



03
02/2026

CfgMgmtCamp 2026 | Campus SchoonMeersen, Gent

Static vs. Dynamic Secrets: What Are We Really Talking About?



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.

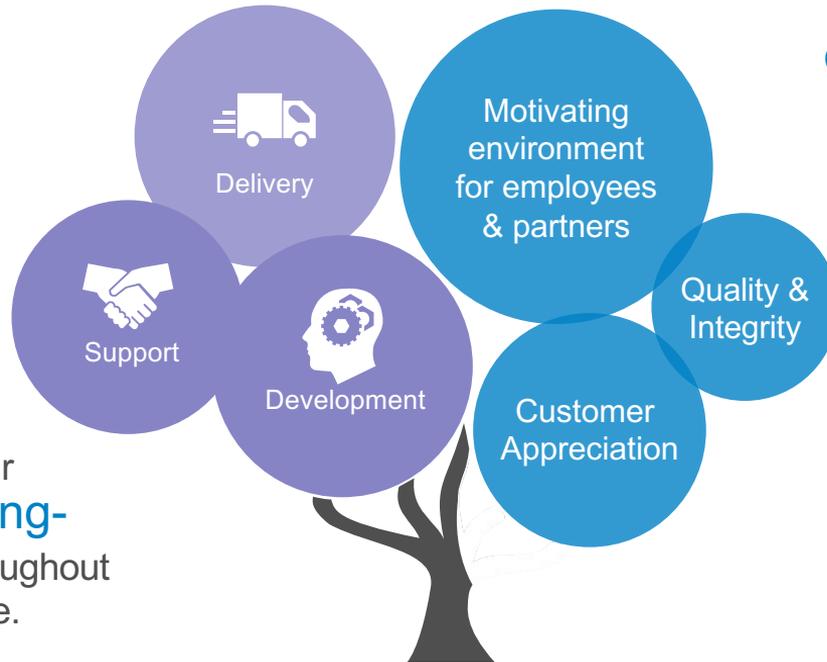
HashiCorp Vault, Kubernetes, Ansible, Terraform

Who is SVA?

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

Steady growth with more than **3.500 employees** in Germany

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



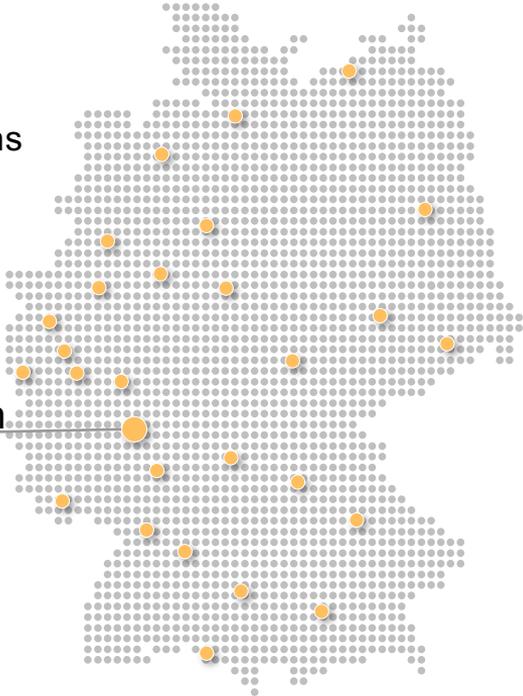
Company
objectives

/ About us

Who is SVA?

28

Locations



INDUSTRIES

such as



AUTOMOTIVE



RETAIL



PUBLIC



HEALTH CARE



MACHINERY & PLANT
ENGINEERING



TELECOMMUNI-
CATIONS



FINANCE &
INSURANCE

Static vs. Dynamic Secrets: What Are We Really Talking About?

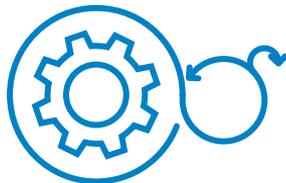
1

Foundation



2

Database Demo



3

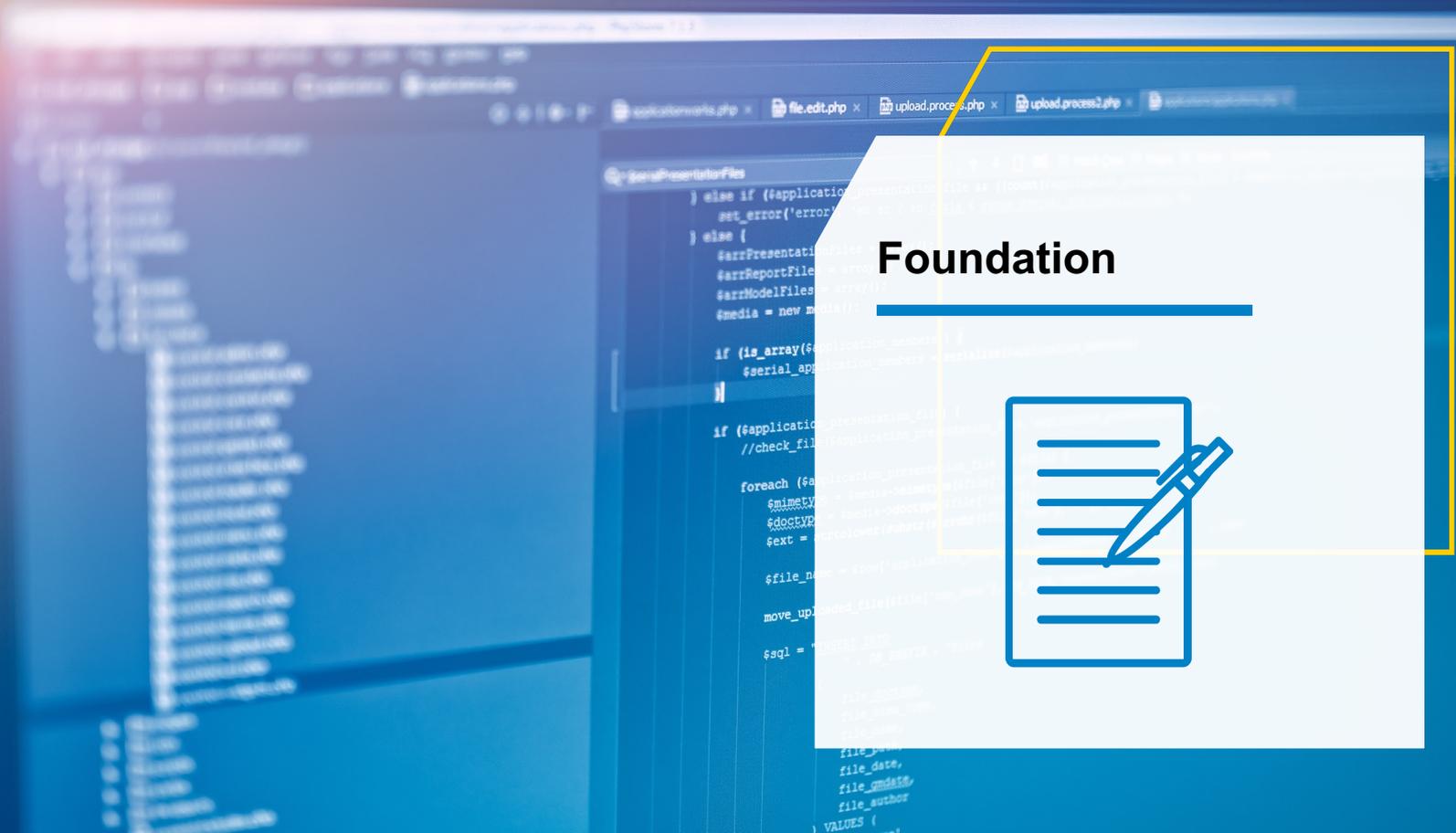
SSH Demo



4

Wrap-Up





Foundation



Identity, Authentication & Authorization

- **Identity** refers to attributes that uniquely distinguish a person, system, or service
- **Authentication** is the process of verifying that an identity is genuine
- **Authorization** defines what a verified identity is allowed to access or perform



What is a Secret?

- Information that is intentionally kept **confidential**
 - Including **personal data**
- Often represents something that enables **trust** or **identity**
- Used to verify, **authorize**, or prove legitimacy in digital systems and gain **(privileged) access**
- Technical POV:
 - passwords, API keys, tokens, certificates, encryption keys, passkeys ...



Where Do Secrets Appear?



Where Do Secrets Appear?

Some examples...

- Configuration files / IaC
- Application code
- Logs & monitoring data
- Container images
- CI/CD pipelines
- Cloud provider metadata & settings
- Operating systems
- Within backups

... and they shouldn't appear here!



Static vs. Dynamic Secrets



Static Secrets

- Human managed
- No automated rotation or expiration
- Rather long-lived, often shared between users



Dynamic Secrets

- Machine managed
- Automated rotation and expiration
- Bound to a (short-lived) personalized lease

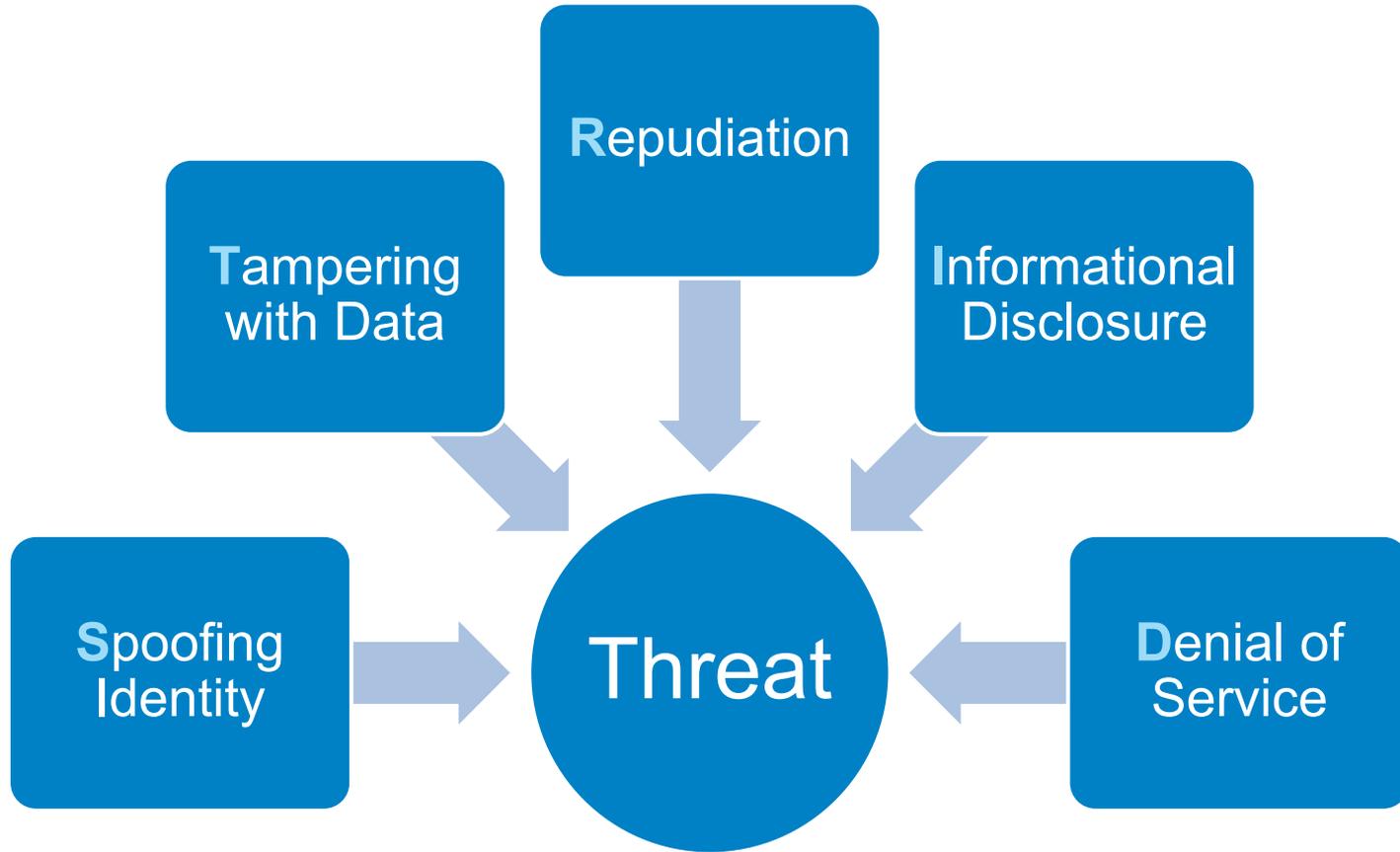




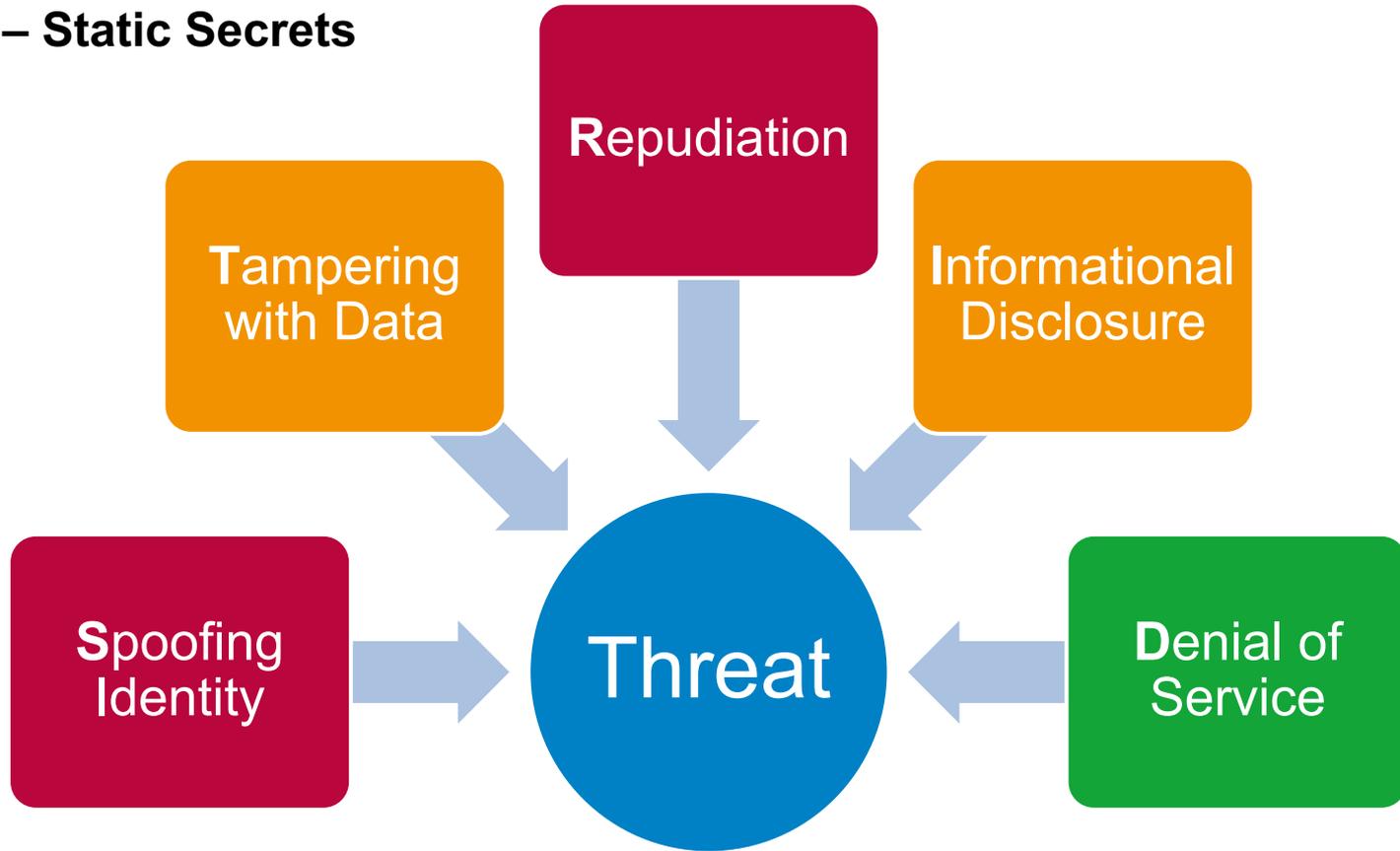
Dynamic Secrets are Superior...

... but why?

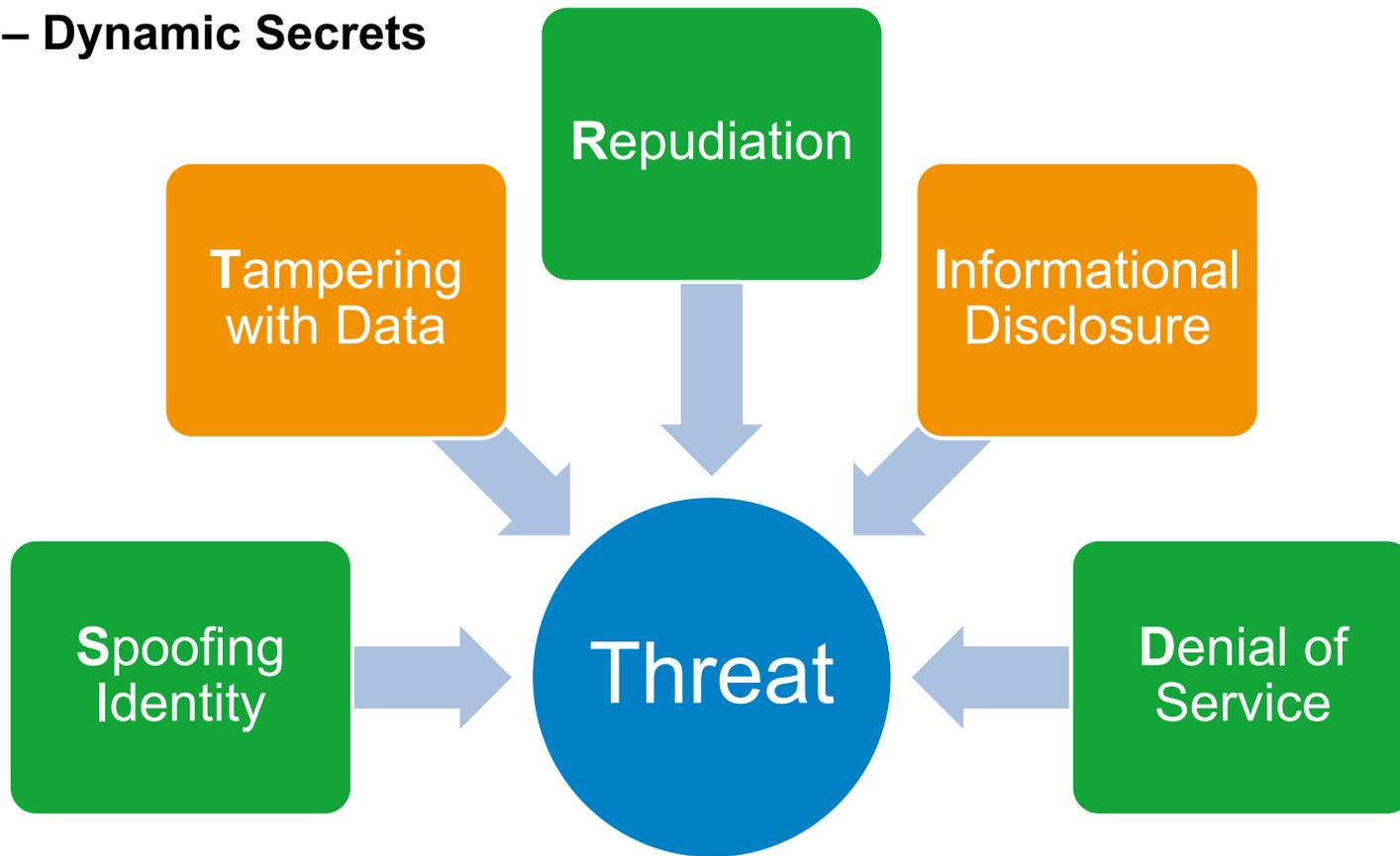
STRIDE



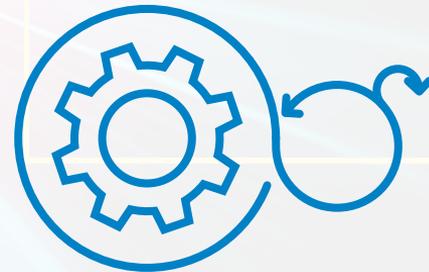
STRIDE – Static Secrets



STRIDE – Dynamic Secrets



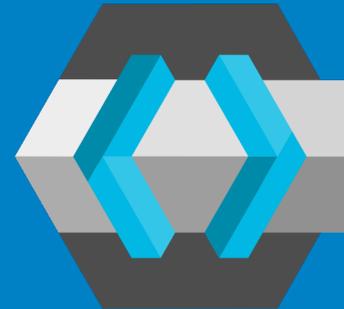
Demo Tech Stack



/ Demo Tech Stack

Identity: Keycloak

- Identity and Access Management (IAM) platform
- Centralized authentication and authorization
- User management, identity brokering, and federation





/ Demo Tech Stack

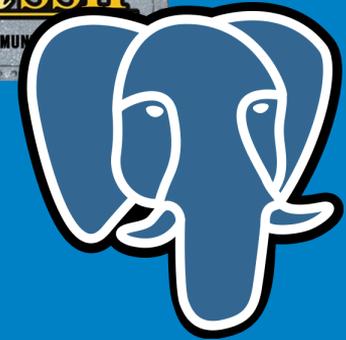
Secrets: OpenBao

- Securely storing and controlling access to secrets
- Identity-based access across distributed systems
- Dynamic, short-lived secrets

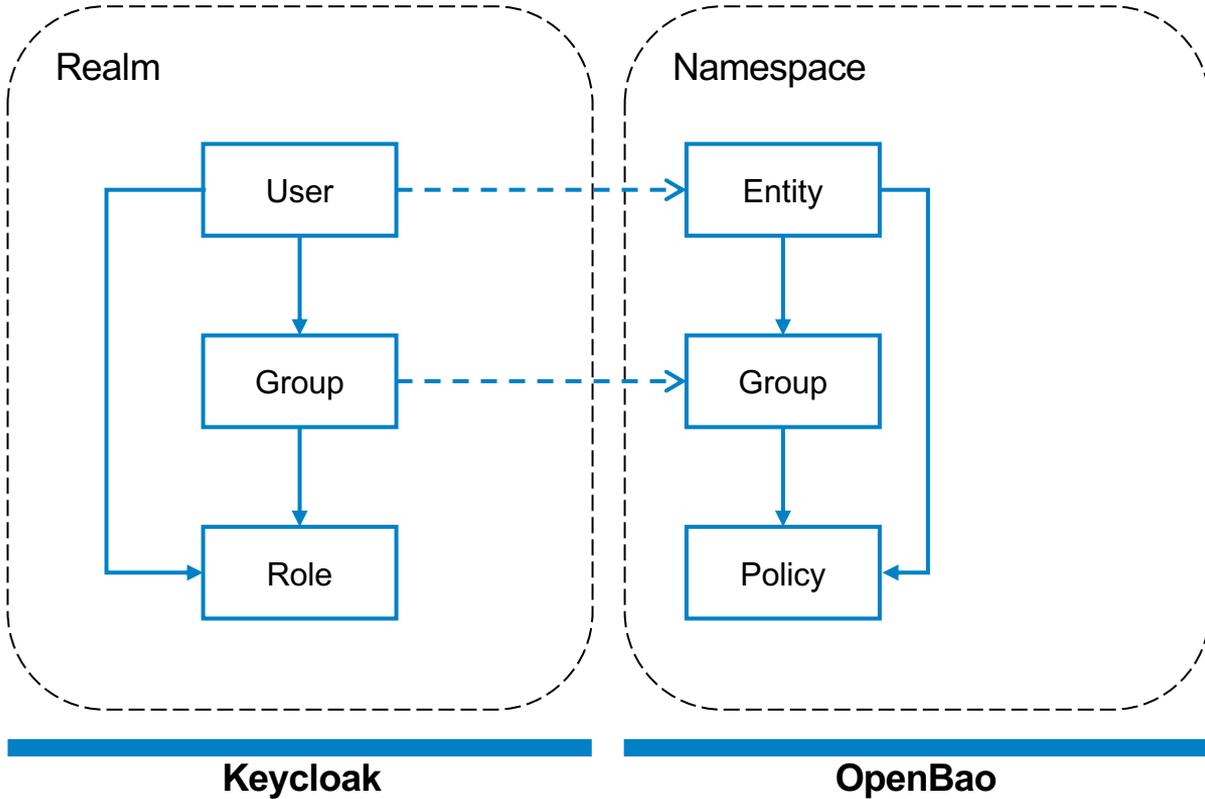
/ Demo Tech Stack

Clients: PostgreSQL, OpenSSH

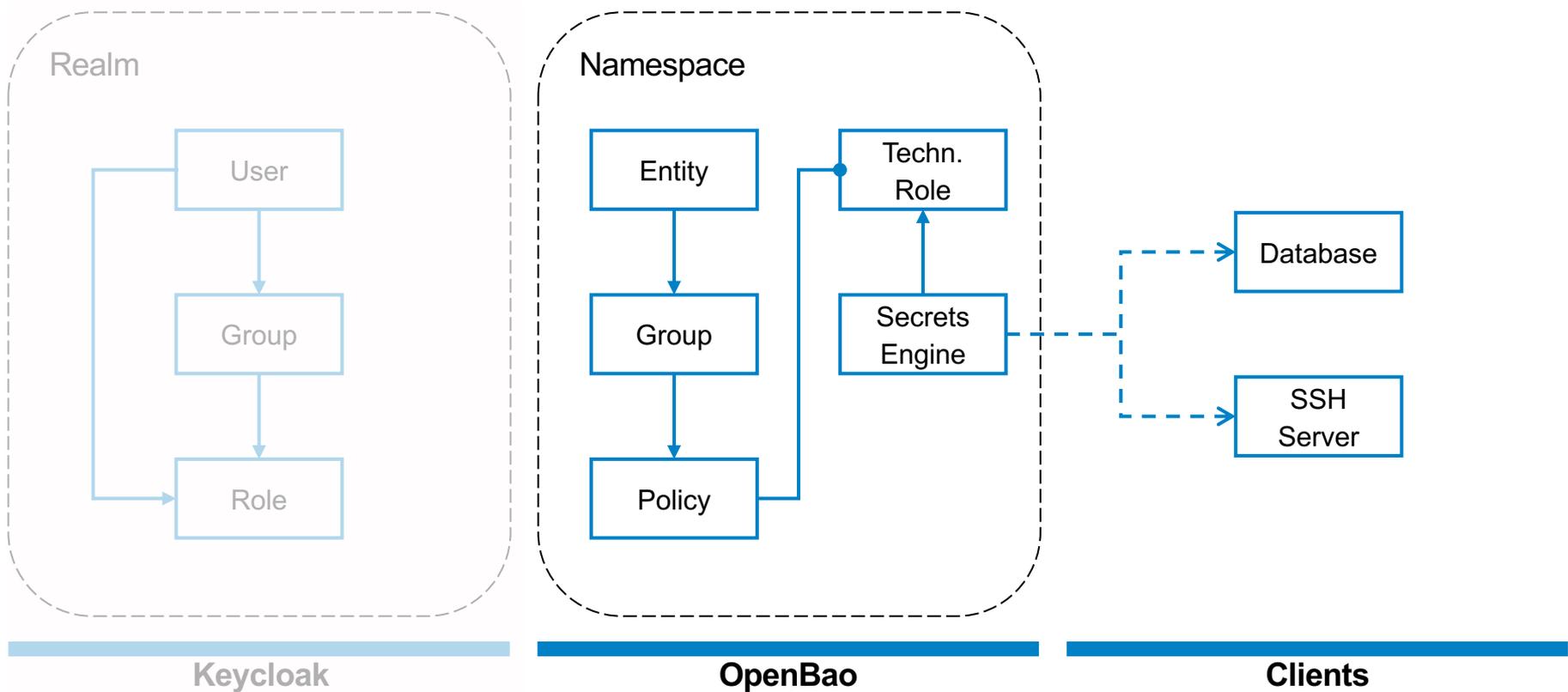
- **PostgreSQL**: object-relational database system
- **SSH**: Cryptographic network protocol to access, manage, and control remote systems



Domain Model



Domain Model



Actors



Alice

→ Member of "Team A"

→ Database admin

→ RW Access

→ SSH user

→ General access



Leon

→ All access 😊



Bob

→ Member of "Team B"

→ Database user

→ RO access

Database Demo



How It Functions



Static Secrets

1. Admin creates user with static credentials
2. Credentials are shared via KV Engine in OpenBao
3. User logs in



Dynamic Secrets

1. Admin configures OIDC Auth, SSH Engine & Policies in OpenBao
2. User Logs in to OpenBao via Keycloak (OIDC)
3. User retrieves dynamic credentials to logs in



SSH Demo



How It Functions



Static Secrets

1. Admin creates user with static credentials
2. Credentials are shared via KV Engine in OpenBao
3. User logs in



Dynamic Secrets

1. Admin configures OIDC Auth, SSH Engine & Policies in OpenBao
2. User Logs in to OpenBao via Keycloak (OIDC)
3. User sings certificate to log in





Wrap-Up



Can We Still Break Dynamic Secrets?

In general: YES, but we can improve our security with them

Some challenges:

- Root credentials
 - How does OpenBao access its target systems?
- Secret zero
 - How do non-human clients access OpenBao?
- Timing
 - How long should leases be?
- User behavior
 - How to prevent users of sharing personal secrets?



/ Grab your copy!

Slides & Demo



/ 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



03
02/2026

CfgMgmtCamp 2026 | Campus SchoonMeersen, Gent

Static vs. Dynamic Secrets: What Are We Really Talking About?