Workload Identifier Origin Hint

`draft-rosomakho-tls-wimse-cert-hint-01`

Yaroslav Rosomakho

Jonathan Hoyland

TLS

IETF125, March 2026, Shenzhen

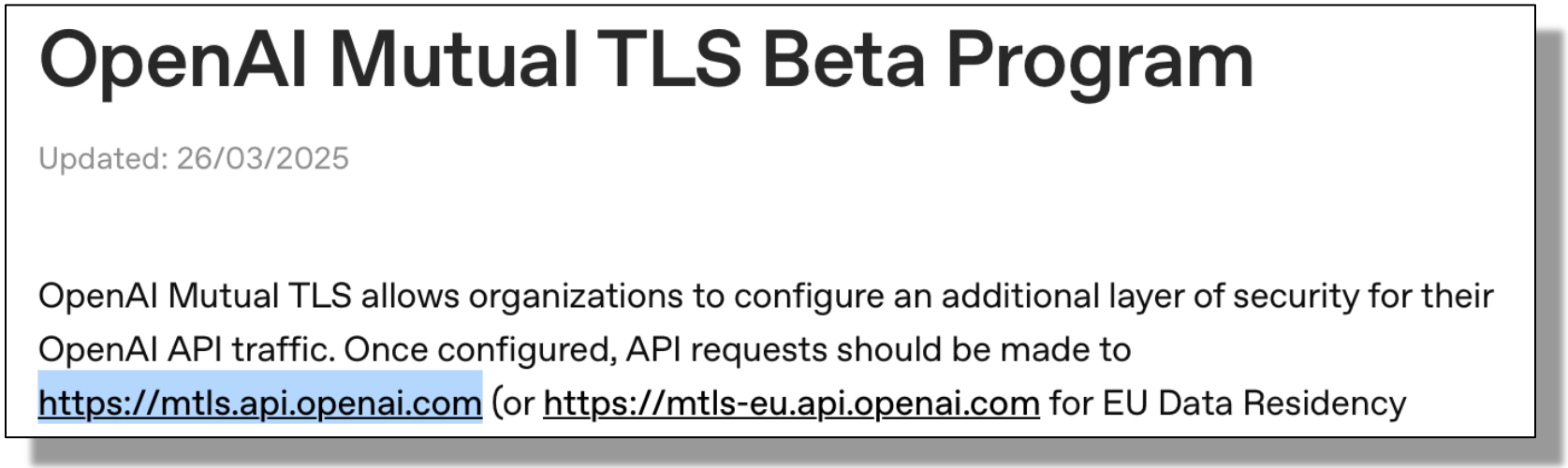
mTLS is awesome

- For bots
- For workloads
- For certain proxies
- For OT/IoT

- But not for user facing web browsers

No easy way to enable mTLS

- Typically, separate TLS server endpoint is required



OpenAI Mutual TLS Beta Program

Updated: 26/03/2025

OpenAI Mutual TLS allows organizations to configure an additional layer of security for their OpenAI API traffic. Once configured, API requests should be made to https://mtls.api.openai.com (or https://mtls-eu.api.openai.com for EU Data Residency

WIMSE workload identifier

An absolute URI

The proposed TLS ClientHello extension

- Contains optional list of workload identifier origins
- Presence of extension indicates that:
  - Client will not freak out from CertificateRequest
  - Client can provide a Certificate for any of listed workload identifier origins
- Server may use the hint in other implementation-specific ways

But if my workload identifier origins need privacy?

- Empty list is valid
  - With empty list this mechanism essentially becomes request mTLS flag
- ECH is a privacy friend
- Approaches could be combined
  - Empty list in Outer ClientHello
  - List of Workload Identifier Origins in Inner ClientHello

Thank you!

Is this something of interest for the working group?