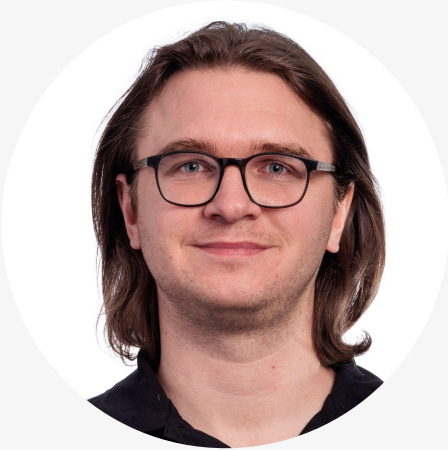
Use OpenShift Tokens to Authenticate With External Services

Adfinis



Lukas Grossar

Sales Engineer

Contact

Adfinis

Bern

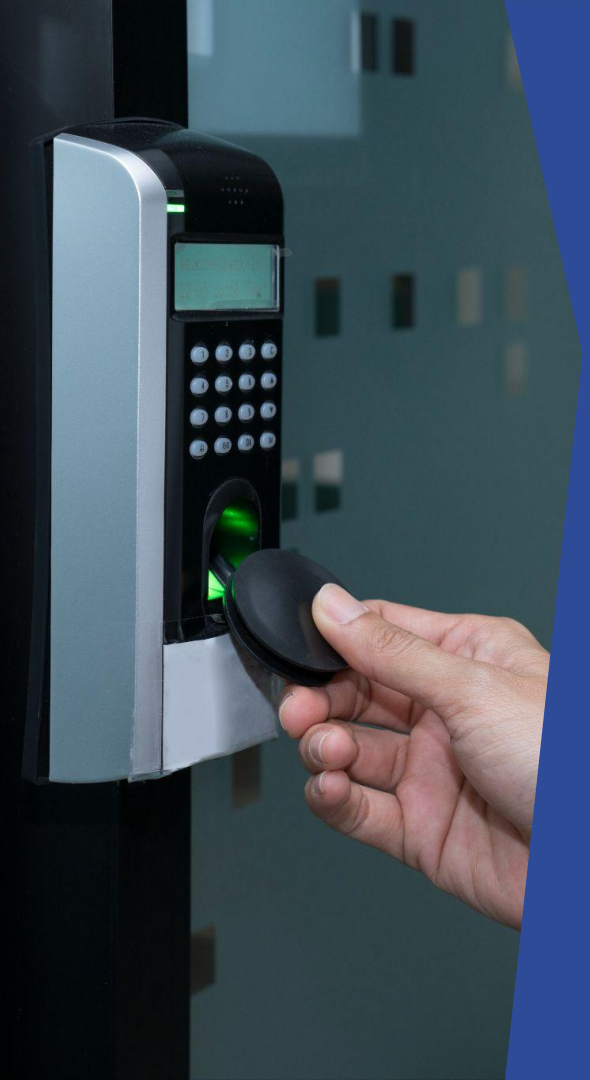
lukas.grossar@adfinis.com

linkedin.com/in/tongpu

github.com/tongpu

My **Goals** for Today

- Introduction to signed ServiceAccount tokens
- Usage of ServiceAccount tokens
- Trust relationships to authenticate with services
- Other areas where this can be used



What is **JWT** and How It Relates to **OIDC**?

JWT is short for **JSON Web Token**, a standard to pass along verifiable information.

JWT **payload** contains **claims**, with information about the JWT **subject**.

OpenID Connect uses JWT for **ID tokens**, which contain claims about user identity.

The JWT payload is **signed** by a private key, to ensure it can't be tampered.

Signed **Service Account** Tokens

Signed Service Account tokens feature **needs to be enabled** to make use of this functionality.

Enabled by default since OpenShift 4.8, which was released four years ago.

Default Service Account token valid for **internal interaction** with the **OpenShift API.**

Integration with external services requires configuration of a **custom audience.**

Authentication with **External Services**

Signed token is sent as **credential** to external services for **authentication**.

External service needs to be configured to **trust** the OIDC provider in OpenShift.

Authorization based on JWT claims, usually using the **subject** (*sub*) claim.

Authorization **configuration** is highly dependent on the external service.

Which Services **Support** This?

AWS: Assume IAM roles with service accounts (**IRSA**).

Authenticate using Azure **Workload Identity.**

Vault/OpenBao: Use JWT or Kubernetes authentication.

Any external API supporting **JWT authentication.**

Other **Areas** to Use JWT and OIDC

ImagePull via SA tokens is in Beta in Kubernetes v1.34 and will replace ImagePullSecrets.

Support for **pod certificates** for encrypted inter-pod comms will be in Beta in Kubernetes v1.35.

Use ID tokens in **GitLab CI** and **GitHub Actions** to authenticate with external services.

Prepare yourself for rollout of **zero trust identities**.

Benefits of JWT Trust

No more secrets need to be managed or passwords need to be rotated.

Tokens are rotated every hour, making **credential theft** less critical.

Authorization is based on **identity claims** in the token.

Questions? Find me at **our booth at S01.**

Start Your **Journey** with **Adfinis**.

Let’s Get in Touch

adfinis.com

info@adfinis.com

/adfinis

/adfinis

Find us at **booth S01**

Adfinis