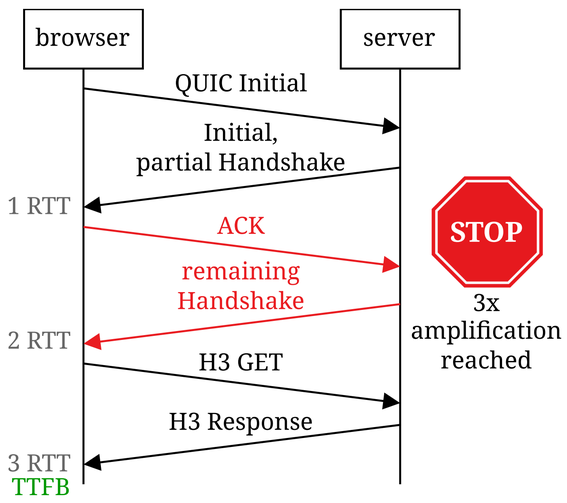
QUIC [RFC 9000] enables fast connection establishment for HTTP/3 in 1 RTT.

To prevent amplification attacks a QUIC server must limit the amount of data sent to an unvalidated address to 3x the amount of data received from the client.

The client address is validated after 1 RTT or with an Address Validation Token (AVT).

- QUIC trades performance for privacy [1]
- Large certificates prolong handshakes [2]

QUIC Handshake



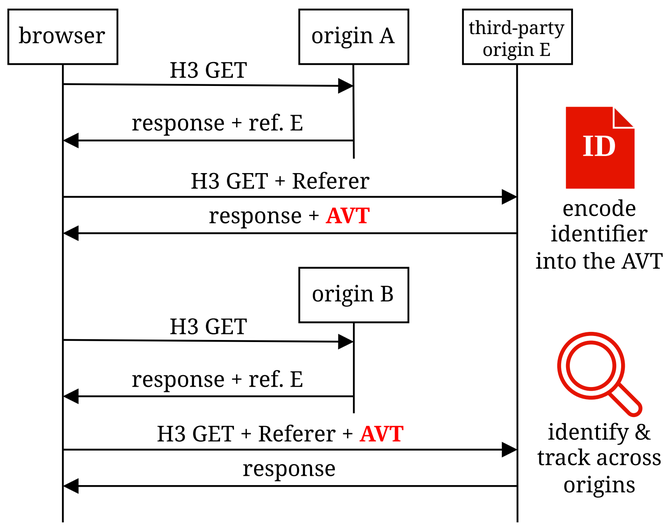
Many QUIC handshakes cannot be completed within 1 RTT because the response of the server exceeds the anti-amplification limit.

Address Validation Token (AVT)

- AVTs are shared by the QUIC server in *NEW_TOKEN* frames
- 15% of HTTP/3 servers issue AVTs, with sizes between 42 to 86 B
- All tested browsers cache AVTs for the whole browser session

- AVTs are not available on first connect
- Server can encode arbitrary data into an AVT

Web Tracking



AVTs can be used for tracking similar to cookies. Currently there is no evidence of AVT trackers.

Embedded third-parties identify origin by *Referer* header or origin specific URLs.

Web Tracking Protection

	Cookie Tracking	AVT Tracking
Chrome	Vulnerable	Vulnerable
Firefox	Protected	Vulnerable
Brave	Protected	Protected

Firefox and Brave use isolated caches per origin to prevent tracking: *Total Cookie Protection* and *Ephemeral Storage*, respectively.

- Common third-party page resources (e.g., fonts) benefit most from fast handshakes, but are also critical vectors for tracking

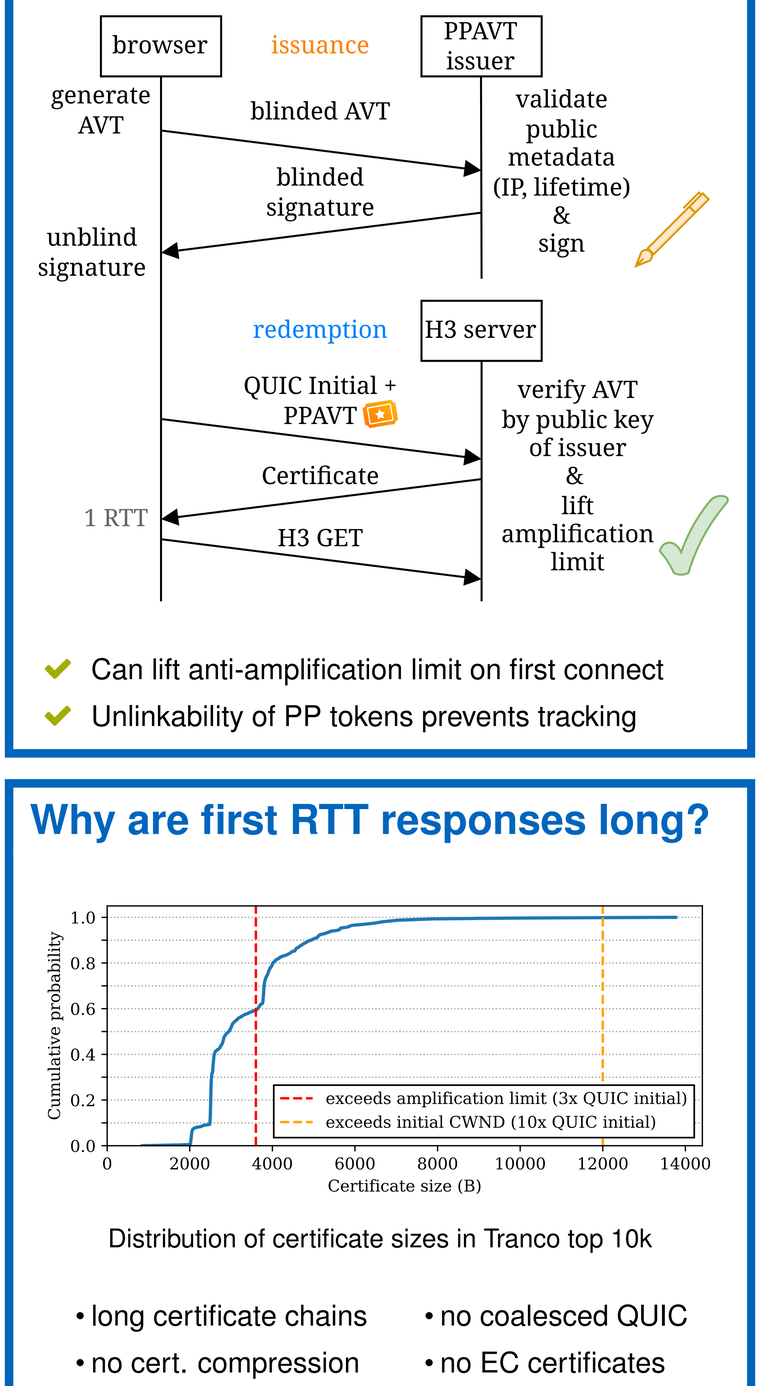
Privacy Pass (PP)

Privacy Pass [RFC 9576] enables privacy-preserving authentication.

Instead of presenting linkable state-carrying information to servers (e.g., cookies, AVTs), clients present unlinkable tokens, only sharing one-bit of information.

More information can be shared, as specified in the *public-metadata-issuance* draft, based on *PBRSA*.

Privacy Pass Address Validation Tokens (PPAVT)



- ✓ Can lift anti-amplification limit on first connect
- ✓ Unlinkability of PP tokens prevents tracking

Why are first RTT responses long?

Distribution of certificate sizes in Tranco top 10k

- long certificate chains
- no cert. compression
- no coalesced QUIC
- no EC certificates

Cryptography (simplified)

Cryptography is based on *RSABSSA* [RFC 9474] and *draft-amjad-cfrg-partially-blind-rsa*.

1 The browser generates a partially blinded request using the issuer's public key `pkI`.

```
nonce = random(32)
ext = { ip, lifetime }
blind_msg = Blind(pkI, nonce, ext)
req = { blind_msg, ext }
```

2 The issuer signs the request, after verifying the client's IP and lifetime.

```
blind_sig = BlindSign(skI, req)
resp = { blind_sig }
```

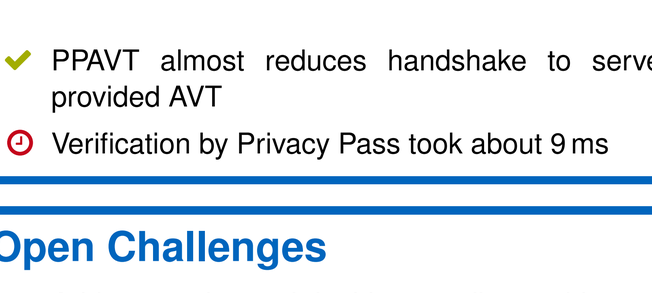
3 The client unblinds the signature, and generates the PPAVT.

```
sig = Finalize(pkI, nonce, ext, resp)
token = { nonce, ext, sig, issuer_id }
```

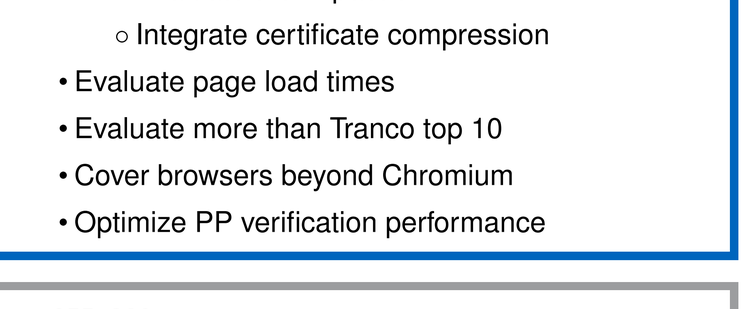
4 The server verifies the IP, lifetime, and signature with the issuer's public key.

```
Verify(pkI, token)
```

Testbed



Evaluation



Distribution of TTFB of different handshake modes

- ✓ PPAVT almost reduces handshake to server-provided AVT
- Verification by Privacy Pass took about 9 ms

Open Challenges

- Address replay and double-spending problem
- Enhance browser and H3 origin replication
  - Evaluate the impact of *ML-KEM*
  - Integrate certificate compression
- Evaluate page load times
- Evaluate more than Tranco top 10
- Cover browsers beyond Chromium
- Optimize PP verification performance

[1] Erik Sy, Christian Burkert, Hannes Federrath, and Mathias Fischer. A QUIC Look at Web Tracking. In *PoPETs '19*, volume 2019, pages 255–266.

[2] Marcin Nawrocki, Pouyan Fotouhi Tehrani, Raphael Hiesgen, Jonas Mücke, Thomas C. Schmidt, and Matthias Wählisch. On the interplay between TLS certificates and QUIC performance. In *CoNEXT '22*, pages 204–213. ACM.