v1

Privacy Pass Media Authorization in MOQ

Cullen Jennings

IETF 123:
22-July-2025

This is not a replacement for CAT.

I think we should do CAT and Privacy Pass and other tokens.

Motivation

Traditional Authorization exposes user view patterns

Content preference becomes **linkable** across sessions

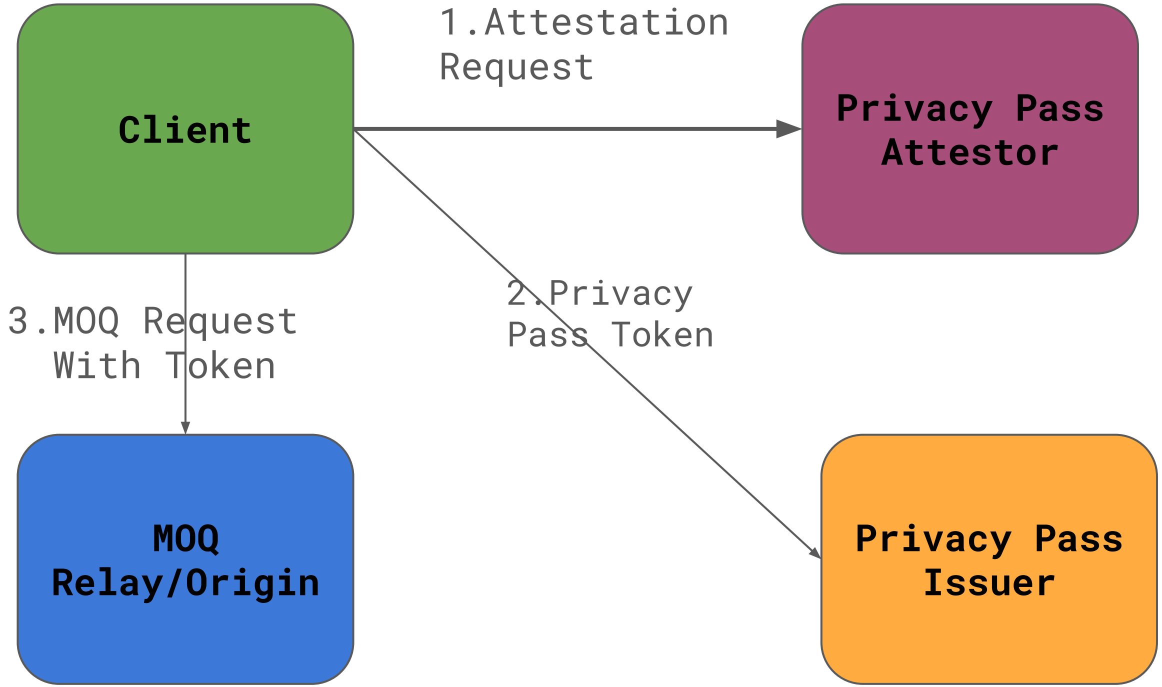
Users want **anonymous access** to media

Content Providers need **authorization guarantees**

Current Trade-off: Users must choose between privacy and access to premium content

Goal: Anonymous authentication without sacrificing fine-grained access control

Privacy-Pass Architecture



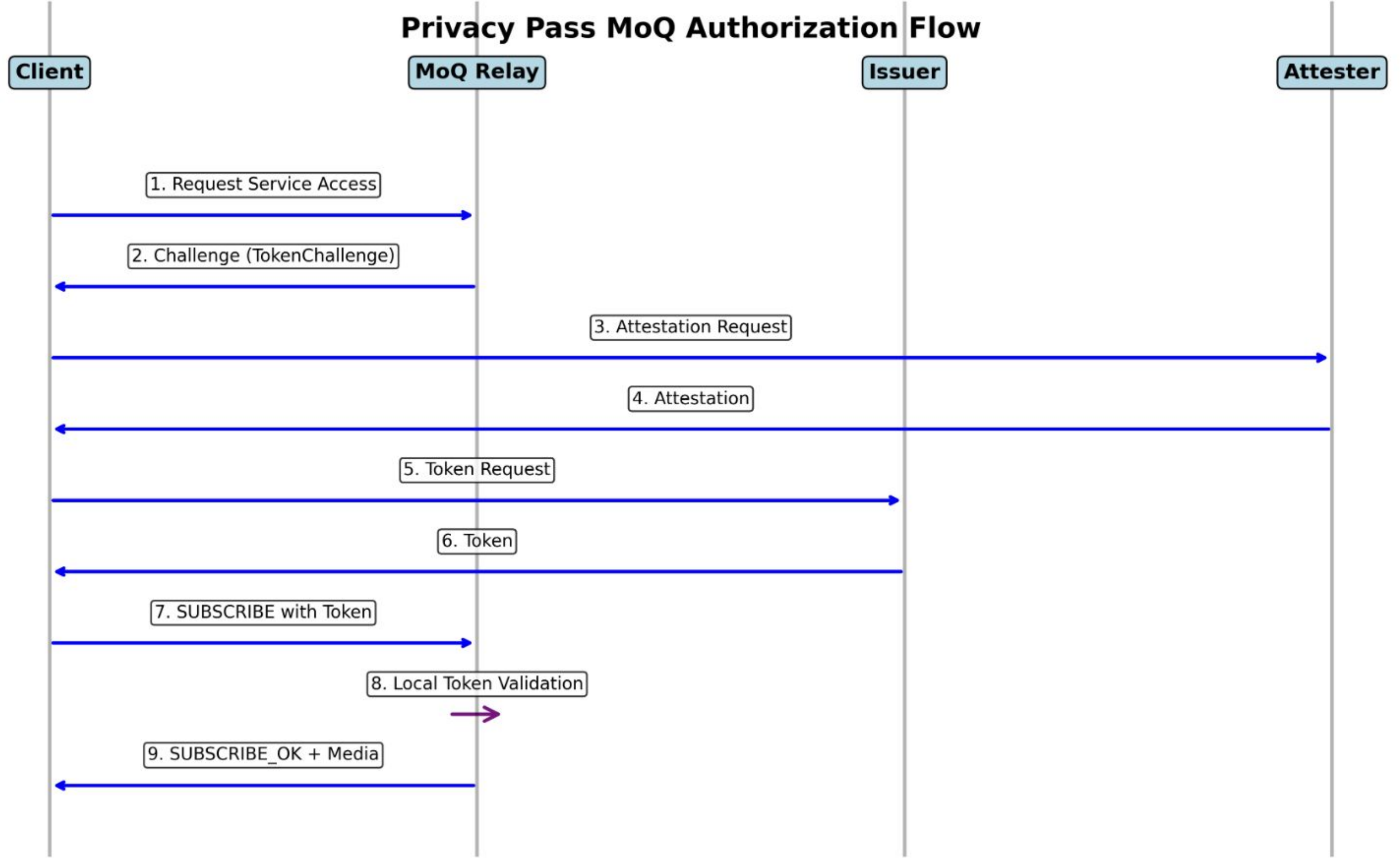
Unlinkability: Token Issuance <-> Redemption

Anonymous: No User identities in the token

Cryptographic: VOPRF or Blind RSA

Verifiable: Proof of eligibility

Privacy Pass Integration with MOQT


Privacy Pass MoQ Authorization Flow
Client
MoQ Relay
Issuer
Attester
1. Request Service Access
2. Challenge (TokenChallenge)
3. Attestation Request
4. Attestation
5. Token Request
6. Token
7. SUBSCRIBE with Token
8. Local Token Validation
9. SUBSCRIBE_OK + Media

Token Challenge (RFC9577 + moq-scope in origin_info)

Token Type
Issuer Name
Redemption
Context
Origin Info

```
moq-scope = operation ":" namespace-pattern [":" track-pattern]
```

Operations:

- subscribe - Request media streams
- fetch - Get specific media objects
- publish - Send media to relay
- announce - Advertise namespace

Example origin_info:
"subscribe:sports.example.com/live/*"

Namespace/Track Matching Rules

Exact Match

Pattern: “example.com/live/sports/soccer”

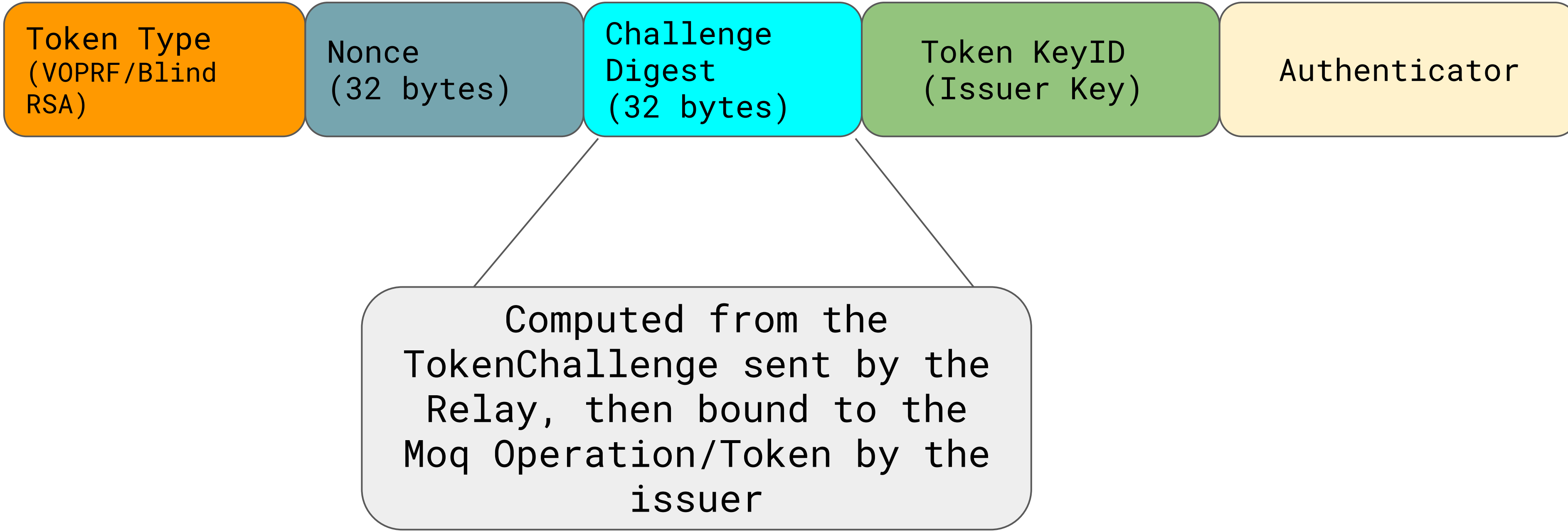
Matches: Only Exact Namespace

Prefix Match

Pattern: “example.com/live/sports/*”

Matches: Any string starting with the prefix

Toke Structure (RFC9577)



Privacy Pass Benefits

Privacy: Relay cannot link client identity to media consumption

Performance: Local token validation

Scalability: Issuer separation enables distributed deployments

Fine-grained: Namespace and track-level access control

Next Steps

Adopt this as a WG draft

And while we are at it, it’s time to adopt CAT as a WG draft