HashiCorp

vodafone | CUSTOMER CASE STUDY

Unlocking possibilities

Vodafone uses HashiCorp Vault and have developed custom plugin capability to power secrets management and their high-speed encryption engine.

About Vodafone

Vodafone is a leading global telecommunications company led by its purpose to connect for a better future. It develops a range of leading products and services to connect its customers and help build digital societies of the future. Vodafone operates mobile and fixed networks in 21 countries, and partners with mobile networks in 47 more. As of 30 September 2022, the company had over 300 million mobile customers, more than 28 million fixed broadband customers, and 22 million TV customers. Vodafone is a world leader in the Internet of Things (IoT), connecting more than 150 million devices and platforms.

VODAFONE FAST FACTS

Vodafone has 300M mobile customers

Achieve low latency, high throughput of 36B data encryptions per hour

Provide a framework to extend capabilities and scalability via a plugin architecture

Vodafone operates in 21 countries

Enable secure encryption technologies for 17 petabyte data lake

Provide encryption as a service to multiple engineering teams

> " Look what you can do if you're a Vault Enterprise customer. Look how easy it is to write a plugin to your own requirements, and make it process as fast as you can afford.
>
> ANDY SHACKLADY
> CLOUD TECHNOLOGY PLATFORM ENGINEERING MANAGER, VODAFONE

Securing streams of analytics

Vodafone's analytics and data engineering team manage a large cloud estate that serves many internal customers on Google Cloud for all analytical machine learning (ML), AI and business intelligence use cases. Vodafone's team, led by Andy Shacklady, platform engineering manager, and Lee Whittingham, cloud platform engineering lead, uses HashiCorp Vault to manage secrets in Google Cloud. Vodafone decided to explore the use of Vault and its extensible plugin architecture to implement its own high volume, low latency authenticated encryption with associated data (AEAD) encryption service for personally identifiable information (PII) data.

As one of the world's leading telcos, Vodafone ingests data from more than 300 million mobile customers and IoT devices. Vodafone engineering teams use Vault on Google Kubernetes engine (GKE) for secrets management, along with the full suite of Google services for ML, AI and dashboarding. In order to facilitate this, Vodafone anonymizes personally identifiable information (PII) on ingestion with either data movement technologies — or Big Query depending on the use case — to keep it secure and compliant with data-privacy regulations. Once anonymized, the AI, ML, and dashboarding tools are used to extract the business value.

Tinkering toward faster encryption

Vodafone had some big issues to deal with at the outset. "We wanted to implement Google Tink for PII data, but we had some specific and challenging requirements," says Andy.

Tink is an open-source cryptography library that implements AEAD for encryption and decryption. There are several patterns to implement AEAD, one way would be to hold the AEAD keys in Vault's key-value store and use it on the client side, but a more secure way is to anonymise the data on the server side, never exposing the AEAD keys to the client. But this meant making a custom implementation of the transit engine. The best secret is the one no-one knows.

In addition to the switch to server-side processing, the new solution would have to securely anonymize billions of bits of data daily, up to 10 million encryption operations each second. The solution Vodafone chose would have to do this fast and at a massive scale. Already familiar with Vault and its extensive functionality, Andy and his team decided to see what else was possible with the solution.

Challenges

High volume, low latency encryption, ability to synchronize AEAD keys securely held in either Vault for ingestion frameworks or BigQuery for analysis tools

Rotate keys and manage key lifecycle on the server side

Write role-based access control (RBAC) policies that allow separation of administration, encryption, and decryption roles

Plugging in to think outside the box

Vodafone invested in Vault Enterprise for its combination of out-of-the-box features and its extensibility to support future projects. Already, Andy's team used Vault for secrets management and multiple data-analytics streams. Vault Enterprise offered these capabilities, as well as extensive governance and policy features, meaning Vodafone could write policies to manage which team members had which privileges, like encrypting and decrypting data. Vault Enterprise also offered remediation as part of its "rock-solid" backup and recovery solution.

The team also needed something to support its data encryption at scale with the Google Tink engine. While the task at hand wasn't the purview of an out-of-the-box Vault feature, Vodafone was enamored with the sheer potential of the platform. "We began experimenting with Vault, wondering what was possible. We needed something to pseudonymize data at scale, handle all sorts of keys, and go really fast while doing so."

- The team decided to explore the potential of Vault by writing its own plugin. When they were done, the major functionality of the plugin included:
- A custom secrets engine plugin to Vault that enables data to be encrypted and decrypted with Google Tink keysets for anonymization purposes.
- Server-side anonymization, key lifecycle management, and synchronization with Big Query.
- Transient or stateless data encryption and decryption, with the configuration and keys held securely in Vault.

"As server-side encryption is a compute heavy task", says Lee, "we decided to utilize the scalability of Kubernetes to keep pace with the demands of changing workloads". To separate compute from storage, Lee provisioned two clusters, one to run Consul for HA storage and an Autopilot cluster for Vault with the Tink plugin preinstalled into the Vault container image for speed. The clusters communicated via a high performance internal load balancer. This separation allowed Vault to scale rapidly, without impacting the backend storage unnecessarily.

Vault extensibility unlocks new possibilities

The Vodafone team got itself up and running, and HashiCorp architects and solutions engineers worked with Vodafone to polish the plugin. HashiCorp's team helped Vodafone fine tune settings and reviewed the architecture and scaling approach to ensure the solution would work seamlessly.

The plugin Vodafone wrote enables an operational change. Rather than Vault dispensing keys to clients, the change allowed Vault to encrypt data and send it back to the client without giving out the keys. "We already had experience with Vault and knew how to use it," says Andy. "It was more a question of what else can we do with Vault? We were using it as a secrets manager. Now we're also using it as an encryption engine."

In fact, Vault has become even more than an encryption engine. For Vodafone, Vault is a full execution framework with built-in security. Because Vodafone could write its own plugin, it could also write its own endpoints for the plugin's functionality. Instead of fulfilling a specific need, Vault became an all-encompassing enabler, showing Vodafone what kinds of things were possible.

Andy says he's impressed with what has been possible with Vault. "Look what you can do if you're a Vault Enterprise customer. Look how easy it is to write a plugin to your own requirements, and make it process as fast as you can afford."

Outcomes

Vodafone created a custom plugin, fine-tuned for its specific purposes, to extend Vault and decrypt and encrypt data using Google Tink

Via horizontal scaling in Google Cloud, and in a test bed, Vodafone achieved up to 10 million encryptions per second or 36 billion per hour

Solution

Vodafone worked with HashiCorp to extend Vault for their specific needs. Vodafone wrote its own plugin that turned Vault from a secrets-management platform into an encryption engine, all while maintaining the speed and thoroughness it required to pseudonymize billions of bytes each hour.

Vodafone Partner

Andy is a Software Engineering Manager with circa 20 years of experience managing engineering teams for Tier-1 global financial and telco institutions. Currently focused on Platform Engineering for Analytics at Vodafone on Google Cloud, his scope includes Infrastructure as Code, Cloud based services and Security. Andy lives in London with his family and dog.

Andy Shacklady
Cloud Technology Platform
Engineering Manager

Specializing in virtualisation, containerisation and security, Lee has over 30 years of experience in the IT industry. He has worked mainly within the banking and telco sectors and is currently the Google Cloud Platform Engineering Lead at Vodafone. He lives near London with his family.

Lee Whittingham
Google Cloud Platform
Engineering Lead

Technology Stack

- **Infrastructure:** Google Cloud and Anthos
- **Workload Type:** Secrets and custom engine
- **Container Runtime:** Containerd
- **Orchestrator:** Kubernetes – GKE and Anthos
- **CI/CD:** GoCD for infrastructure
- **Version Control:** GitHub

HashiCorp