SBB CFF FFS | Adfinis | CUSTOMER CASE STUDY

Modern Secrets Management for a Modern Railway Operator

One of the world's most punctual railway operators introduces modern secrets management based on HashiCorp Vault to provide the foundation of its digitization strategy.

// Infrastructure Enables Innovation

About SBB

Swiss Federal Railways (SBB) is one of the top three punctual railways in the world. Founded in 1902, SBB's core business includes passenger services as well as real estate, freight services, and infrastructure. With an average headcount of almost 34,000 it is also one of the biggest employers in Switzerland. Each day SBB connects nearly one million people by ensuring they travel safely and reliably and arrive on time. SBB traverses all of Switzerland and connects the country to Europe through the Gotthard Base Tunnel in the Alps - the longest and deepest train tunnel in the world.

SBB's railway is far-reaching, popular, and punctual. The network hosts 11,260 trains every day. Each train arrives and departs within three minutes of schedule 91.9% of the time. In order to sustain this impressive performance, support a more flexible consumer experience, and reduce carbon emissions, SBB is undertaking a digital transformation journey based on its strategy 2030 - a four-pronged plan for enhancing the robust railway's operations.

SBB FAST FACTS

Strengthened SBB security in the right place

Helped stabilize IT systems to satisfy high expectations from customers for on-time trains

Increased agility for SBB's developers and reduced business risk

Integrated seamlessly with SBB's systems due to developer-first approach

Established security automation for critical IT systems

Built a lighthouse use case for ongoing SBB transformation

> " Vault is resilient, stable, and highly available; and it's like a Swiss army knife of secrets management, providing many integrations out of the box with a fast-paced roadmap.
>
> ANDREAS MEISTER
> ENGINEERING TEAM LEADER AND SECURITY ARCHITECT

Connecting more than railways

SBB's digitization strategy aims to enhance the company's customer orientation, improve efficiency, grow the core business, and achieve carbon neutrality. Reaching these goals requires more interconnectivity for the railway network and its components and systems, such as ticketing to traffic management, customer information systems, various IoT devices, the IT backbone and, most importantly, the customers themselves. Each SBB train is, in essence, a small data center on rails.

To update and connect these systems, SBB's developer team needed secure authentication for all of its tools. Their certificates, tokens or log-in credentials ("secrets") had to be accessible but safe from unauthorized users. Robust authentication required a scalable, reliable, and feature-rich secrets management. For the digitization to succeed, any solution SBB selected also had to improve security posture by eliminating hard-coded and plain-text secrets and establish security automation for critical IT systems.

Challenges

SBB IT required a solution with a developer-first approach.

SBB operates a highly complex railroad system around the clock, so any secrets management solution it implemented must also offer the best conditions and flexible options for high availability.

Future-oriented digitization requires well-integrated solutions. Secrets management tools would have to be versatile and fit with a fast-paced roadmap.

> " A platform, no matter how good, does nothing for the company if it is not used. That's why we have invested in the training and awareness of developers, but also in automation.
>
> ANDREAS MEISTER
> ENGINEERING TEAM LEADER AND SECURITY ARCHITECT

Why Vault: The secrets management journey

Engineering Team Leader and Security Architect, Andreas Meister has been at the heart of the company's digitization. He received internal inquiries about secrets management as early as March 2019. Safeguarding credentials has become a major point of emphasis during the company's transformation.

Meister and his teams gathered requirements for a potential secrets management solution. Any platform the group chose would have to properly store secrets, streamline access to those secrets, and minimize business risk along the way. Based on these requirements, it quickly became clear that HashiCorp Vault best met SBB's needs.

"There are three main reasons why we chose Vault," Meister revealed. "The developer-first approach is a perfect match for SBB IT; Vault is resilient, stable, and highly available; and it's like a Swiss army knife of secrets management, providing many integrations out of the box with a fast-paced roadmap."

From zero to production in 6 months flat

"For a project to be successful, the right people have to work together," Meister underscored. Collaboration would be key for the entire Vault implementation journey. The application security team worked with SBB's identity & access management (IAM) team. Every SBB stakeholder worked with Adfinis, a global open source service provider specialized in planning, building and running cloud native and Linux-based workloads..

Michael Hofer, Chief Technology Officer at Adfinis, summarized the joint effort between the two companies. "Collaboration was very important and at the core of the relationship. We provided the Vault experience from beginning to go-live." Adfinis guided SBB through the Vault adoption trail, including strategy, architecture design and engineering. Importantly, the collaboration ensured SBB's site-reliability engineers could take over core aspects of operating Vault.

SBB and Adfinis implemented four Vault clusters on OpenShift platforms operated by SBB. The primary clusters leveraged AWS and the secondary clusters, Swiss OTC, T-Systems' private cloud platform.

“When building the platform, we placed great emphasis on automated processes. This means that the entire configuration is in code and GitOps is not just a buzzword. The team was able to perform a complete migration from one cloud platform to another within a few hours,” emphasized Hofer.

With all stakeholders working together, getting Vault up and running was seamless and quick. “It is really impressive how fast our colleagues have built the Vault platforms in under 6 months and have already taken the first customers on board,” said Meister.

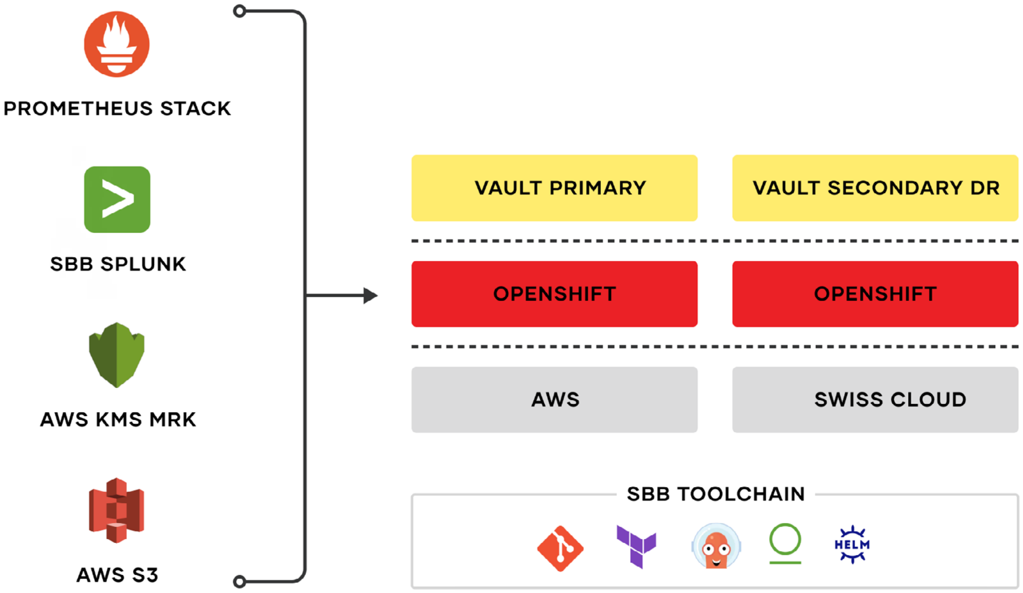

Figure 1: Technology stack of the Vault platform

A renewed emphasis on customer orientation

“A platform, no matter how good, does nothing for the company if it is not used. That’s why we have invested in the training and awareness of developers, but also in automation,” explained Meister.

Beyond Vault implementation, SBB’s AppSec team organized various presentations and Vault trainings. Meister’s teams also developed comprehensive documentation with tutorials for developers. To tie everything together and streamline developer access to Vault, Meister’s teams enhanced SBB’s Developer Self Service Portal. Now, developers can order access to Vault (and other tools) without invoking manual processes. Automating this process guarantees strong Vault governance by enforcing least-privileged access.

The Journey goes on

Meister recognized the potential for the secrets management effort to be the foundation for future transformations.

“This was our lighthouse use case,” he said.

Today, other applications at SBB’s disposal can also benefit from Vault, even if those apps don’t come with native Vault integration. That other applications can already leverage Vault is evidence of its power as a light tower. The solution gives SBB’s developers the tools they need when they need them without fear of exposing valuable credentials. Vault has strengthened SBB’s security in the right place.

Outcomes

Provided a higher degree of automation, leading to increased IT agility, and reduced business risk through securely stored developers secrets.

Significantly improved security posture by eliminating hard-coded secrets and secrets stored in plain text for APIs and databases.

Established security automation for critical IT systems for the SBB fleet to satisfy high customer expectations and set groundwork for future IoT enhancements.

Solution

Vault setup was secure, resilient, simple, and integrated seamlessly with SBB's container-first and multi-cloud strategy. With its many out-of-the-box integrations, Vault met SBB's resilience and reliability requirements, all of which help ensure SBB remains one of the most punctual railways in the world.

SBB Partner

Andreas Meister is passionate about software architecture, agile methods, code design, DevSecOps and his team of engineers. By drawing on his vast experience with both large projects and in SME environments, he leads SBB's engineering team as it consistently improves the technical underpinnings of its vast railway network.

Andreas Meister
Engineering Team
Leader and Security
Architect

Adfinis Partners

Michael Hofer engineers open source solutions which are like the pâtisserie he makes in his free time: precise, elegant, and balanced. As Head of Engineering at Adfinis he is focused on building bridges and supporting organizations on their digitization journey.

Michael Hofer
Head of Engineering

Simon Nussbaum is part of the cloud native team at Adfinis. In his role as engineer and architect he designs, engineers and provides guidance around everything related to containers, secrets management and service mesh.

Simon Nussbaum
Cloud Native Engineer

Pascal Reeb is a cloud native engineer at Adfinis and supports organization around the globe in engineering solutions such as Kubernetes, HashiCorp Vault and Consul.

Pascal Reeb
Cloud Native Engineer

Technology Stack

- **Infrastructure:** AWS and Swiss Cloud
- **Container Runtime:** OpenShift
- **Orchestrator:** OpenShift, Kubernetes
- **CI/CD:** Argo CD, Jenkins
- **Version Control:** Bitbucket
- **Provisioning:** HashiCorp Terraform OSS, Helm
- **Configuration Management:** ServiceNow
- **Security management:** HashiCorp Vault

About Adfinis

Open source is at the heart of Adfinis.
Adfinis is a leading service provider of open source solutions, and they have been in the market for over 20 years. As a company, Adfinis contributes to innovative, sustainable, and reliable IT Infrastructure by being strongly involved in the open source community. They work together with partners like HashiCorp, Red Hat, SUSE, and GitLab and help customers from the very first inquiry to the optimization of solutions. This includes everything from planning to integration, as well as 24/7 operations and managed services. Adfinis is located in Switzerland, the Netherlands, and Australia and has over 90 employees. And they are proud to say that every one, no matter what role they have in the organization: "We are techies by heart."

Find out more: adfinis.com

HashiCorp