Privacy Pass for MOQ

IETF 124 MOQ/Privacy-Pass

Cullen, Suhas, Thibault

Media over QUIC (MOQ)

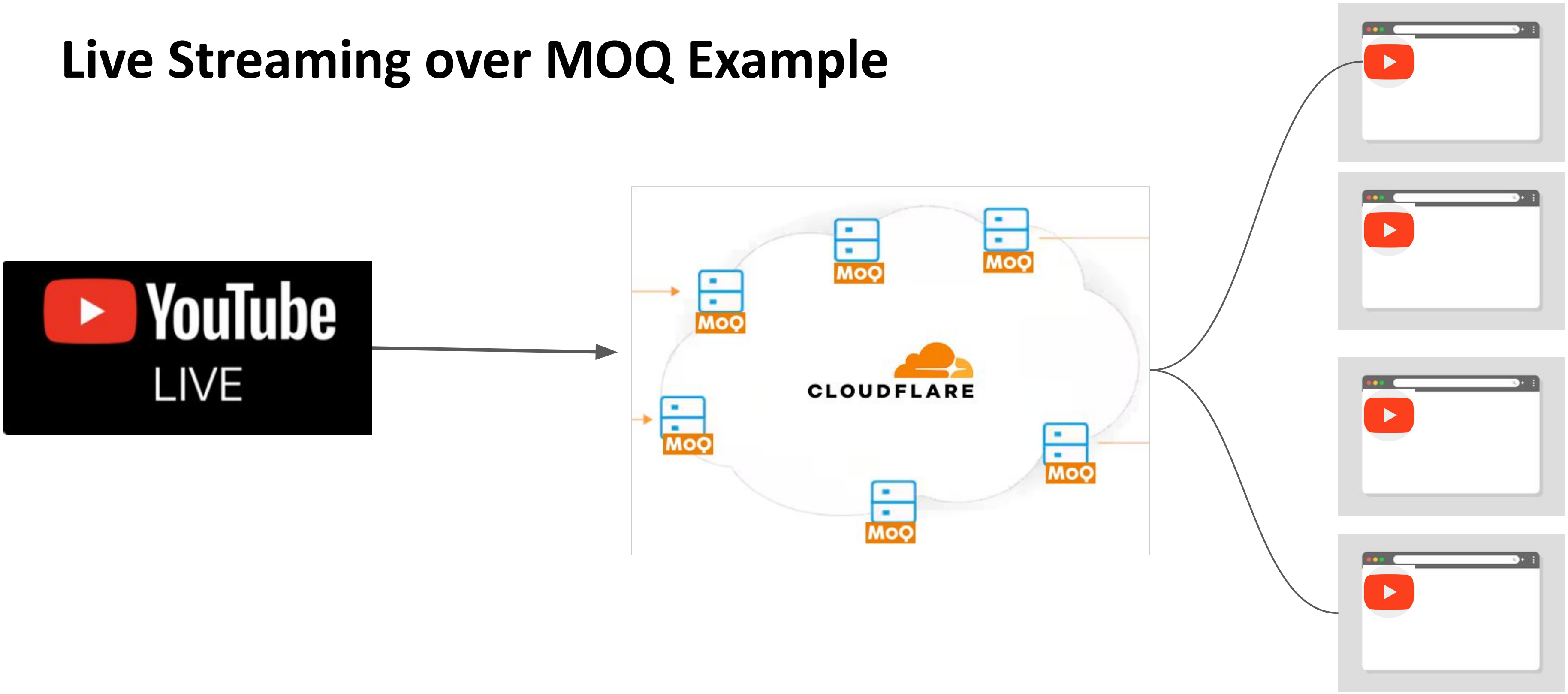
Media over QUIC (MOQ) provides **low-latency, pub/sub-based, highly scalable, cache-friendly transport** for applications such live streaming, real-time conferences, video on demand, cybersecurity event distribution, and many more.

It enables the rapid transport of data using a network of MOQ relays installed along the transport chain.

Built on top of QUIC for enhanced performance

Supports plug-in authorization framework via tokens

Live Streaming over MOQ Example



Content Provider
(MOQ Publisher)

CDN
(MOQ Relay Infrastructure)

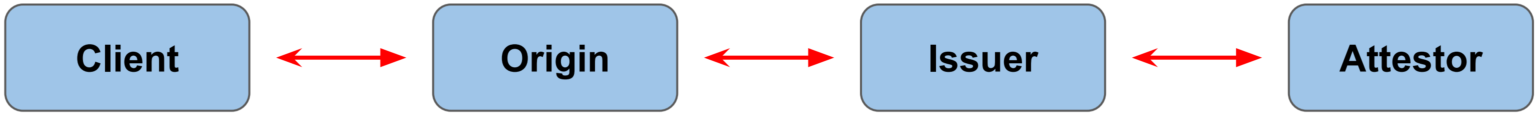
Cliets
(MOQ Subscribers)

Privacy Pass

Privacy-preserving authorization architecture enabling anonymous authentication

Uses unlinkable tokens to protect user privacy

Defined in RFC 9576 with issuance protocols in RFC 9579



Requests access and presents tokens

Resource server requiring authorization

Creates and issues privacy pass tokens

Verifies client's eligibility for token issuance

Privacy Pass benefits for MOQ applications

Privacy protection

1. User viewing patterns remain private
2. Content preference protection through unlinkable tokens
3. Anonymous authentication for media consumption

Fine-grained access

1. Namespace-based authorization controls access for specific content
2. Operation-specific tokens
3. Track-level granularity

Security enhancements

1. Replay protection
2. Time bounded token expiration with strong cryptographic validation
3. Separation of concerns between issuer and the relay

Trust model benefits

1. Issuer-attester non collusion
2. Distributed validation (Relays can validate locally)
3. Policy enforcement consistently across the network

Proposed use

Supported token types

1. **Publicly verifiable tokens**
   a. Blind RSA for distributed validation across relays

2. **Privately verifiable tokens**
   a. VOPRF P-384, SHA-384 for origin as issuer deployments
   b. VOPRF ristretto 255 for batched issuance support
   c. ARC P-46 for anonymous rate limiting credentials

Token integration points

1. **Connection-level authorization**

   SETUP { Version = 1, Parameters = [{ Type = AUTHORIZATION, Value = base64url(PrivateTokenAuth) }] }

2. **Operation-level authorization**

   SUBSCRIBE { Track_Namespace = "sports.example.com/live/soccer", Track_Name = "video", Parameters = [{ Type = AUTHORIZATION, Value = base64url(PrivateTokenAuth) }] }

Deployment models (1) - Separate relay and issuer

```
+-----------+              +--------+         +----------+ +--------+
| MoQ Relay |              | Client |         | Attester | | Issuer |
+-----+-----+              +---+----+         +----+-----+ +---+----+
      |                        |                   |           |
      |<------ Request ------+                   |           |
      +--- TokenChallenge -->|                   |           |
      |                      |<== Attestation ==>|           |
      |                      |                   |           |
      |                      +--------- TokenRequest ------->|
      |                      |<-------- TokenResponse -------+
      |<--- Request+Token ---+                   |           |
      |                      |                   |           |
```

Deployment models (2) - Shared origin-attestor-issuer with reverse flow

```
+--------------------------------------.                           +----------------------------------.
|  +----------------+ +-------------+   |          +---------+      |  +------------+ +----------+   |
|  | Origin Issuer  | | MoQ Relay   |   |          | Client  |      |  | Attester   | | Issuer   |   |
|  +---+------------+ +------+------+   |          +---+-----+      |  +----+-------+ +---+------+   |
 `-----|---------------------|---------'               |             `-------|------------|-------'
       |                     |                         |                     |            |
       |                     |                         |<--------- TokenResponse --------+
       |                     |<----- Request     ------+                     |            |
       |                     |      +Token             |                     |            |
       |                     |      +TokenRequest0     |                     |            |
       |<- TokenRequest0 ---+                          |                     |            |
       +- TokenResponse0 ->|                           |                     |            |
       |                    +------ Response      -->|                     |            |
       |                     |      +TokenResponse0    |                     |            |
```

Changes summary

Major updates:

1. Added new co-author Thibault Meunir (Cloudflare, Inc)
2. Reverse flow support for deployment and scale friendly token acquisition

Architectural enhancements:

1. Shared origin-attestor-issuer flow for MOQ relays to participate in token issuance for MOQ operations, thus improving scalability
2. Privately verifiable token support
3. Bootstrap mechanism for improved token exchange from public to private verification

Scalability Enhancements:

1. Amortized token issuance via batched issuance for improving streaming performance
2. Local validation reducing the dependency on the issuer for token verification
3. TokenRequest0/TokenResponse0 for reverse flow credential exchange