



29
10/26

HashiConf at IBM TechXchange 2026

Beyond Secret Zero: SPIFFE, Vault, and Platform Trust for Secure AI Workloads



Leon Krass

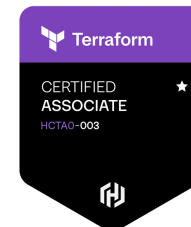
Technical Leader
for HashiCorp Vault

[/ About me](#)

Introduction

Passionate about secrets management and (sometimes over-) engineering IT automation with a touch of Kubernetes, Terraform and/or Ansible magic.

HashiCorp Vault, Kubernetes, Ansible, Terraform



Profile and Corporate Objective

Biggest **owner-operated system integrator** in Germany

Steady growth with more than **3,900 employees** in Germany

We accompany our customers on a **long-term basis** throughout the project lifecycle.



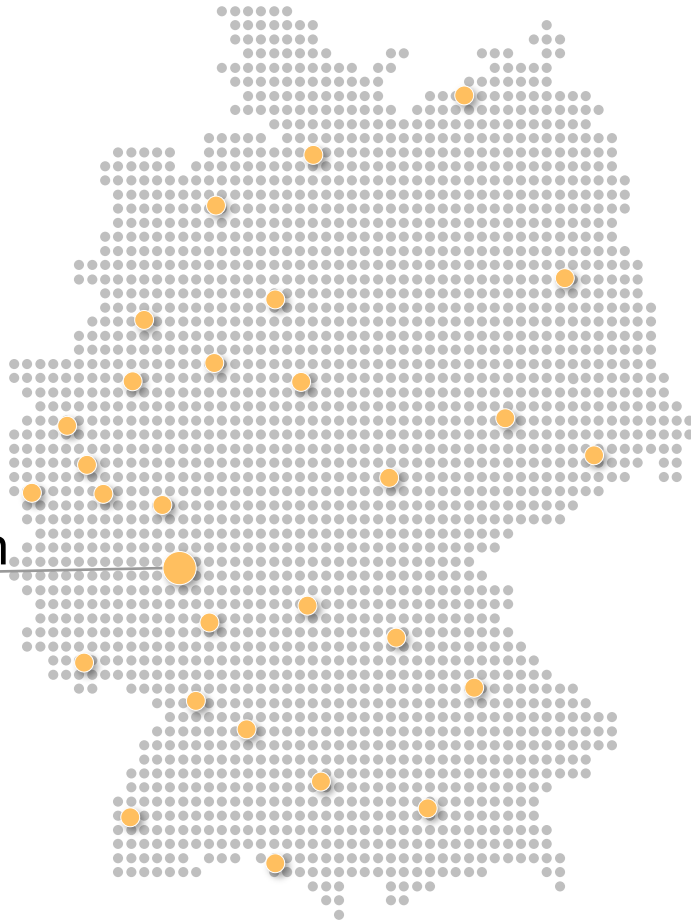
Company
objectives

Company

29

Locations

Wiesbaden



INDUSTRIES

such as



AUTOMOTIVE



RETAIL



PUBLIC



HEALTH CARE



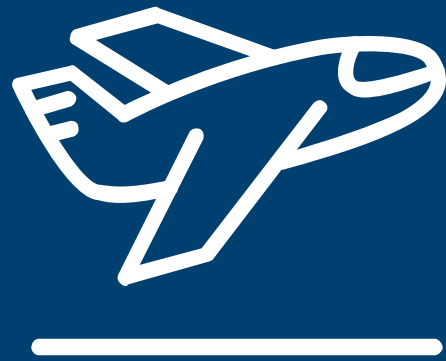
INDUSTRIAL
ENGINEERING



TELECOMMUNI-
CATIONS



FINANCE &
INSURANCE



/ About us

What brings a German company to the US?

- Partnership with HashiCorp & IBM to bring their products to the German market
- Sharing insights from deploying these products for our customers
- Exchanging lessons learned and contributing back to the community

Beyond Secret Zero: SPIFFE, Vault, and Platform Trust for Secure AI Workloads

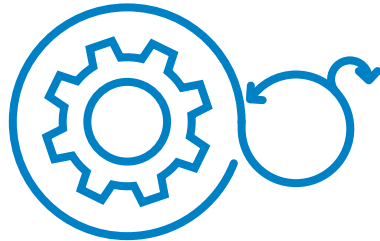
1

Drivers & Objectives



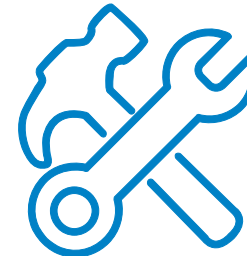
2

Introducing SPIFFE



3

Demo



4

Wrap-Up





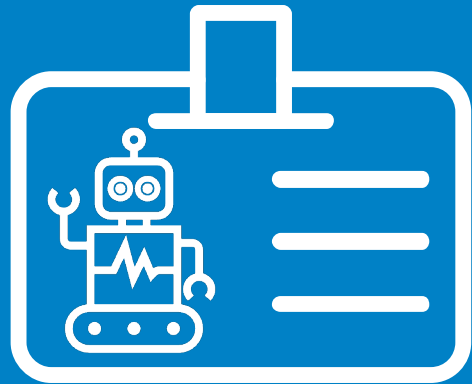
Drivers & Objectives

Challenges with (Non-) Human
Identities and the Secret Zero
Problem

Human Identities

- Represent **individual people**
- Authentication is commonly **interactive** using multiple factors
- Authentication factors include
 - a password (something you know)
 - a smart card (something you have)
 - a fingerprint (something you are)
- IdPs translate **physical attributes** into digital identities during authentication
- Digital identities are handled like non-human identities but are human-bound



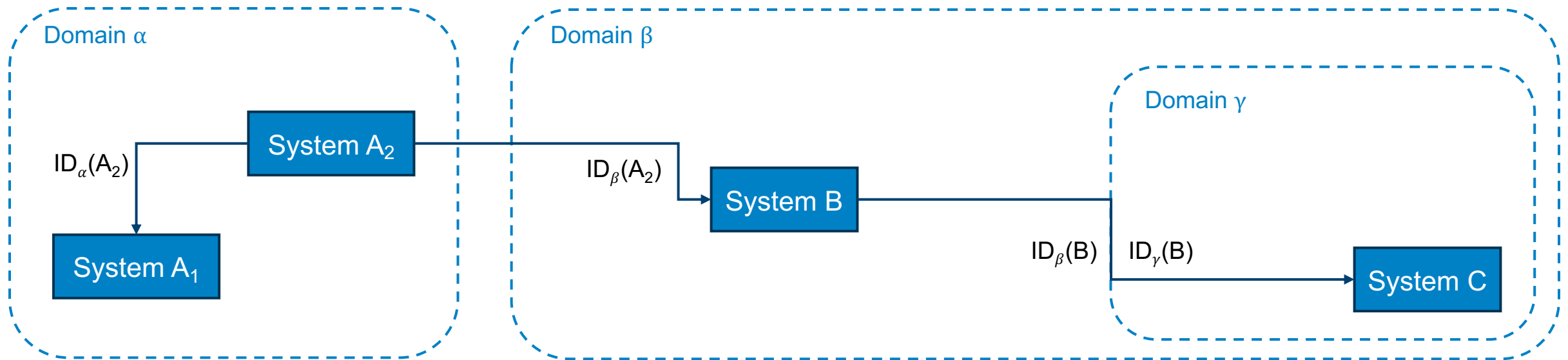


Non-Human Identities

- Represent services, processes, containers, virtual machines, **AI agents**, ...
- Authentication is commonly **non-interactive** using a single factor
- Authentication factors are usually
 - Tokens
 - Keys
 - Certificates
- Validation of these factors relies on
 - asymmetric key pairs
 - chains of trust
 - shared (symmetric) secrets
 - digital signatures

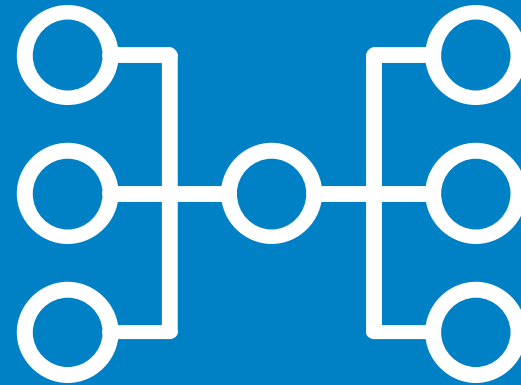
Trust Domain and Identity Federation

- A **trust domain** is both an identity namespace and a security boundary
- Separate trust domains can isolate environments, platforms, or organizational ownership
- **Federation** exchanges trust bundles so workloads can verify identities across domains



Distributed Systems

- Schedulers constantly reassign IP addresses, weakening **network-based identity**
- **Different identity mechanisms** across VMs, containers, and cloud platforms
- Service-to-service authentication must **cross platform** and organizational boundaries
- Identities must remain **specific, auditable, and portable**



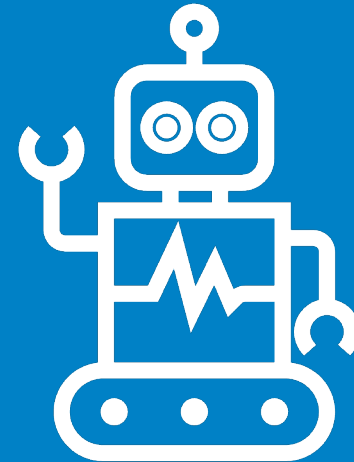
The Secret Zero Problem



- A workload must authenticate before it can retrieve a managed secret or credential
- Bootstrapping that first request with a static token or key only **moves the problem**
- The goal is to derive initial trust from verifiable **runtime or platform evidence**

AI Workloads

- Access to other systems must follow the **principle of least-privilege** and be bound to the intended use case
- Fine-grained access control requires **unambiguous identification**
- Only **dynamic secrets** should be used to access external systems
- Every action must be **auditable** across trust domains

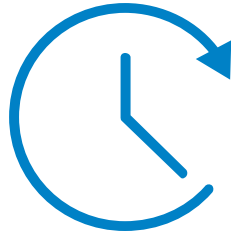


Challenges with (Non-) Human Identities



Secret Zero

→ A workload must authenticate before it can retrieve a managed secret or credential



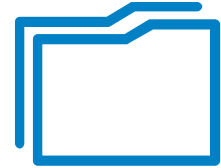
Credential Lifespan

→ Long credential lifetimes increase the attack window if credentials are exposed



Identity Sprawl

→ Without automated NHI lifecycle management, orphaned and stale identities accumulate



Trust Boundaries

→ Establishing trust across multiple nested trust domains and identity systems is complex



Introducing SPIFFE

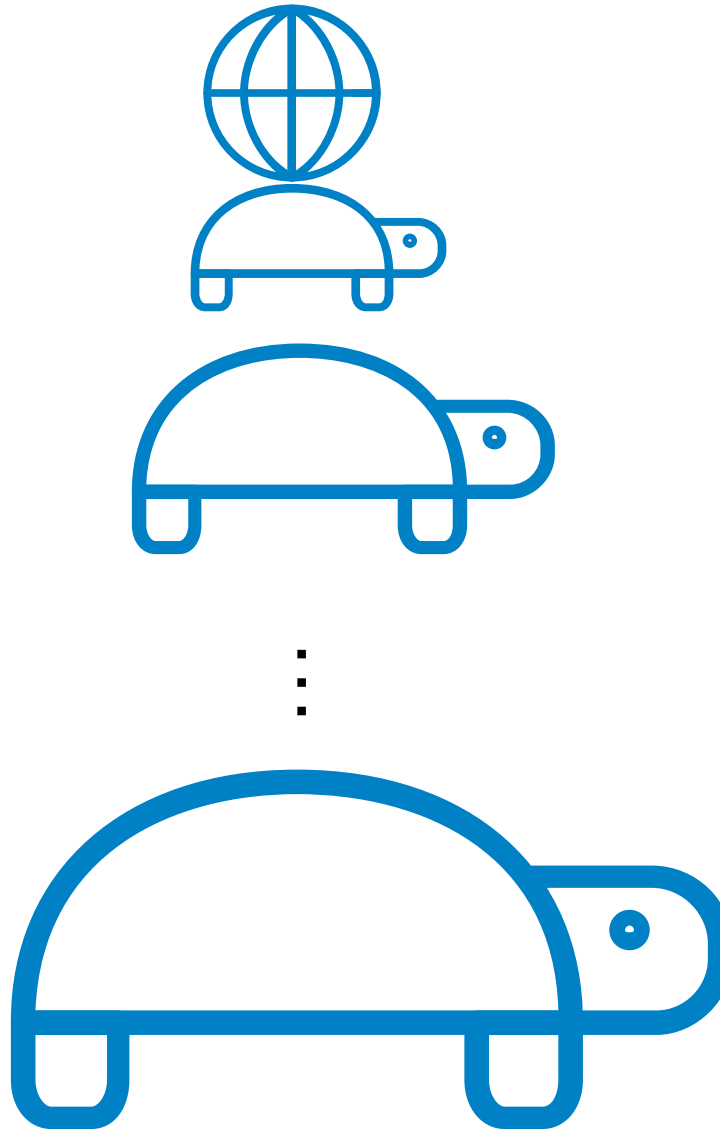
What is SPIFFE? How does it work? Why is it helpful?

What does SPIFFE mean?



Secure Production Intity Framework for Everyone

The Bottom Turtle Analogy

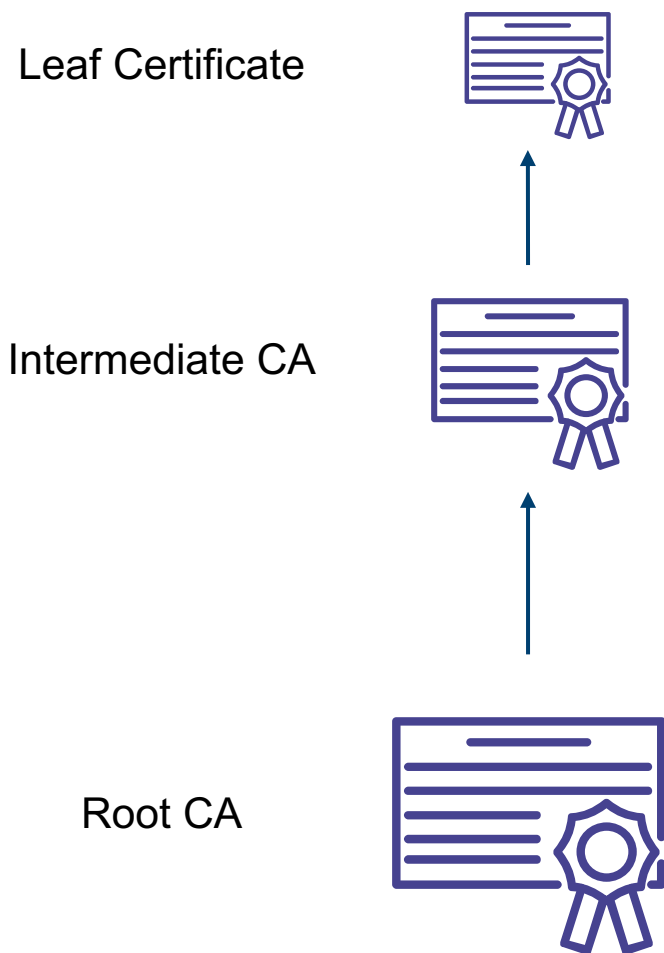
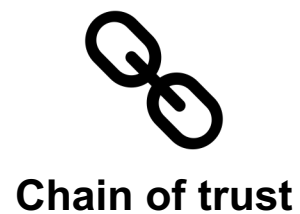
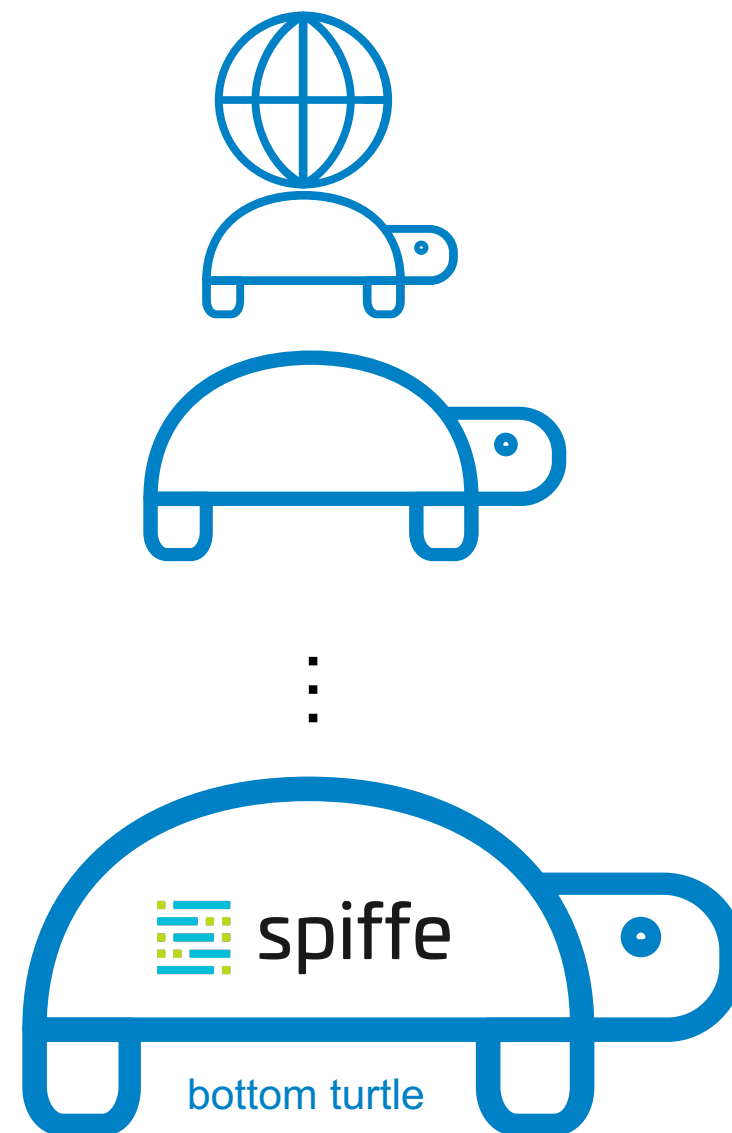


The world sits on top of a turtle ...

... but what does the turtle sit on?

It's turtles all the way down!

The Bottom Turtle Analogy



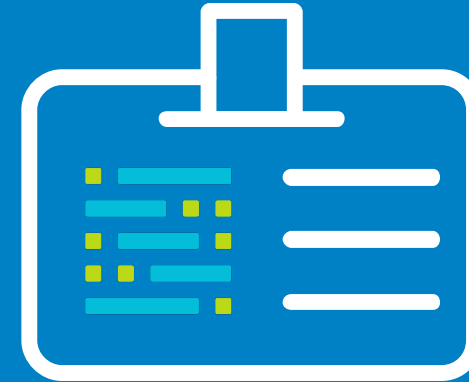
What is SPIFFE?

- SPIFFE is a framework for securely managing NHIs
- A **SPIFFE ID** provides a platform-neutral identity within a trust domain as URI
- **SVIDs** bind that identity to short-lived cryptographic credentials
- The **Workload API** delivers identities and trust bundles to workloads at runtime

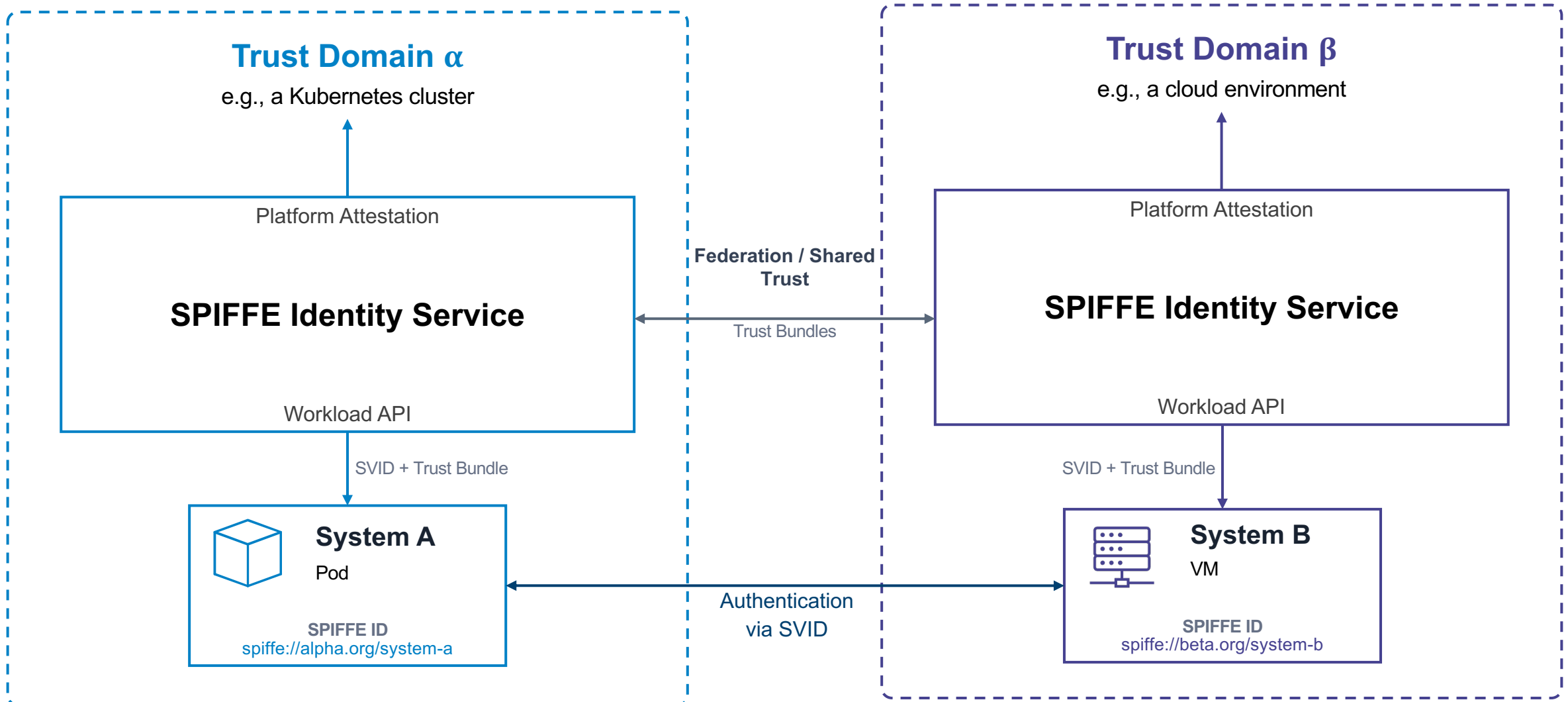


SVIDs

- SPIFFE Verifiable Identity Document
- A SVID is a verifiable identity document that binds a SPIFFE ID to cryptographic material
- SVIDs are short-lived and retrieved at runtime through the Workload API
- SVIDs can be X.509-Certificates, JWTs, or WITs
- Trust bundles let workloads validate peers in the same or a federated trust domain
- SVIDs support mutual TLS (X.509) and token-based authentication (JWT, WIT)



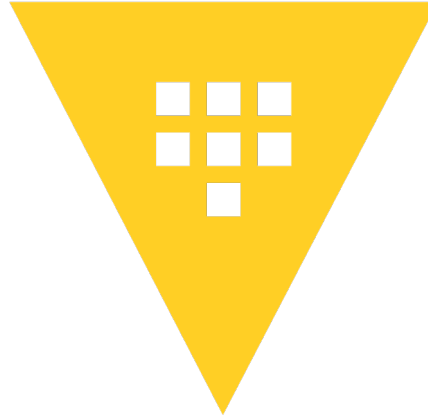
How does it work?



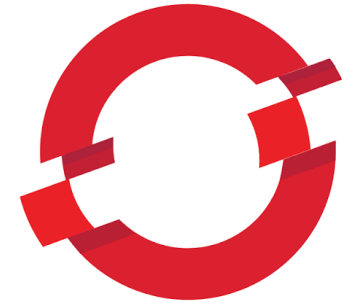
Implementation Examples



SPIRE

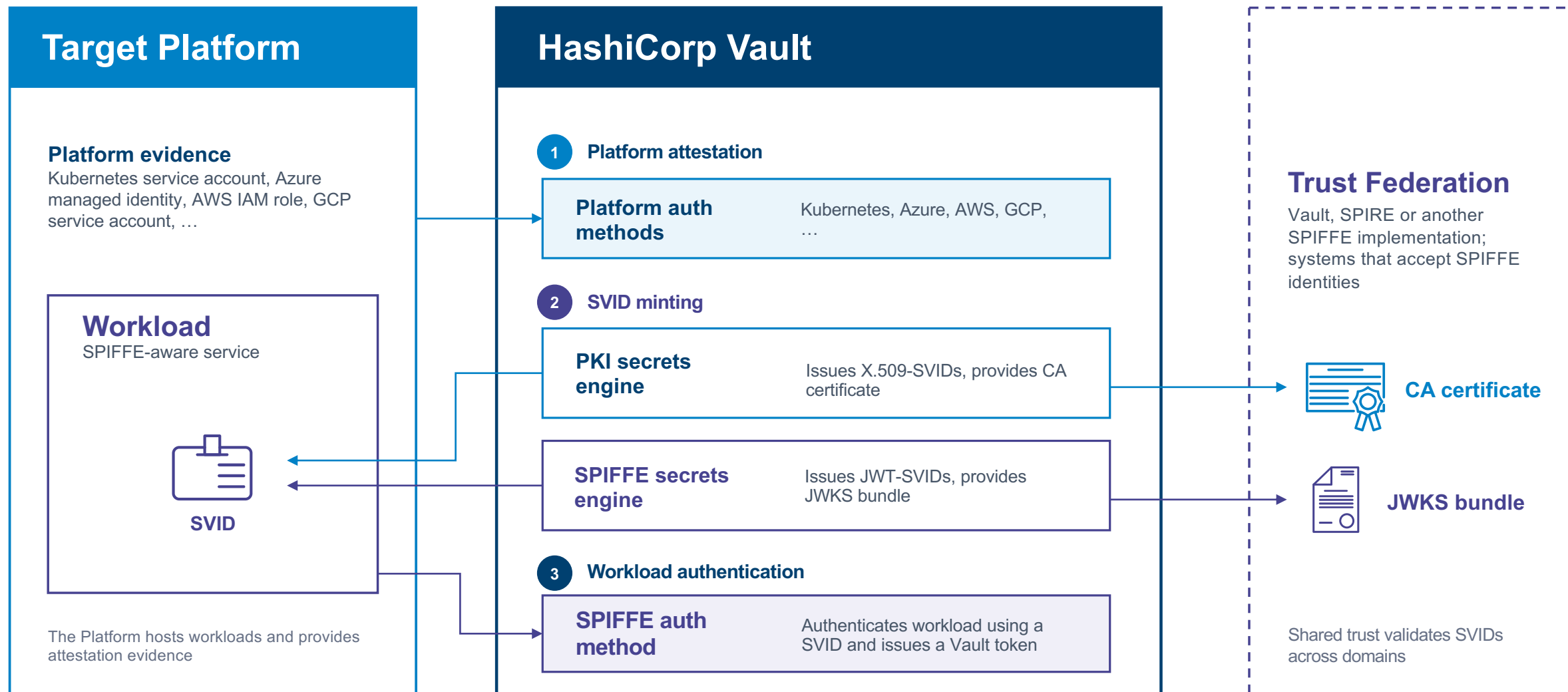


HashiCorp Vault
Enterprise



Red Hat OpenShift
Service Mesh

HashiCorp Vault as a SPIFFE Identity Service



```
elif operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the deselected mirror mo
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0
#me = bpy.context.selected_objects[0]
#me.data.ob[me.name].select = 0
```

Demo

Watch SPIFFE and Vault in action!

A background image showing a group of people in a professional setting, likely a meeting or collaborative work environment. They are gathered around a table, looking at a laptop screen. The image is slightly blurred, emphasizing the text overlay. A white rectangular box with a thin yellow border is positioned on the right side of the image, containing the text.

Wrap-Up

What did we learn today?

/ GitHub



/ LinkedIn



/ Got questions?

Contact



Leon Krass

Technical Leader for HashiCorp Vault

+49 151 53882677

leon.krass@sva.de

www.sva.de

SVA System Vertrieb Alexander GmbH

Hamburg office

Große Elbstraße 273

22767 Hamburg