MoQ
Auth Design Team Update

Mike English (Cloudflare)
2026-07-20
IETF 126, Vienna, AT

Auth Design Team - Contributors

- Cullen Jennings
- Manu Gupta
- Suhas Nandakumar
- Aman Sharma
- Manish

wsg:

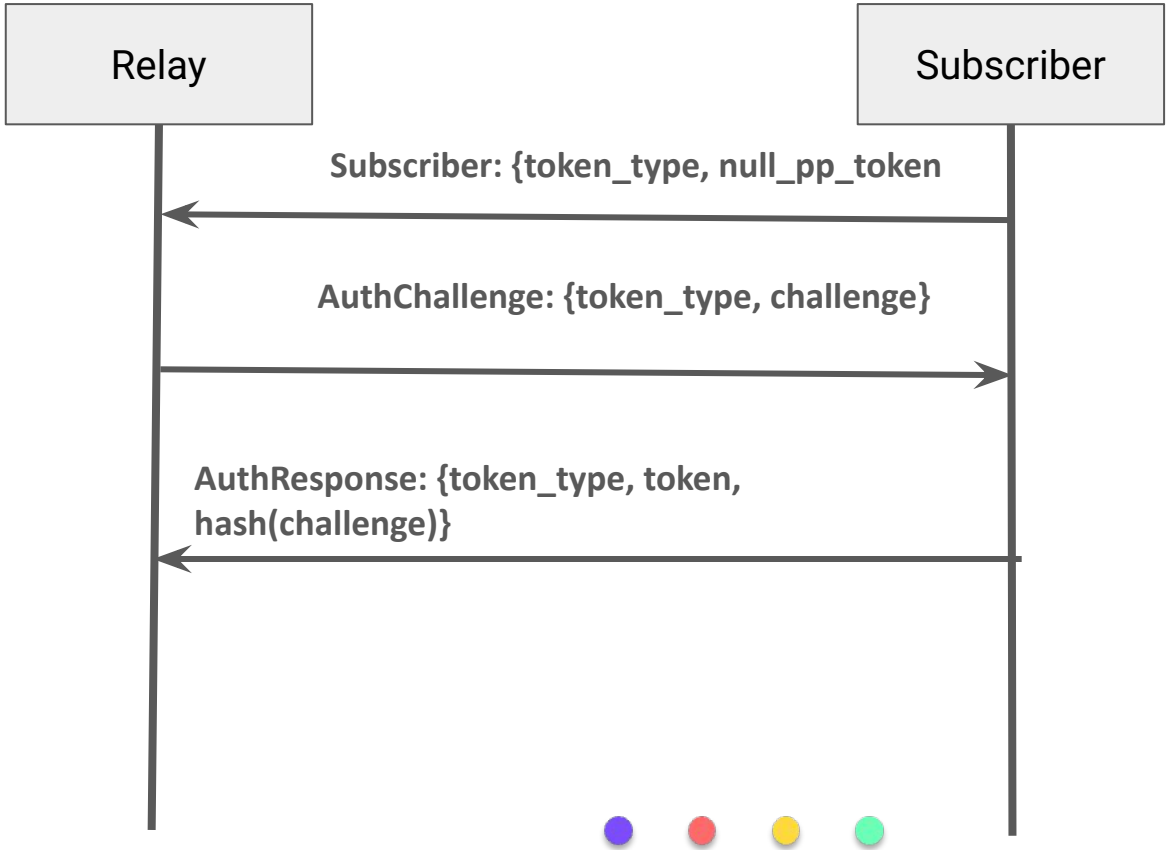
- Joe Lin
- Thibault Meunier

Auth Design Team - charter/scope

- Three main topics, aiming to have solutions by October interim:
  - Challenge mechanism for Privacy Pass
  - Aggregated subscription authorization
  - Relay-to-relay authorization

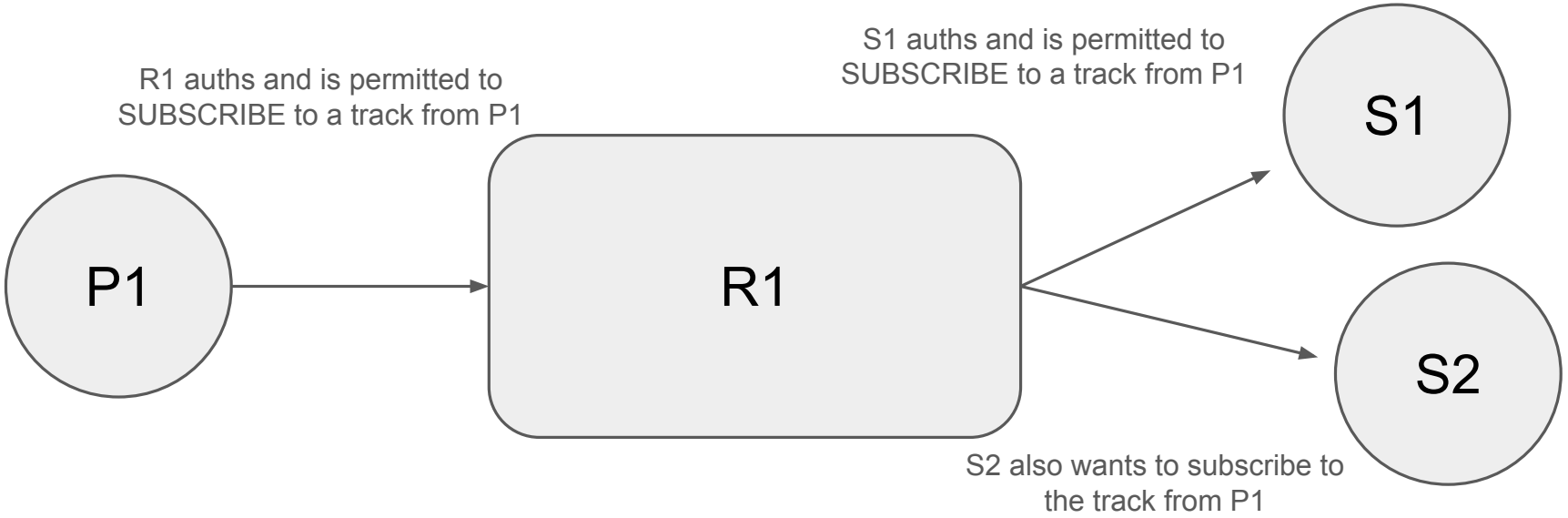
- 9 open issues tagged “Auth” on the base moq-transport draft:
  - #1658, #1662, #1685, #1688, #1737, #1740, #1744, #969, #968

Proof-of-Possession, not just bearer tokens



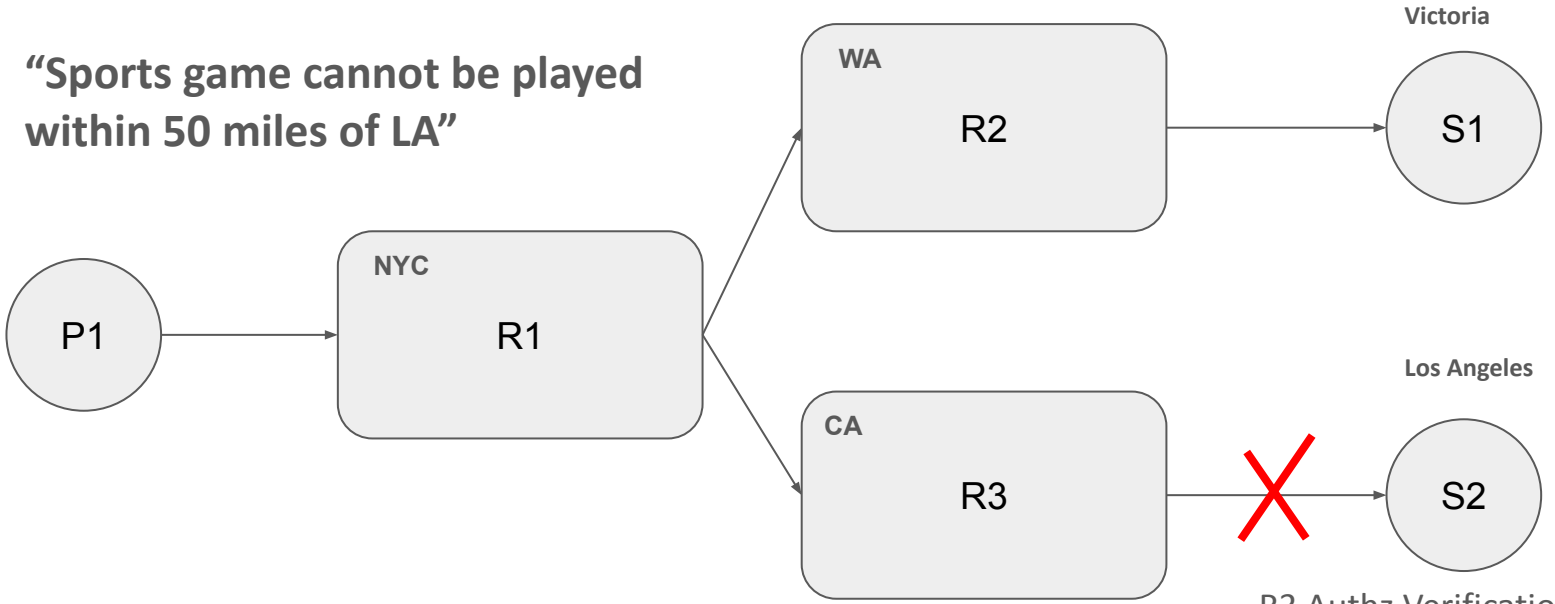
#1688, #1740

Aggregation Challenges



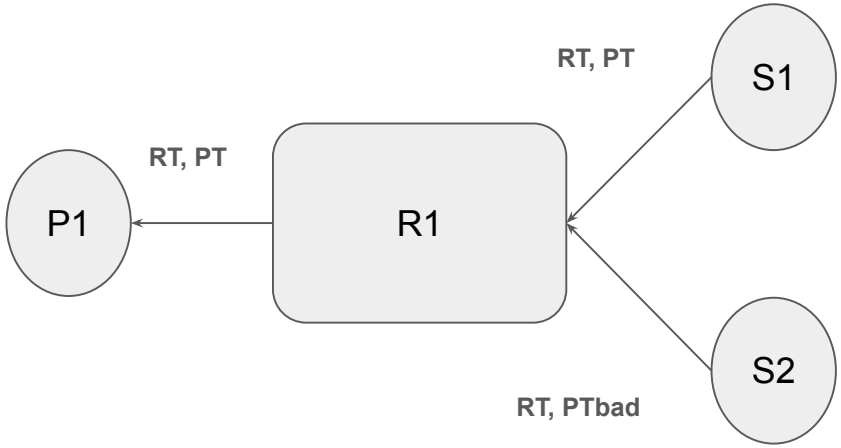
Broadcast scenarios & delegation

“Sports game cannot be played within 50 miles of LA”



R3 Authz Verification blocks the content to S2

Aggregate Subscription Authorization



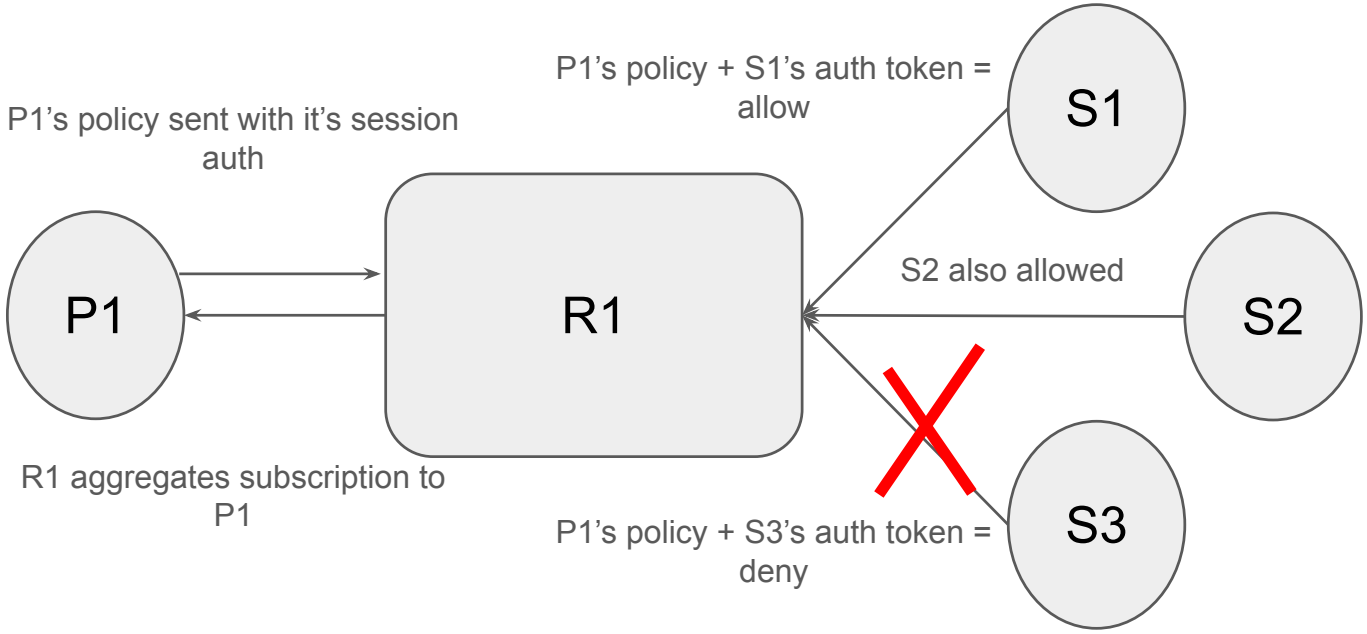
Problem

- S1 subscribe with a RT and PT. RT provided access to Relays. PT provides access to P1.
- S2 subscribe with a RT and Invalid PT.
- By default R1 would aggregate and give media to S2 without checking PTbad.

Proposal:

- Allow R1 to send a new “Auth” message to P1 to validate PTbad for some percentage of subscribes it aggregates.
- Have a way for the PT token to set that percentage with 0% and 100% allowed.

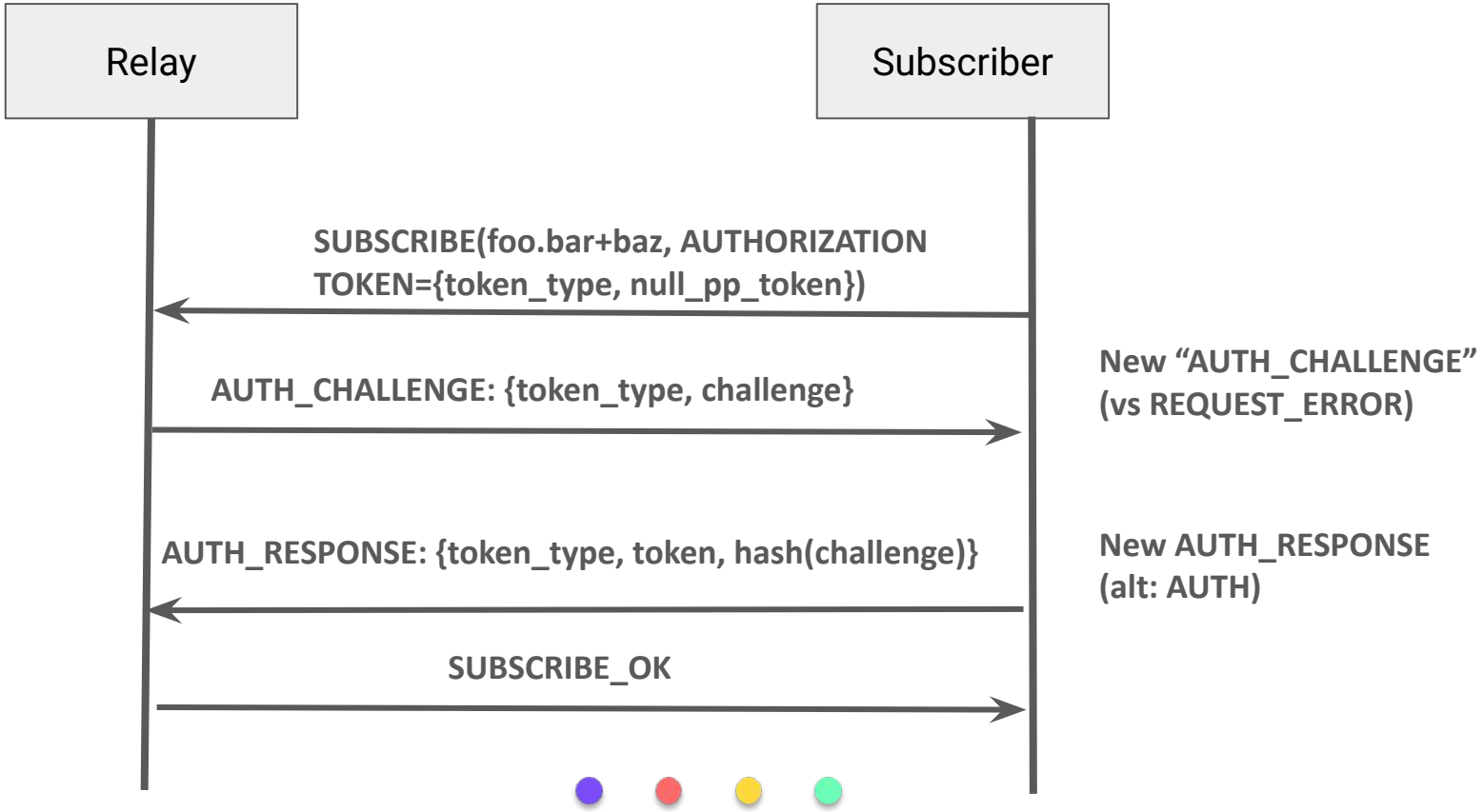
Third way? Publisher-Provided Policy



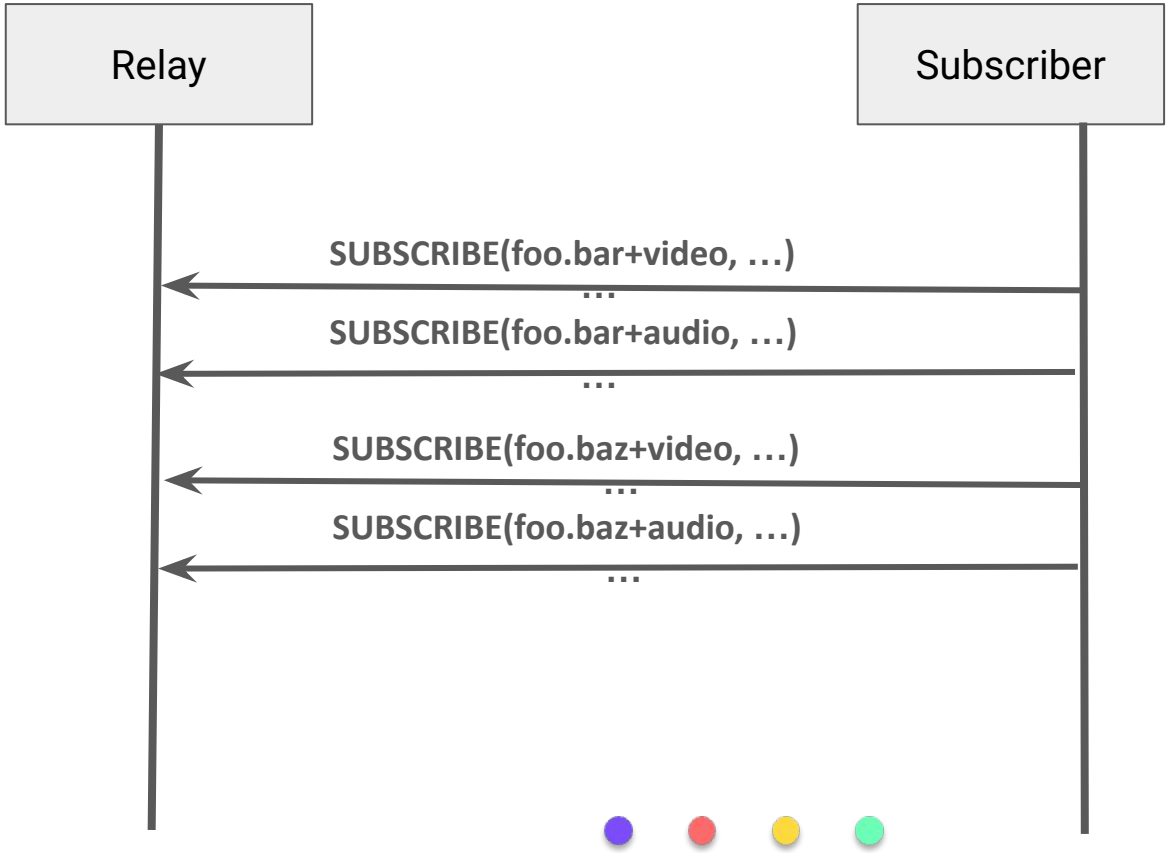
Protocol Implications

- AUTH_TOKEN is hop-by-hop (SETUP Option / Message Parameter)
- (Only properties are currently end-to-end)
- If Original Publisher needs to validate End Subscribers, it implies a requirement to relay auth in ways we don't currently specify
- Additionally, aggregated SUBSCRIBEs imply a potential need for a separate message to handle relaying additional auth validation (keep auth alias? #969)
- We do need a spelling for Request/Challenge/Response exchange
- We think this is a generic pattern usable across token types
- Some potential ordering issues to resolve, we think these are solvable

Example: Auth on SUBSCRIBE



Example: Auth on SUBSCRIBE



Auth for each SUBSCRIBE?
Or shared reusable alias?
Or session-level auth in SETUP?

Proposed MoQT Protocol Changes

1. Should we add auth challenge+response messages? (yes - how to spell?)
2. Should we add a way for relays to statistically validate upstream tokens (for aggregation) (maybe?)
3. Should we specify types of scopes that need to be supported (in C4M, P4M)? (yes - e.g. for multi-CDN token sharing)
4. Should we specify authorization on data plane and control plane? (yes?)