Best Current Practice for Workload Identity

draft-hofmann-wimse-workload-identity-bcp-00

Hannes Tschofenig, Benedikt Hofmann

Background

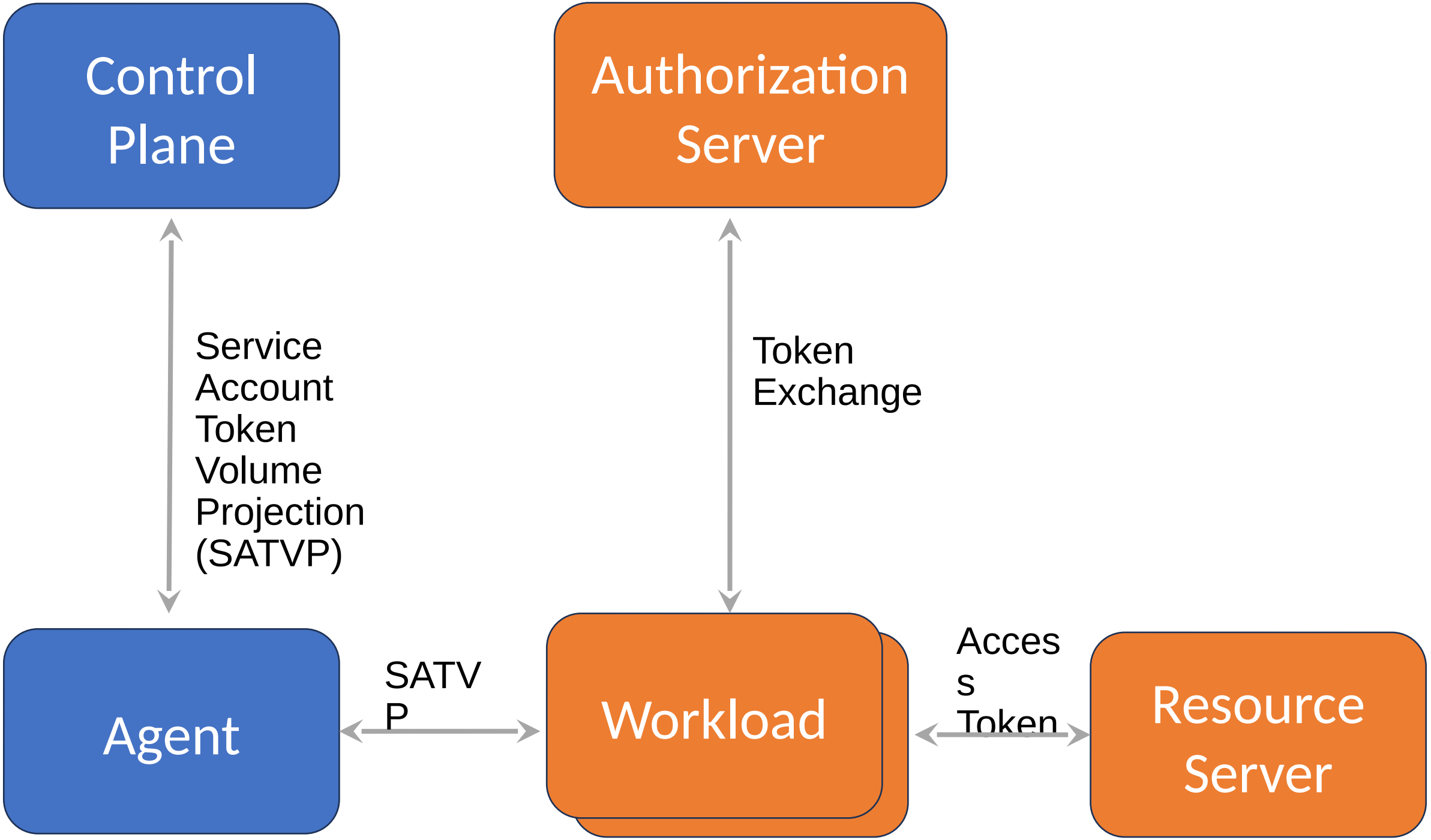
- Workloads in distributed systems often need to access protected resources.
- Often, they are provisioned with *client_id* and *client_secrets*
  - This often requires considerable effort by dev-ops teams
  - Rotating these credentials is often not easy
  - These credentials are not time bound
- Each new workloads needs configuration effort to be issued credentials.

Why not utilize the control plane?

Control plane already issues JWTs to every workload already anyway.

Service Account Token Volume Projection

- Workloads are issued service account token by the control plane
  - These JWTs are time bound
  - These JWTs are issues for each workload
- Only the public key needs to be configured at the AuthorizationSserver
- Less configuration overhead for developers and operators.
- Relies on existing RFC 6749 and RFC 7523


Control Plane
Authorization Server
Service Account Token Volume Projection (SATVP)
Token Exchange
Agent
SATV P
Workload
Acces s Token
Resource Server

Need for Standardization

- Authorization Servers implement RFC 6749 according to OIDC
  - enforce JTI (JWT ID)
  - enforce sub=iss -> does not work out of the box
- Adoption of this best practice motivates providers of ASs to allow this option.
- Adoption of this best practice will lead to increased adoption, which leads to:
  - time bound credentials
  - less secrets to be managed
  - less configuration on the authorization server

Write-up provides initial example of guidance

Guidance will help developers to increase interoperability of identity systems in workload identities.