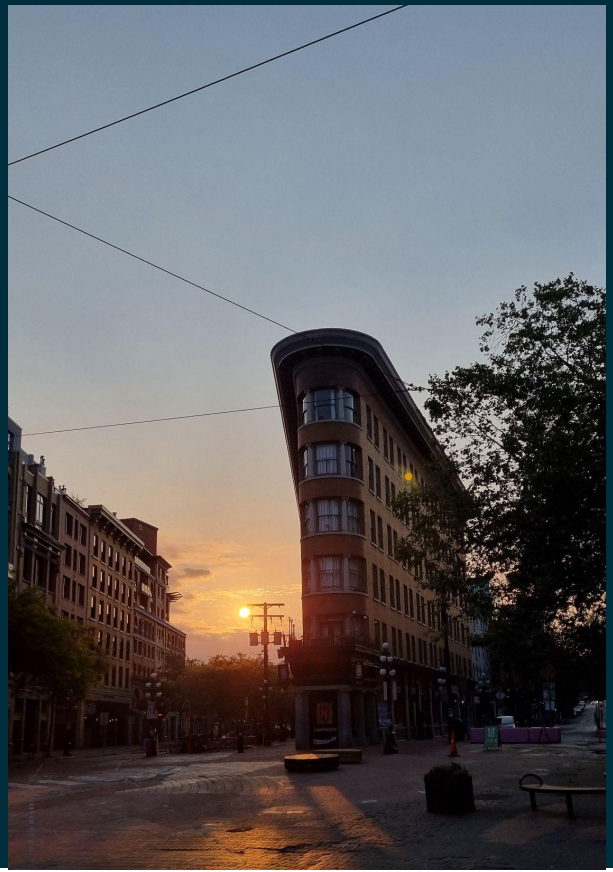

24 July 2024

Workload Identity in a Multi System Environment (WIMSE) Architecture

Hannes, Yaroslav, Joe

Internet Engineering Task Force

Production by Meetecho

IETF

Agenda

- Status Update
- WIMSE Identifier
- Use Cases & Deployment Models

Status

1. Published 00 and 01 since last IETF
2. Added text on workload identity
3. Separated Authentication and Authorization Sections

WIMSE Identity

Current direction from working group

- Avoid general identity Topic
- Focus on WIMSE Identifier

WIMSE Identifier

WIMSE Identifier is URI

- Well Understood - this is what SPIFFE uses
- Well-Defined
- Ways to insert in JWT and X.509

Basic Format:

<scheme>://<trust-domain>/<path>

Same basic format as SPIFFE

Scheme

Allow schemes to be defined?

- Allow registration of schemes for Wimse
- Must define trust domain
- Can it specify the “path” format

“spiffe” ?

- Ties identity to the SPIFFE specifications
- Best chance of interoperability

“wimse” ?

- Provides more flexibility for the working group

Trust Domain

- Defines a namespace and mechanism for verify an identity based on issuers
- Mapping of trust domain to issuer
  - Configuration
  - Discovery
- Specific format?
  - Hostname
  - Must it be “registered
- Trust domain defines Path

Path

Authorization and other use case magic. Up to scheme or trust domain to define. Identifies the important aspects of the identifier

- /<role>/<instance>
- or /<id>
- or /<namespace>/<account>

Use Cases & Deployment Models

Use Cases

- Service Authentication
- Security Context Establishment and Propagation
- Service Authorization
- Delegation and Impersonation **(Needs Text)**
- Asynchronous and Batch Requests **(Needs Text)**
- Cross-boundary Workload Identity
- Attestation **(Not included yet)**

Deployment Models **(Not Discussed Yet)**

- Service Mesh
- API Gateway
- Application Library

Next Steps

- Alignment with Design Team work on Token Translation and Service-to-Service Protocol (as Appropriate)
- Work on use-cases (add or remove?)
- Do deployment models make a difference for the architecture