Federated SCIM AuthN/AuthZ

Jakob Schlyter

kirei

Components

- Metadata
- Authentication
- Authorization

kirei

Metadata

kirei

Metadata via federation

- Publish endpoints and public keys via federation (as JSON/XML)
  - Well known, similar to SAML ID federation
  - Simple to implement for both federation and users (client/server)

kirei

Metadata Contents

- Entity ID
- Endpoint certificate issuers
- Servers
  - List of name, URI and certificate pinning data
- Clients
  - List of name and certificate pinning data

kirei

Authentication

- Via web server or reverse proxy
- Normal PKI client/server authentication
  - May be self-signed or private CA

kirei

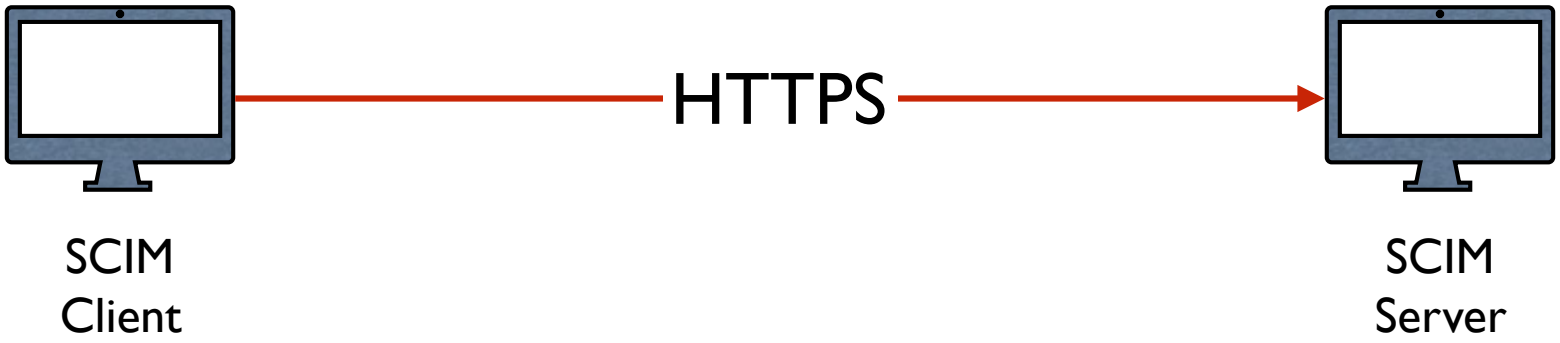
Authorization

- Certificate pinning based on metadata information
  - Public key hash per RFC 7469 (HPKP)
  - Performed by application – not web server

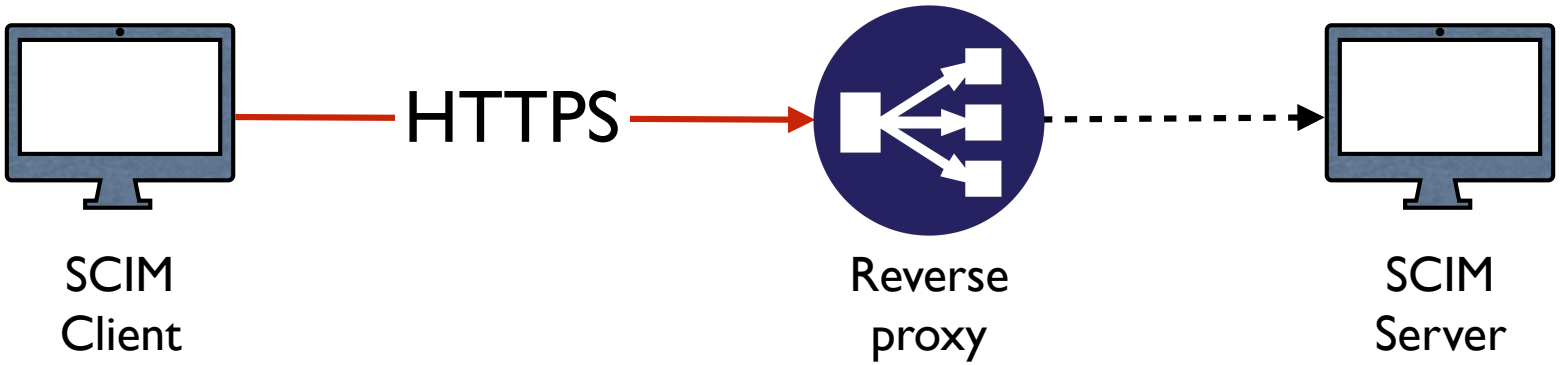
kirei

Deployment Scenarios

kirei



kirei



kirei

https://github.com/kirei/scim-fed-auth

kirei