OAuth Identity and Authorization
Chaining Across Domains

IETF 119 WIMSE Working Group Meeting

Arndt Schwenkschuster (Microsoft)
Pieter Kasselman (Microsoft)
Kelley Burgin, (MITRE)
Mike Jenkins (NSA-CSS)
Brian Campbell (Ping)
Why Identity Chaining Across Trust Domains

Transaction Tokens
- Who was the Resource Owner?
- What authorization did they grant?
- What other entities were involved?
- What authorization did they have?

Image Courtesy Justin Richer (justin@bspk.io)
Why Identity Chaining Across Trust Domains

Client

Authorization Server Domain 1

Gateway

Foo

Bar

Resource Owner

Trust Domain 1

Trust Domain 2

Gateway

Baz

Qux

Image Courtesy Justin Richer (justin@bspk.io)
Why Identity Chaining Across Trust Domains

- Who was the Resource Owner?
- What authorization did they grant?
- What other entities were involved?
- What authorization did they have?
Why Identity Chaining Across Trust Domains

Image Courtesy Justin Richer (justin@bspk.io)
Proposal Concepts
Getting an Authorization Grant for another Trust Domain

1. Client in Domain 1 exchanges a token with the AS in Trust Domain 1 to get an authorization grant for the AS in Trust Domain 2

2. Client uses the authorization grant with the AS in Trust Domain 2 to get an access token

3. Client presents the access token to the Resource server in Trust Domain 2

Token Exchange (RFC 8693)

Assertion Framework (RFC 7521)
Section 2.1 Overview: Generic Identity and Authorization Chaining Across Domains
Appendix B.1: Resource Server acting as Client
Appendix B.2:
Authorization Server acting as Client