



04
09/26

ContainerDays Hamburg 2026

Federated Identity for Distributed Systems: Understanding SPIFFE



Leon Krass

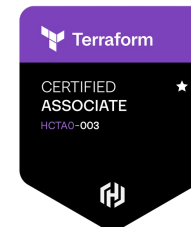
Technical Leader
HashiCorp Vault

/ 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 **3.800 employees** in Germany

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



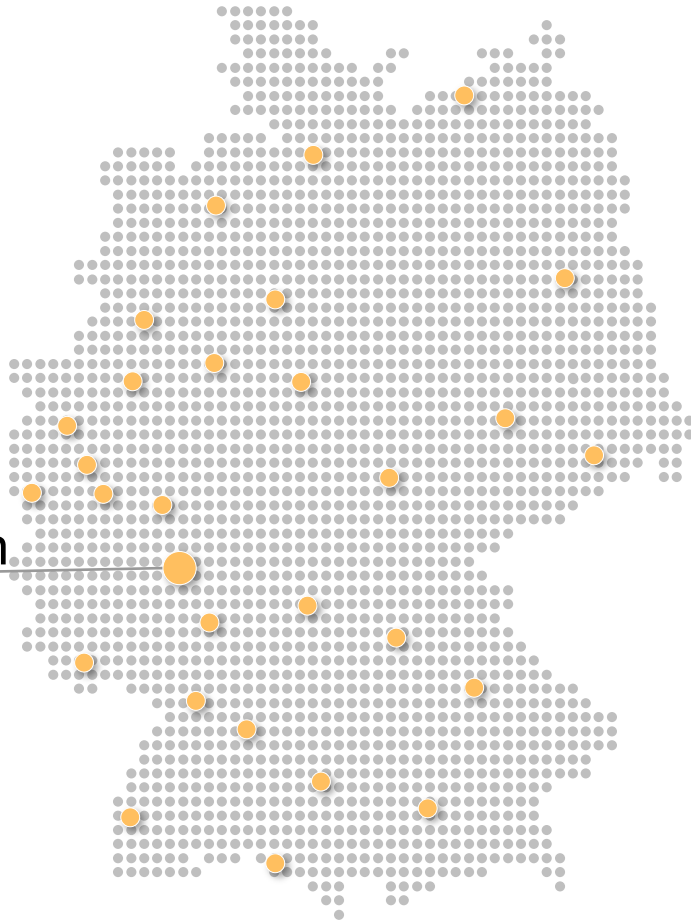
Company
objectives

Company

29

Locations

Wiesbaden



INDUSTRIES

such as



AUTOMOTIVE



RETAIL



PUBLIC



INDUSTRIAL
ENGINEERING



HEALTH CARE



TELECOMMUNI-
CATIONS



FINANCE &
INSURANCE

/ What makes us unique?

SVA ...



Owner-operated

High employee satisfaction
and loyalty

Long-term technical support
for solutions delivered by us

Customer satisfaction and
recommendation above average

Federated Identity for Distributed Systems: Understanding SPIFFE

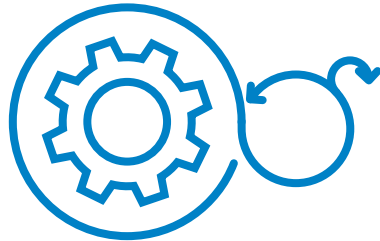
1

Drivers & Objectives



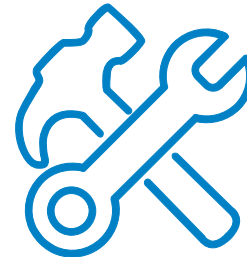
2

Introducing SPIFFE



3

Demo



4

Wrap-Up

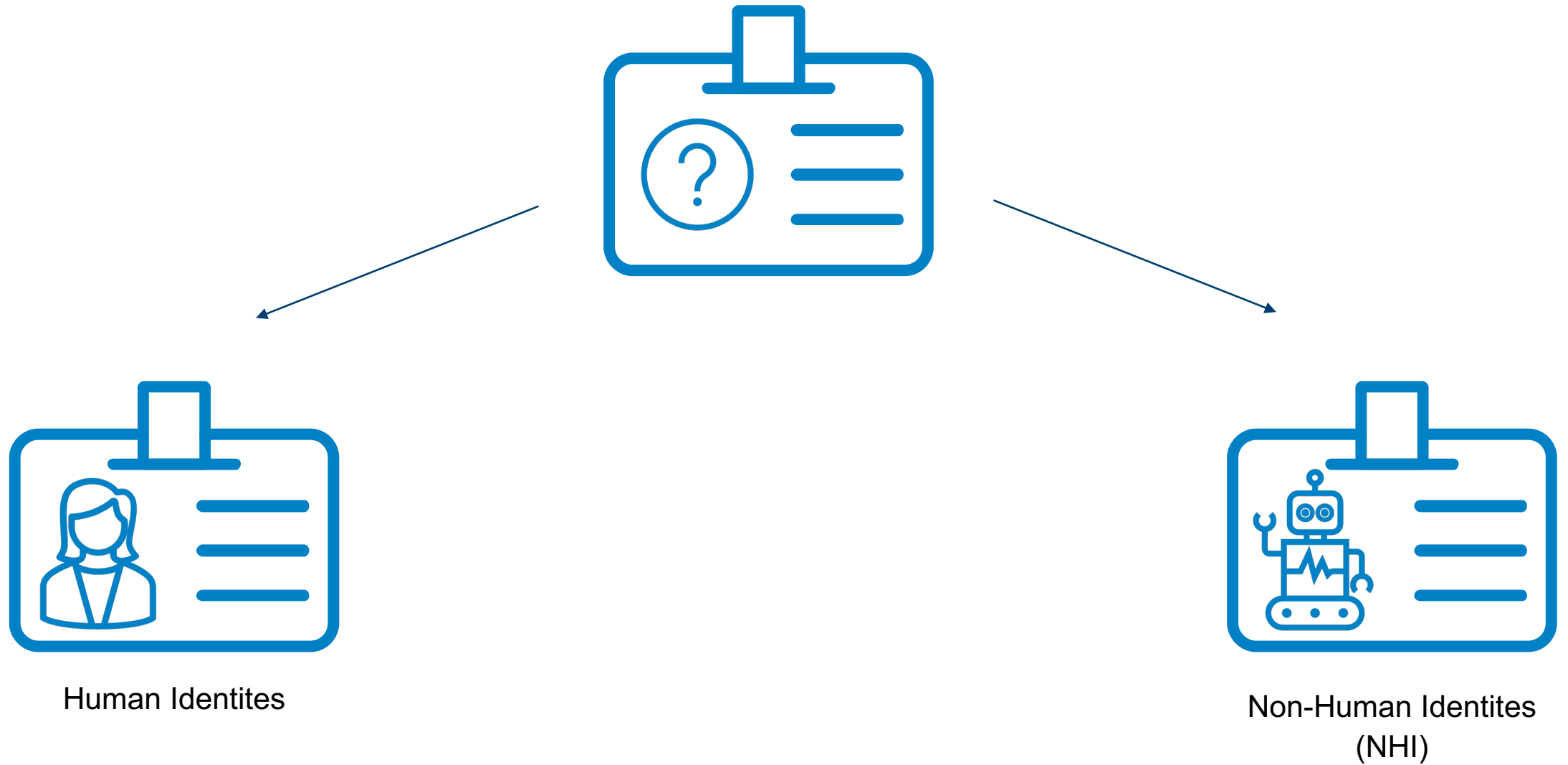




Drivers & Objectives

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

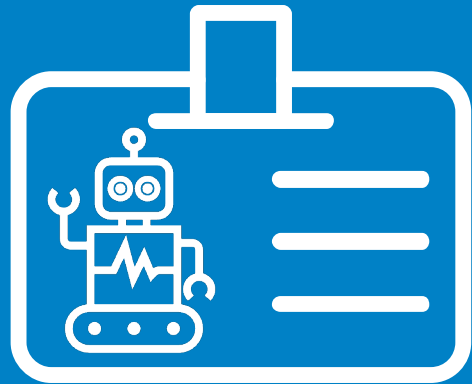
Identities



Human Identities

- Represent individual people
- Authentication is commonly interactive using multiple factors
- Authentication factors include
 - a passwords (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

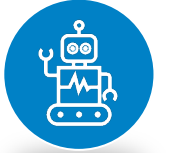
- Represent services, processes, containers, virtual machines, AI agents, ...
- Authentication is commonly non-interactive using a single factor
- Authentication factors are usually
 - Tokens
 - Keys
 - Certificates
- Validation of these factors relies on
 - asymmetric key pairs
 - chains of trust
 -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

Human vs. Non-Human Identities



Human identities are...

- ... bound to real persons
- ... a digital representation of (multiple) physical attributes

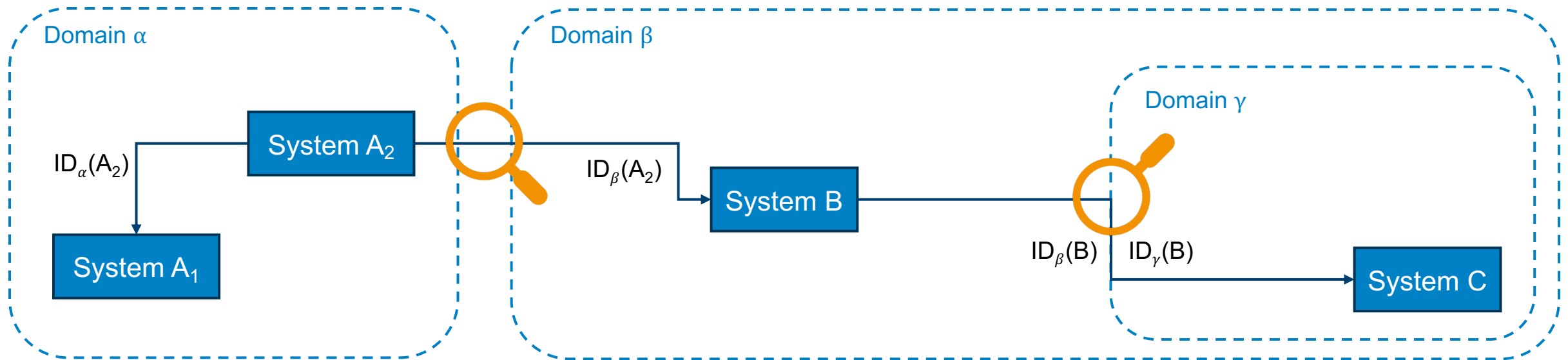


Non-Human identities are...

- ... bound to digital entities
- ... a digital fingerprint for entities without physical attributes

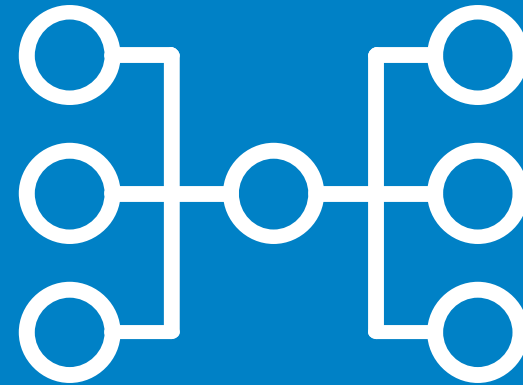
Trust Boundaries and Identity Federation

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



Distributed Systems

- Schedulers constantly change IP addresses, weakening **network-based identity**
- **Different identity mechanisms** across VMs, containers, and cloud platforms
- Elastic scaling creates **high-volume** credential issuance, rotation and revocation
- Service-to-service authentication must **cross platform** and organizational boundaries
- Identities must remain **specific, auditable and portable**



The Secret Zero Problem



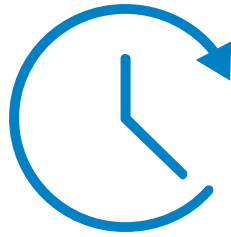
- A workload must authenticate before it can retrieve a managed secret or credential
- Bootstrapping that first request with a static token or key only moves the secret problem
- The goal is to derive initial trust from verifiable runtime or platform evidence

Challenges with (Non-) Human Identities



Secret Zero

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



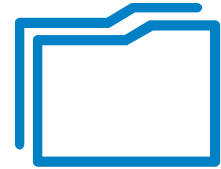
Credential Lifespan

→ Extended credential lifetimes expand the attack window in case of exposure



Identity Sprawl

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



Trust Boundaries

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



Introducing SPIFFE

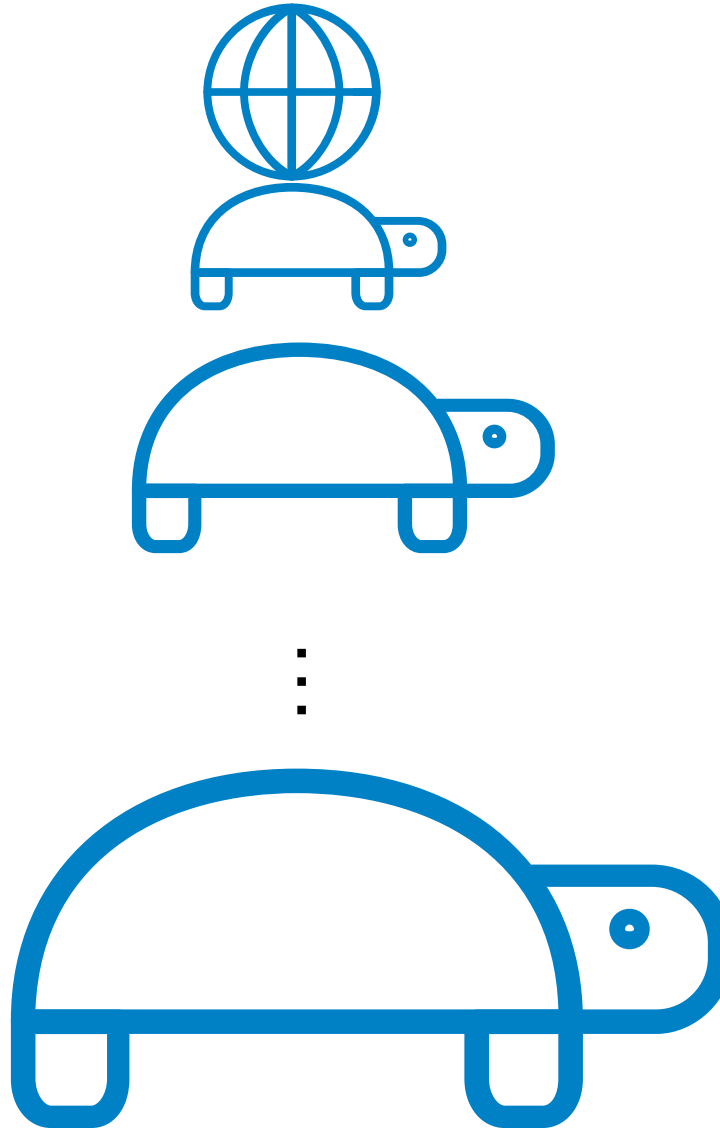
What is SPIFFE? How does it work? Why is it helpful?

What does SPIFFE mean?



Secure Production Intity Framework For Everyone

The Bottom Turtle Analogy

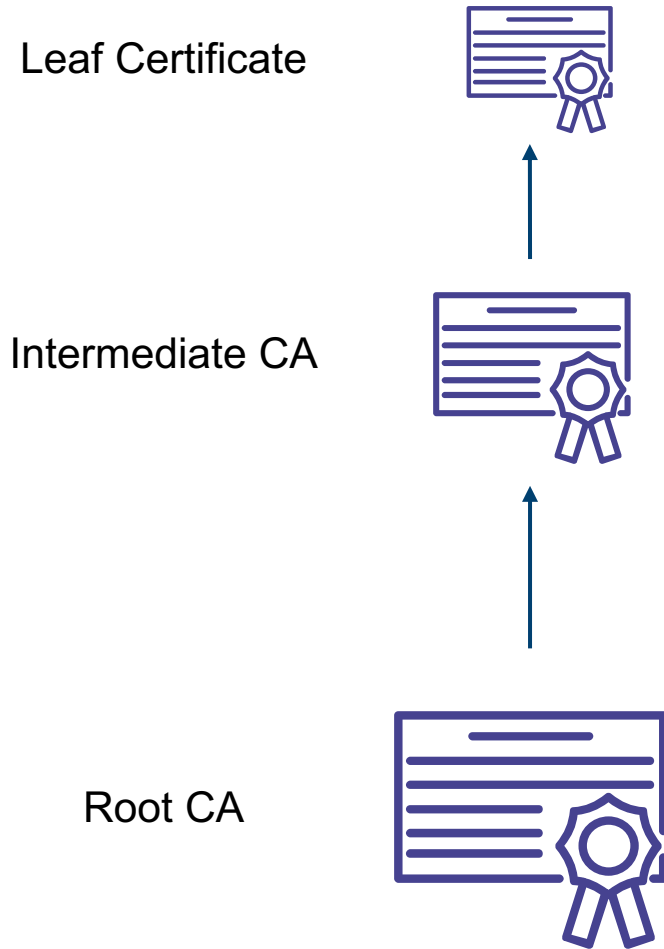


world sits on top of a turtle ...

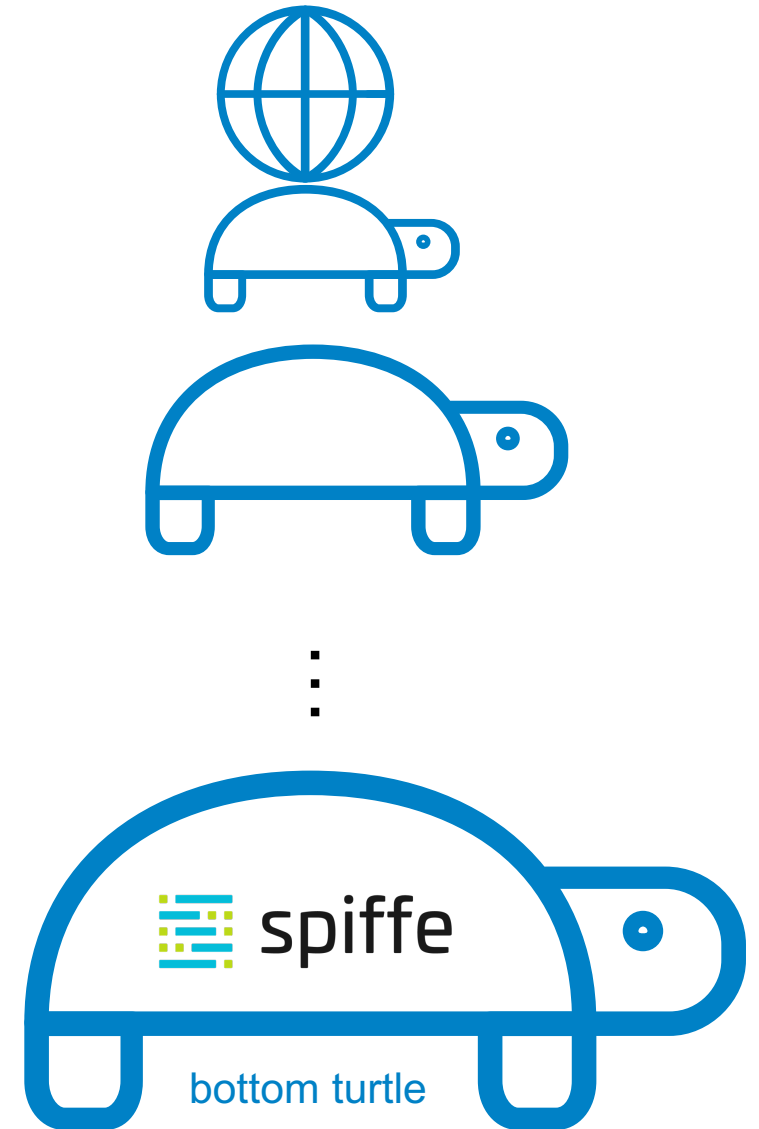
... but what does the turtle sit on?

It's turtles all the way down!

The Bottom Turtle Analogy



Chain of trust



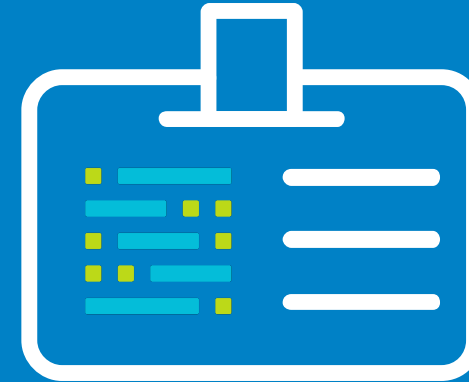
What is SPIFFE?

- 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

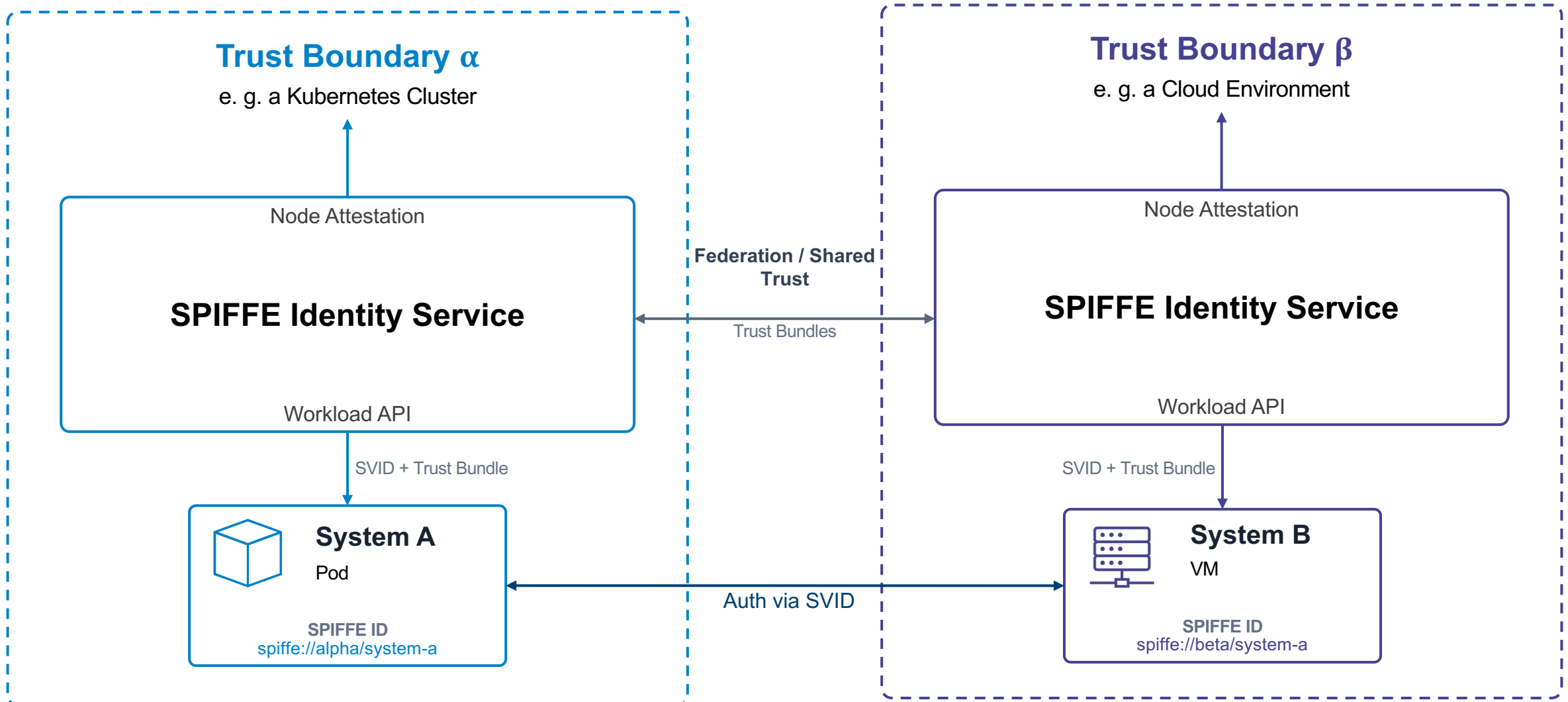


SVIDs

- 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-Certs, 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)



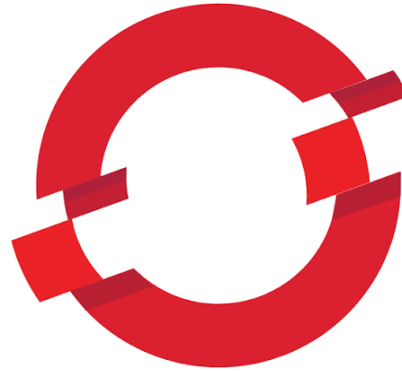
How does it work?



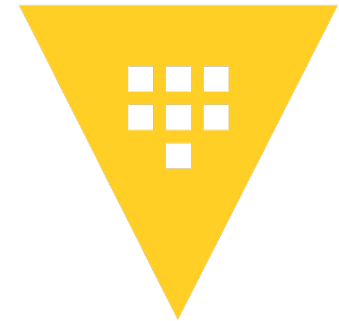
Implementation Examples



SPIRE



Red Hat OpenShift
(Service Mesh)



HashiCorp Vault
(Enterprise)

```
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]
#bpy.data.objects[me.name].select = 0
```

Demo

Watch SPIFFE in action!

A blurred 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 has a soft, out-of-focus quality with warm lighting. A white text box with a yellow border is overlaid on the right side of the image.

Wrap Up

What did we learn today?

/ GitHub



/ LinkedIn



/ Got questions?

Contact



Leon Krass

Technical Leader HashiCorp Vault

+49 151 53882677

leon.krass@sva.de

www.sva.de

SVA System Vertrieb Alexander GmbH

Location Hamburg

Große Elbstraße 273

22767 Hamburg