WIMSE Architecture

(draft-ietf-wimse-arch-02)

Joe Salowey, Yaroslav Rosomakho , Hannes Tschofenig

Overview

Changes since Last IETF

- Update to Identity and Trust Domain
- Expanded Use Cases:
  - Impersonation
  - Batch Processing

Next Steps

Workload Identity

Composed of

- Trust Domain
- Workload Identifier
- Workload Identity Credentials

* Bootstrapping identity as well, but this section has not changed much

Trust Domain

- A trust domain is a logical grouping of systems that share a common set of security controls and policies.
- Trust domains **SHOULD** be identified by a fully qualified domain name
- A trust domain maps to one or more trust anchors for validating X.509 certificates and a mechanism to securely obtain a JWK Set [RFC7517] for validating WIMSE WIT tokens
- If two identifiers differ only by trust domain they still refer to two different entities.

Workload Identifier

scheme://***trust-domain***/*path*

URI from RFC 5280

- Trust domain as IP address is discouraged
- Path defined by scheme and deployment
- X.509 URI SAN
- WIT ‘sub’ claim

- SPIFFE SVIDs are valid workload identifiers
  - Scheme = spiffe
- Should we define a *wimse* scheme?

Workload Identity Credentials

- X.509
- WIT (S2S work)

- What about identity jwts (bearer)?

Workload Identity Definition in Multiple Documents

Currently in both S2S and Arch Spec

Can we remove from S2S and reference Arch Document?

Expanded Use Cases

New Text for

- Impersonation & Delegation
- Asynchronous and Batch Processing

* Thanks to Ken McCracken

Next steps

1. Terminology & Alignment with other WIMSE Documents (Many Open Issues)
2. Threat Model
3. Authorization & Context (Integration with Transaction Tokens)
4. Cross Domain
5. Expanded use cases (Impersonation, Async, etc)
6. Attestation & Bootstrapping

PRs and Discussion are Welcome

Interim(s)?