Federated TLS Authentication (FedTLS)

https://datatracker.ietf.org/doc/draft-halen-fed-tls-auth

Jakob Schlyter, Stefan Halén

What is FedTLS

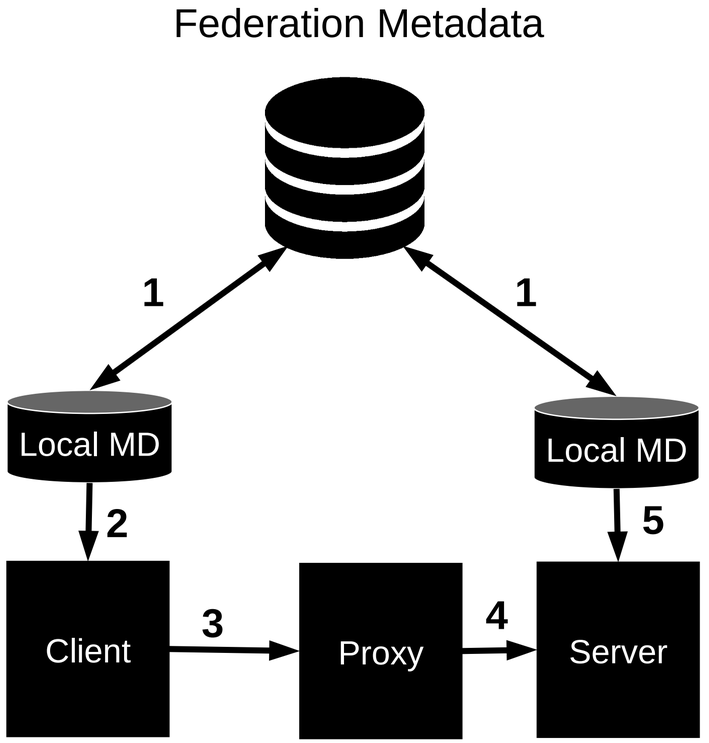
- Federated machine-to-machine authentication
- Mutual TLS Authentication
- Federation Metadata

Background

- Federations for the school sector and the health sector
- Need for secure data transfer
- Open standards
- Open Source implementations:
  - https://github.com/Sambruk/EgilSCIM
  - https://github.com/joesiltberg/bowness
  - https://github.com/Sambruk/windermere

Example

1. Entities collect member metadata from the federation metadata
2. The client pins the server's public key pins
3. The client establishes a connection with the server using the base_uri from the federation metadata
4. The proxy terminates the TLS session either by populating list of trusted CAs using all entities' published issuers, or configure optional untrusted TLS client certificate authentication (e.g., optional_no_ca). The proxy then forwards the client certificate to the server application
5. The application converts the public key to a pin and checks the federation metadata for a match



Dispatching?

- WG
- AD sponsorship
- ISE