Automatic Certificate Management Environment with OpenID Federation 1.0

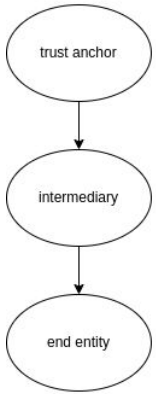
Tim Geoghegan

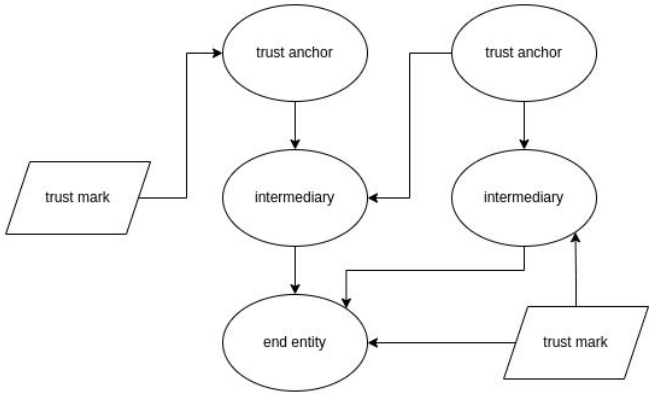
ACME - IETF 124 Montreal

November 4, 2025

OpenID Federation 1.0

- OpenID Federation is a way to build identity federations at scale
- A PKI with multiple overlapping hierarchies, flexible entity metadata and policy via trust marks





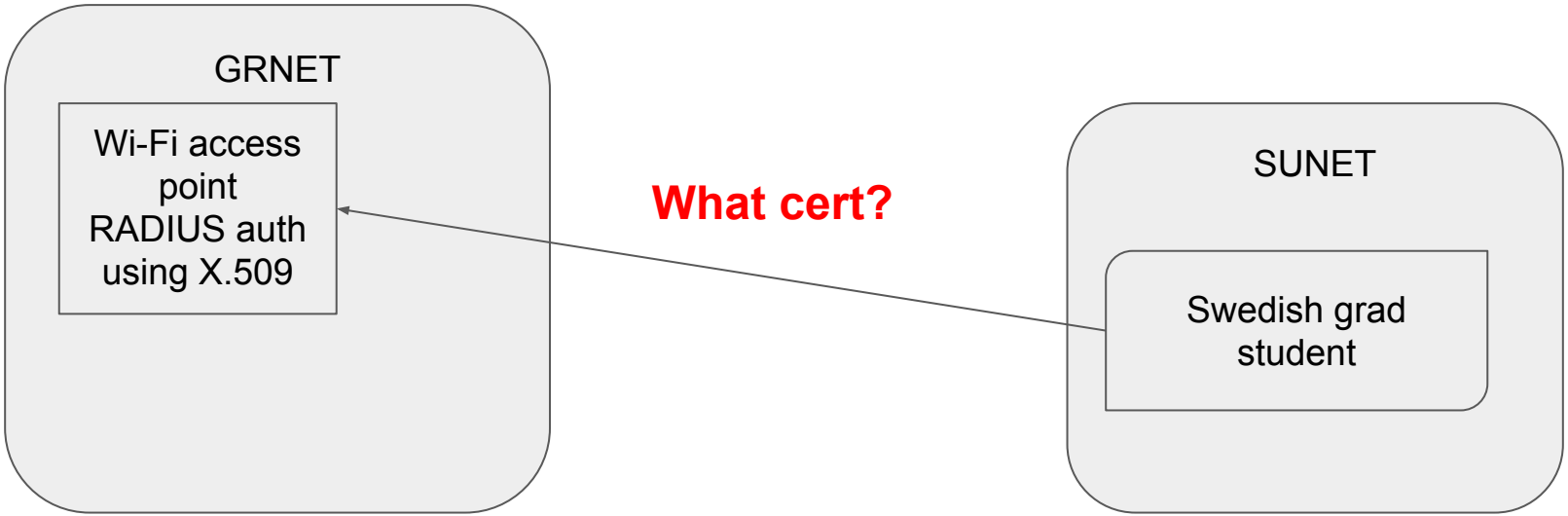
OpenID Federation 1.0 vs. X.509 PKI: a loose analogy

- JWTs instead of RFC 5280 certificates
- Trust anchor list instead of root certificate store
- Subordinate statement instead of cross-signing

https://openid.net/specs/openid-federation-1_0.html
https://www.youtube.com/watch?v=XjZnDFsXGwE

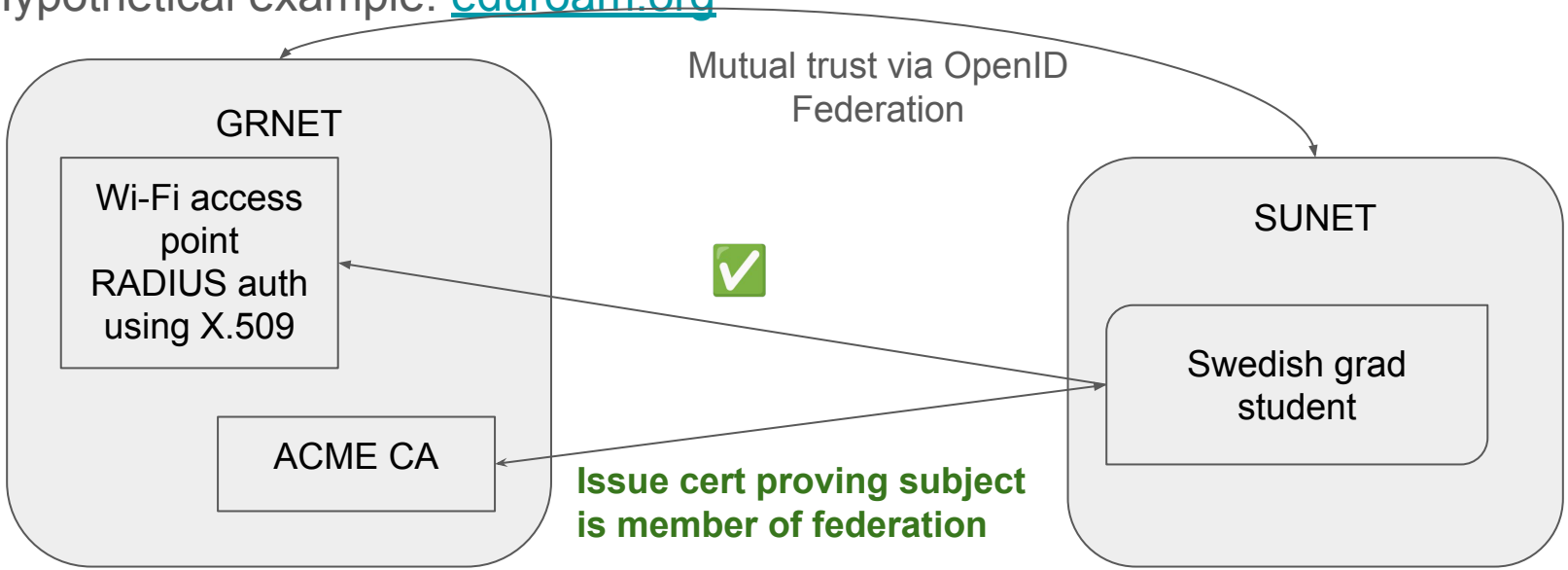
OpenID Federation 1.0 plus X.509 PKI

- Organizations using OpenID Federation to federate trust deploy applications which require X.509 certificates
- Hypothetical example: eduroam.org



OpenID Federation 1.0 plus X.509 PKI

- Organizations using OpenID Federation to federate trust deploy applications which require X.509 certificates
- Hypothetical example: eduroam.org



draft-demarco-acme-openid-federation-01

- Job: issue certificates attesting that subject is a member of an OpenID Federation
- Defines `openid-federation` ACME Identifier Type
- Defines `openid-federation-01` ACME challenge type
- Defines OpenID Federation 1.0 Entity types `acme_issuer` and `acme_requestor`

Changes since draft-demarco-acme-openid-federation-00

- Reorganized document
  - Match layout of RFC 8737
  - Punt ACME and OpenID Federation explanatory material to an appendix
- Stay focused on this draft's job
  - Just an ACME identifier type and challenge mechanism
  - Improve discussion of "discovery"
  - Don't discuss revocation
- Thanks Aaron and Mike for detailed feedback on the list!

Implementation status

- ACME client: https://github.com/abetterinternet/lego-oidf
  - Fork of Lego
- ACME server: https://github.com/abetterinternet/pebble-oidf
  - Fork of Pebble, not usable in production!
- Test harness: https://github.com/abetterinternet/oidf-box

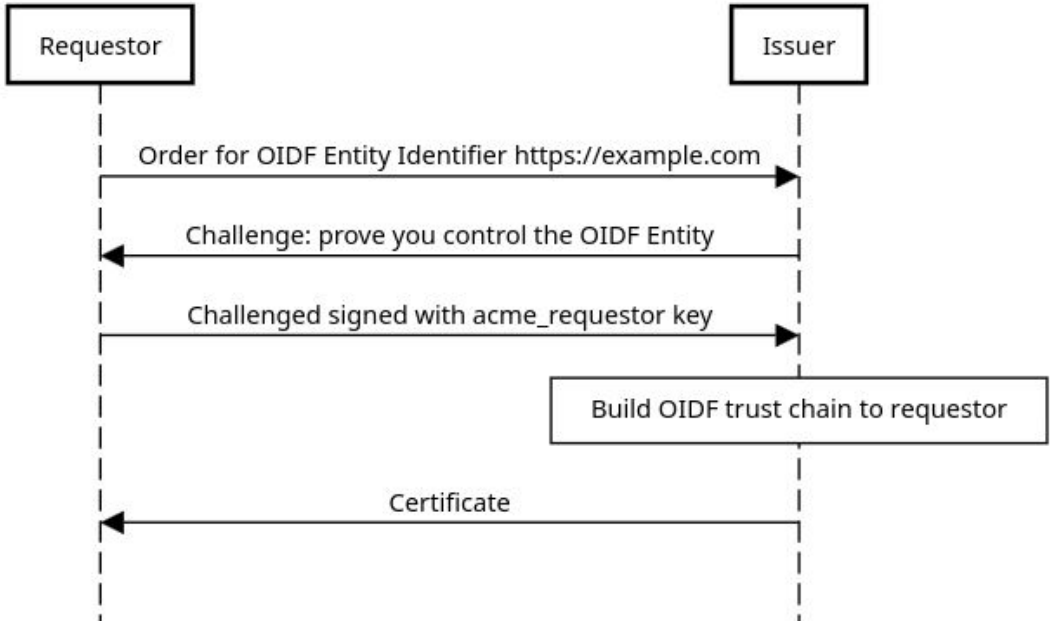
Risks and what’s next

- OpenID Federation 1.0 isn’t finished
  - Entities may not be required to advertise Entity Configuration
  - Discovery mechanisms not finished
  - Mitigation: clear separation of responsibilities
- Editorial improvements

Thanks!

Backup: How does it work?

- Requestor proves control of `acme_requestor` public key
- Issuer verifies that requestor is in trusted federation



Backup: What do the certificates look like?

- Different applications will require different certificate profiles
- draft-demarco-acme-openid-federation-01 adds no new requirements on issued certificates
- We *do* define a new `SubjectAlternativeName` type `id-on-OpenIdFederationEntityId` that issuers MAY use