Mutual X.509 Transport Layer Security (TLS) Authentication for OAuth Clients

Brian Campbell
John Bradley

IETF 97
Seoul
November 2016

https://tools.ietf.org/html/draft-campbell-oauth-tls-client-auth-00

What is it?

- Mutual TLS client authentication for OAuth 2.0

Why Bother?

- Mutual TLS client authentication is something that's been done in practice for OAuth but we've never had a spec for it
- At the request of the OpenID Foundation Financial Services API (FAPI) Working Group
  - Banks want to use it for some server to server API use cases being driven by new open banking regulation

How it Works

- TLS connection from client to token endpoint is established or reestablished with mutual X509 certificate authentication
- Client includes the "client_id" HTTP request parameter in all requests to the token endpoint
- Trust model intentionally left open
  - Subject DN
  - Subject public key
- “tls_client_auth” token endpoint authentication method for use with registration and AS metadata

Initial ~~complaints~~ Feedback

- Be more explicit about requiring some certificate to client binding?
  - Sure
- Can client_id be optional?
  - No.
  - Favor protocol consistency over minor & occasional space savings and awkward conditional text
- More metadata
  - to advertise supported binding type(s):
    - tls_client_auth_bind_method(s):
  - and register credentials?
    - jwks_uri & jwks (already exist)
    - tls_client_auth_subject_dn
    - Other?
- More examples and guidance
  - Okay

Next Steps?

- Adopt as a WG document?
  - Read/review (it's relatively short)
    - https://tools.ietf.org/html/draft-campbell-oauth-tls-client-auth-00
  - Find consensus on feedback and update draft
- Let FAPI define it?
- Other…?