Best Current Practice for Workload Identity

draft-hofmann-wimse-workload-identity-bcp

Benedikt Hofmann, Yaroslav Rosomakho, Edoardo Giordano, Arndt Schwenkschuster, Hannes Tschofenig, Evan Gilman
Status

• Presented draft-hofmann-wimse-workload-identity-bcp at IETF#118.
• Time between IETF#118 and #119 was mostly dedicated to the charter discussions
• Interested parties met to discuss possible enhancements.
  • But not enough time to update the draft in time for the deadline
Short Refresher
Service Account Token Volume Projection

• Workloads are issued service account token
  • These JWTs are time bound
  • These JWTs are issued to each workload
• Less configuration overhead for developers and operators.
• Relies on RFC 7523 “JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants”
• Challenges arise when Authorization Servers are implemented according to OIDC Core
Access Token

Workload Identity Server

Authorization Server

Service Account Token Volume Projection (SATVP)

Token Exchange

Agent

Workload

Resource Server

SATVP

Access Token
Going forward
Questions

• Scope is currently focused on use of JWTs for workload identities.
  +: Narrow focus allows us to finish the work quickly.
  -: Does not consider PoP tokens or X.509 certificates as credentials.

• Proposal to make recommendations regarding the host-local communication with the workload (environment variables, domain sockets, file system).

• Current version good enough as a starting point for work in the group.