

# MASQUE Implementation

Status Update: 21Mar22



# Reminder

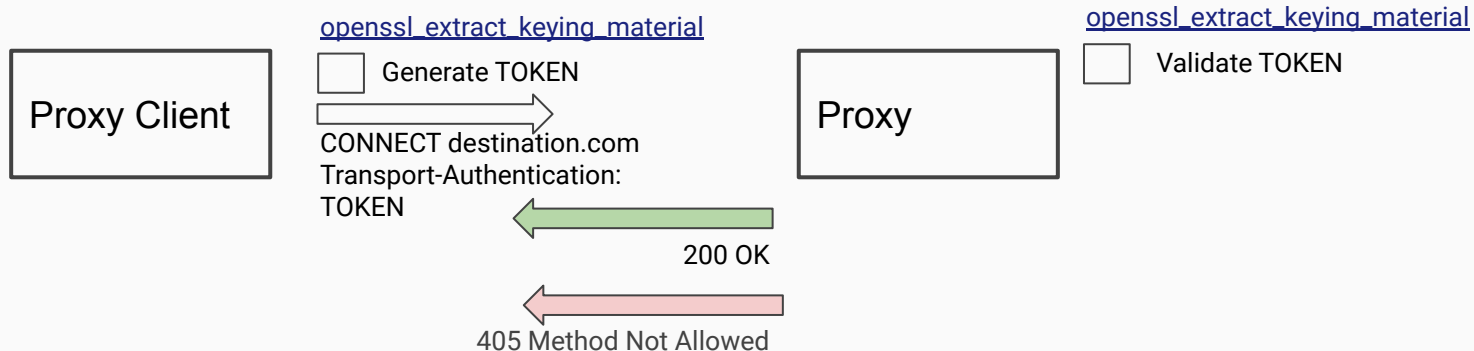
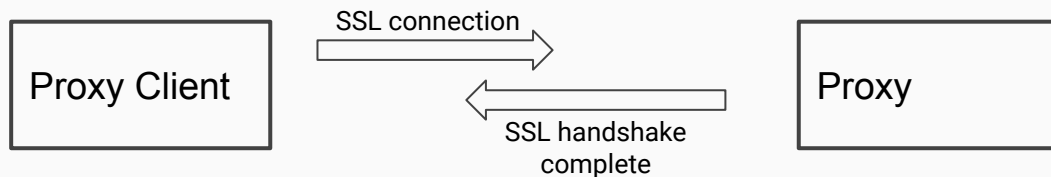
- MASQUE: Multiplexed Application Substrate over QUIC Encryption
  - Started small (“generalized VPN”), got big (“defining future modes of IP Transport Layer proxying”)
    - “Multiplexed” meaning “diverse services gathered within a generalized resource”
- IETF Working Group chartered to pursue requirements definition and specific mechanisms to implement requirements
  - Use cases of interest to Human Rights and Internet Freedom included in requirements definition

# HTTP Transport Authentication

- The “rump stub” of the original MASQUE
- Proposed enhancement to HTTP CONNECT method, authenticating the TRANSPORT not the REQUEST
  - Consonant with unique semantics of the CONNECT method
  - Reuses existing authentication schemes (e.g. “user/password”) and supports extension/addition of others
  - Fails “silently” (issuing standard 405 Method Not Allowed response code) to discourage active probing

Standards document: [draft-schinazi-httpbis-transport-auth-05](#)

# HTTP Transport Authentication



# Implementation Status

- At IETF113 Hackathon (Vienna, March 2022)
  - Completed an initial implementation of HTTP Transport Authentication using HMAC
  - open-source fork of Google Conscrypt stack
  - Vagrant-based demonstration
  - Published to [GitLab](#)