OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens

Brian Campbell

IETF 103, Bangkok

November 2018

Context & Overview

- Why?
  - Enhanced security for OAuth 2.0 based on TLS client certificates
    - Draft is already being used by OpenBanking/PSD2esque regulatory regimes and other SDOs
- What?
  - Asymmetric key based client authentication to the AS using mutual TLS
    - Two methods:
      - PKI based mode using subject DN
      - Self-signed certificate mode
  - Mutual TLS certificate bound access tokens for proof-of-possession protected resources access
    - “`x5t#S256`”: X.509 Certificate SHA-256 Thumbprint Confirmation Method for JWT and Introspection

Happenings since IETF 102 Montreal

- WGLC was already done!
- Shepherd write up done
- -10: use RFC 8414 for AS Metadata reference
- -11: Mention/reference TLS 1.3 RFC8446 in the TLS Versions and Best Practices section
- Developer feedback [off list]
- -12: Add an example certificate, JWK, and confirmation method claim + editorial updates based on the above
- And then more feedback…
- And yesterday the AD review…

Sans SAN Support

(**S**ubject **A**lternative **N**ame)

- Apparently all the cool kids are using SANs rather than Subject DNs nowadays (and not just for HTTPS server certs)
- It's been suggested that the usefulness and the useful life of the MTLS draft could be greatly expanded by supporting subject alternative names in the PKI client auth mode
  - One specific request was for a URI SAN
- What's an editor and WG to do?
  - Tell them kids to get off my lawn?
  - Add new client metadata(s) in support of SAN value? (note that there are different types)
  - Allow existing client metadata value to convey the expected subject DN or SAN value?
    - The current name would be a bit awkward: tls_client_auth_subject_dn
    - Potential security implications
  - Change existing client metadata name and allow it to convey the expected subject DN or SAN value?
    - would be a breaking change
    - Same potential security implications
  - Something else?
- Would really really prefer to avoid introducing breaking changes…

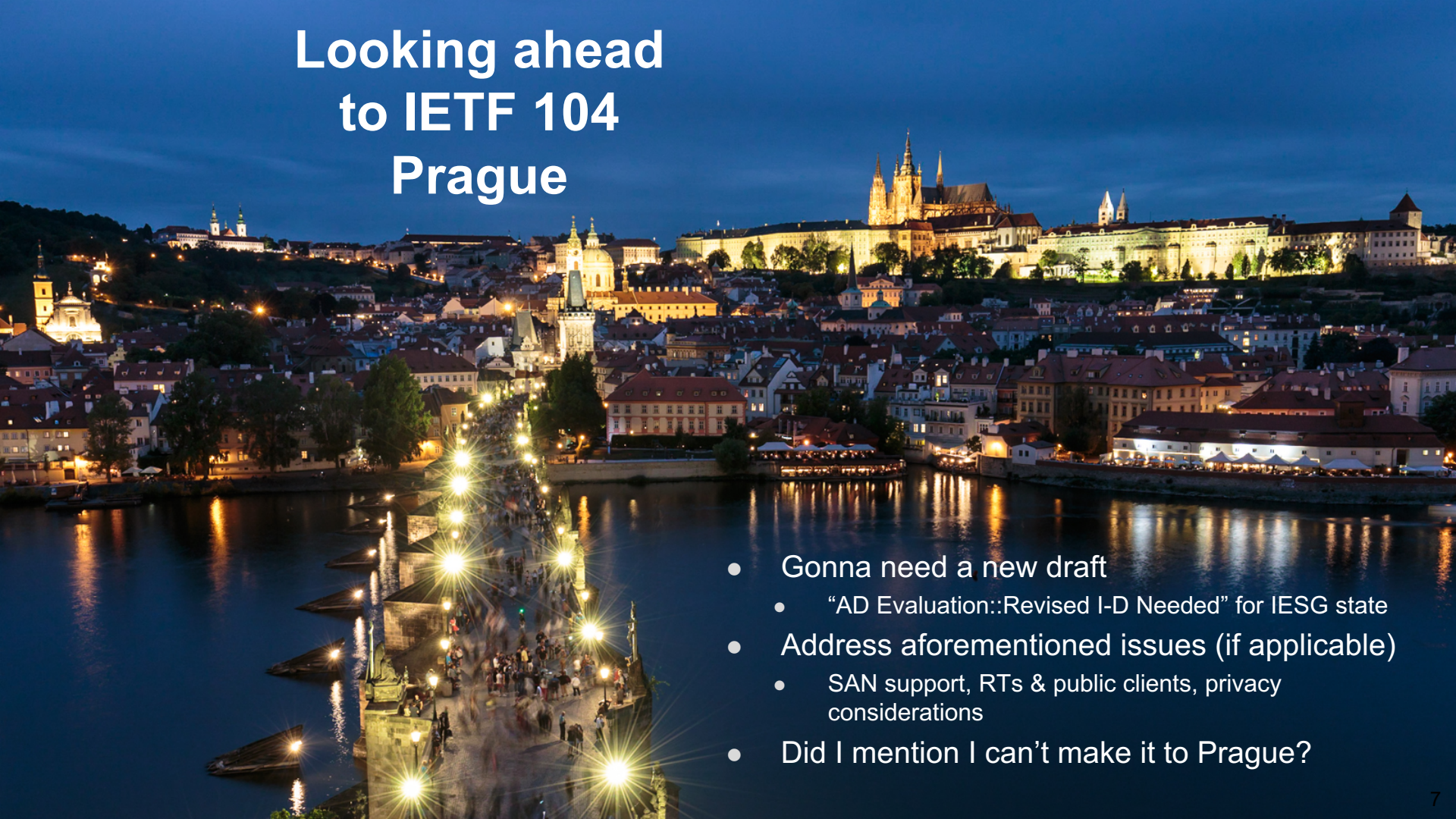
Public Clients and Refresh Tokens

- Draft currently describes how to do certificate bound access tokens with public clients
  - (maybe needs more better explanation)
- It's been suggested that it'd be useful to describe certificate binding refresh tokens for public clients too
- Should we do this?

Considerations to Consider

- TLS client certificates are sent in the clear in versions prior to 1.3
- It's been suggested that some security/privacy considerations be added to OAuth MTLS about that fact
- Do we really need or want this?

Looking ahead to IETF 104 Prague



- Gonna need a new draft
  - “AD Evaluation::Revised I-D Needed” for IESG state
- Address aforementioned issues (if applicable)
  - SAN support, RTs & public clients, privacy considerations
- Did I mention I can’t make it to Prague?