WIMSE for CCC

YARON SHEFFER, INTUIT

SEP. 2024

Charter

The Workload Identity in Multi-Service Environments (WIMSE) working group is chartered to address the challenges associated with implementing fine-grained, least privilege access control for workloads deployed across multiple service platforms, spanning both public and private clouds.

WIMSE Charter and Plan, approved March 2024

Goals

Identify, articulate, and bridge the gaps and ambiguities in workload identity problems and define solutions across a diverse set of platforms and deployments, building on various protocols used in workload environments. The WG will standardize solutions and document existing or best practices…

In collaboration with:

- Other IETF working groups that address topics related to identity, authentication, and authorization, including, but not limited to, OAuth, SCIM, SCITT, and RATS.
- The Cloud Native Computing Foundation (CNCF), particularly with regard to the SPIFFE/SPIRE project.
- The OpenID Foundation.

WIMSE will also serve as a standing venue to discuss operational experience and requirements with workload identity. These discussions need not be restricted to technologies currently in scope to this charter.

Deliverables

- WIMSE Architecture
- Service to Service Protocol
- Token Issuance with Limited Authority
- Token Exchange

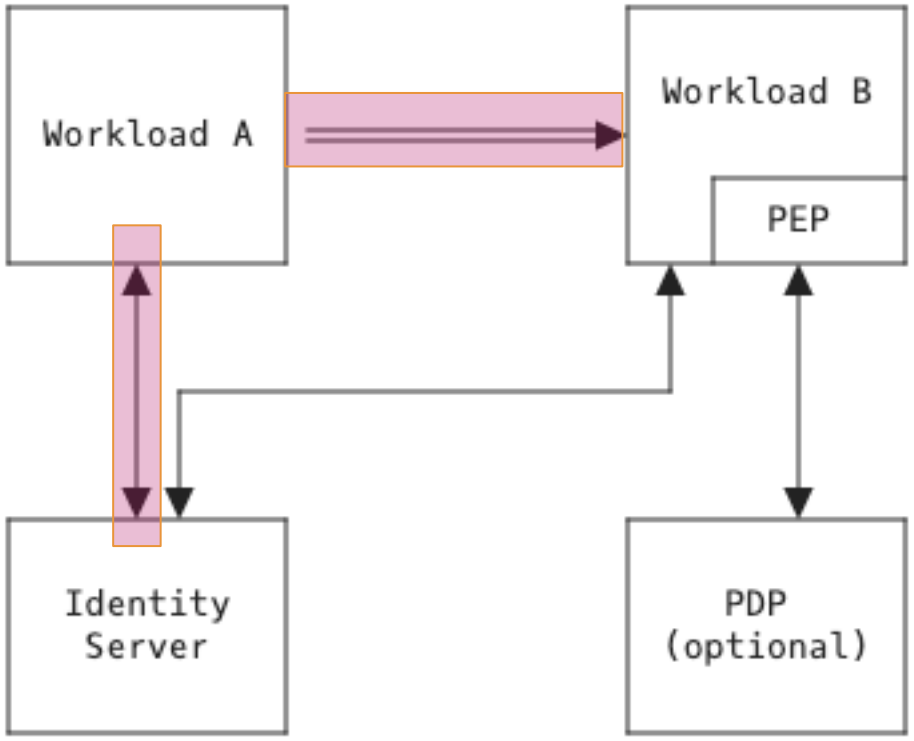
- Token Distribution Best Practices

What are Workloads?

- A workload is a running instance of software executing for a specific purpose
- A workload typically interacts with other parts of a larger system
- A workload may exist for a very short duration of time (fraction of a second) and run for a specific purpose such as to provide a response to an API request
- Other kinds of workloads may execute for a very long duration, such as months or years. Examples include database services and machine learning training jobs

- *From the WIMSE Architecture I-D*

The WIMSE Model



- Workloads receive their credentials (WIMSE Identity Token) from an Identity Server
- The credential contains a public key, which is then used to authenticate the request
  - Bearer tokens are out!
  - Mutual TLS and good old X.509 also supported, with similar security properties
- Small print:
  - The draft is at -00, no implementations yet
  - SPIFFE exists in production, covers credential provisioning, but is not compatible with our tokens

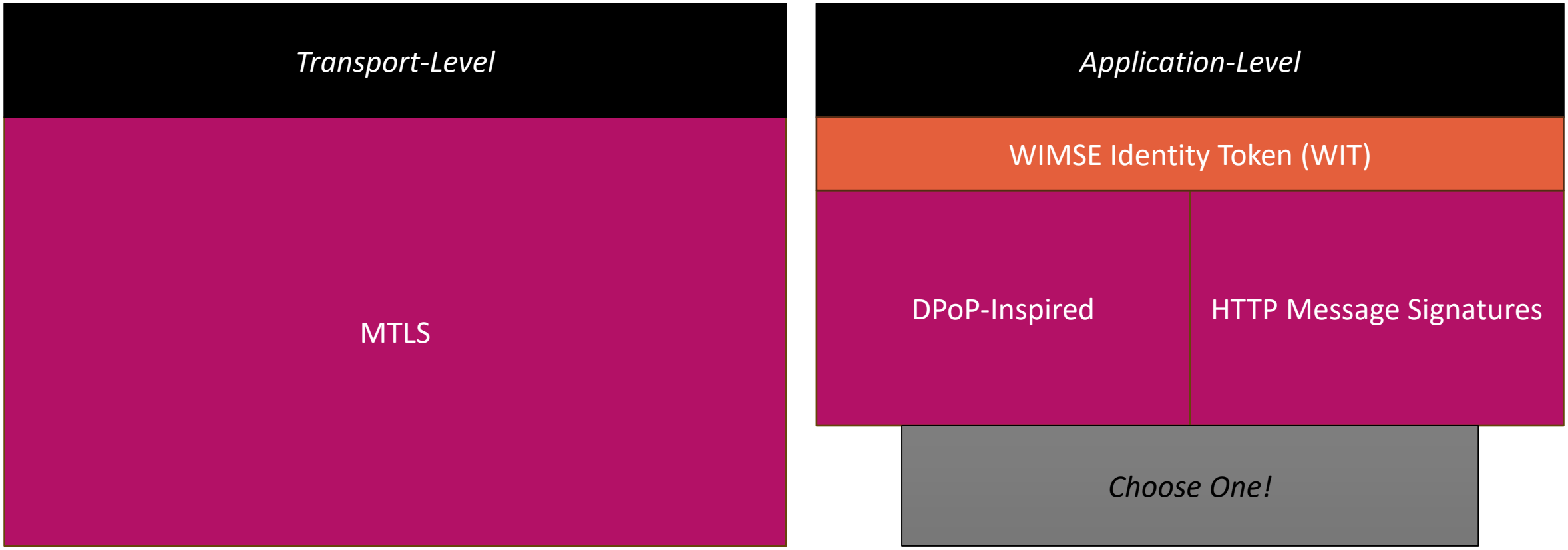
Source: *draft-ietf-wimse-s2s-protocol-00*

Service to Service Protocol

- Workload authentication protocol covering a single hop of the call chain
- Interaction within a single trust domain
- Current focus on HTTP (REST) APIs
- Either Mutual TLS or Token Based, see next slide

- Draft has just been adopted by the WG, expect major changes before publication

Protocol Options



Workload Attestation

- WIMSE Charter: *[the protocol] should support associating context with the token, including but not limited to user identity, platform attestation, and SBOM artifacts*
- The credential provisioning process *could* involve attestation of the workload, or of an associated agent
- The protocol provides additional "context" information that's passed down the call chain, could include attestation evidence

Thank You!

yaron_sheffer@intuit.com