Secrets as a Code

Empower teams with self-service secrets management

23.07.2025 Freiburg DevOps Meetup, Maksym Prokopov

Agenda

- Intro
- Status Quo
- The problem
- Tools Overview ⚒️
- Demo 😍
- Diagrams
- Summary

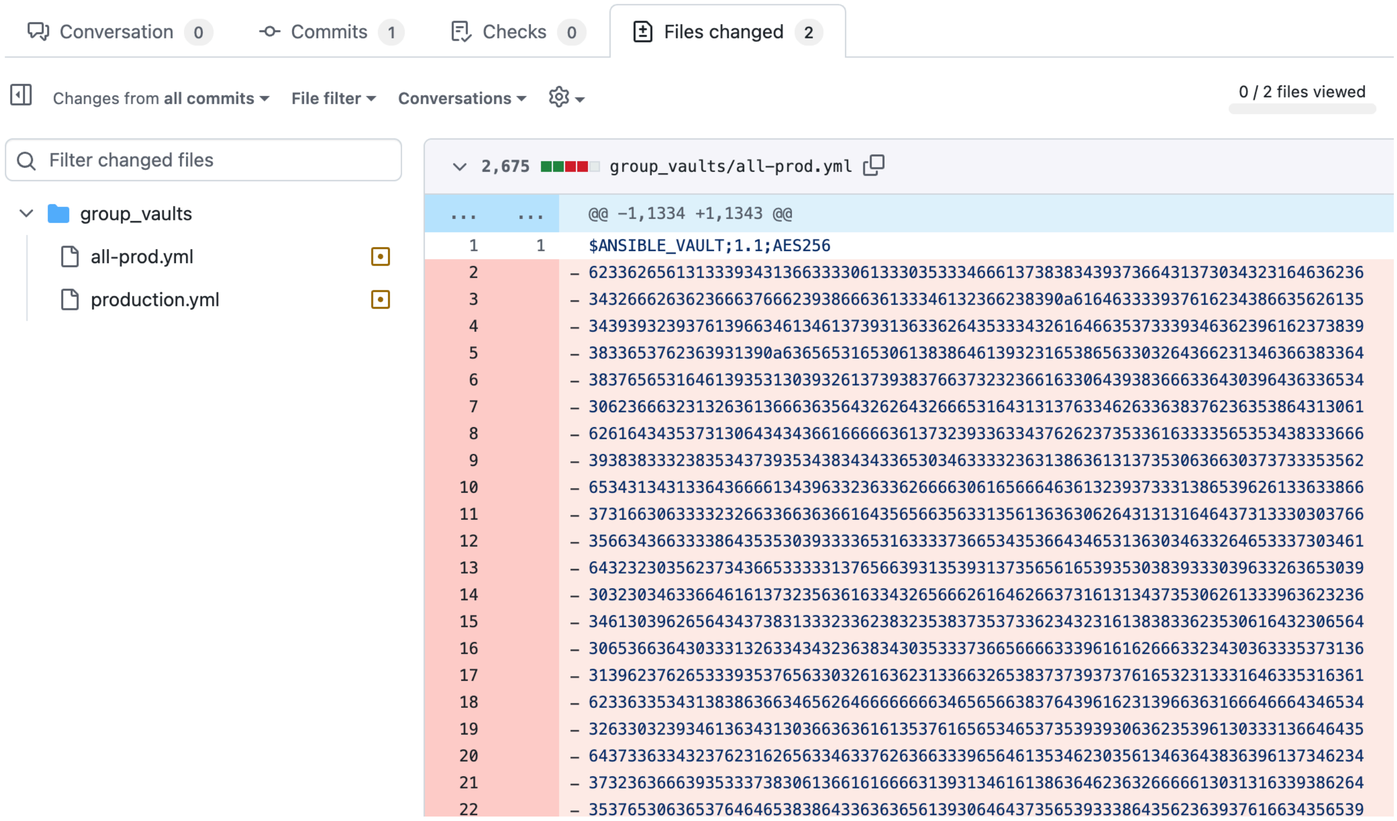
About Me

Maksym Prokopov

- Many years in the software development
- Work at Billie - **Buy Now Pay Later** from Berlin
- Love to fiddle with tech and build projects

The Old Way
Ansible Vault

- Single Encrypted File
- Developers take care of development
- SRE take care of production
- Git diffs 🙈



The Old Way
Ansible Vault

- Single Encrypted File -> Encrypted String
- Better Git diffs 🎉

The Old Way

Hashicorp Vault - good parts

- Dynamic secrets – better security! 🏅
- Support in Terraform
- Versioning

The Old Way

Hashicorp Vault – not so good parts

- Network Access
- Token Management
- Policy Management
- Maintenance

The problem

- Dependency on the Platform team
- Difficult to audit
- Kubernetes compatibility
- Burden of maintenance

Solutions short-list

Hashicorp Vault Operator

- Consul Agent in a docker image
- Complexity
- References

Cloud Native
What about AWS?

- Secrets Manager
- Systems Manager Parameter Store
- Key Management Service

https://external-secrets.io/

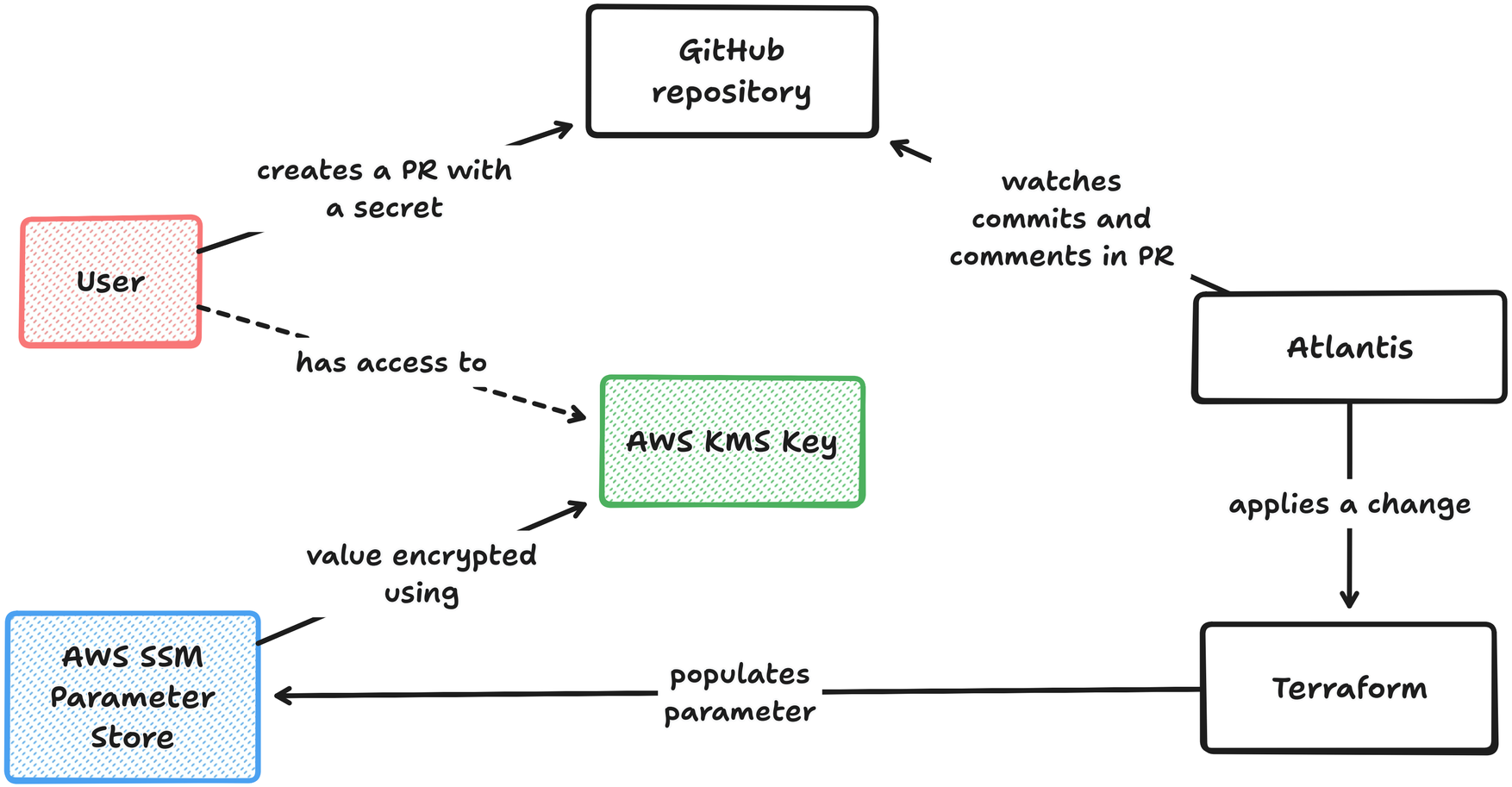
- Ansible support
- Kubernetes support
- Cloud integration

Developer-friendly

- Git + GitHub
- Workflow around Pull Request
- Transparent encryption
- 2FA support 😍

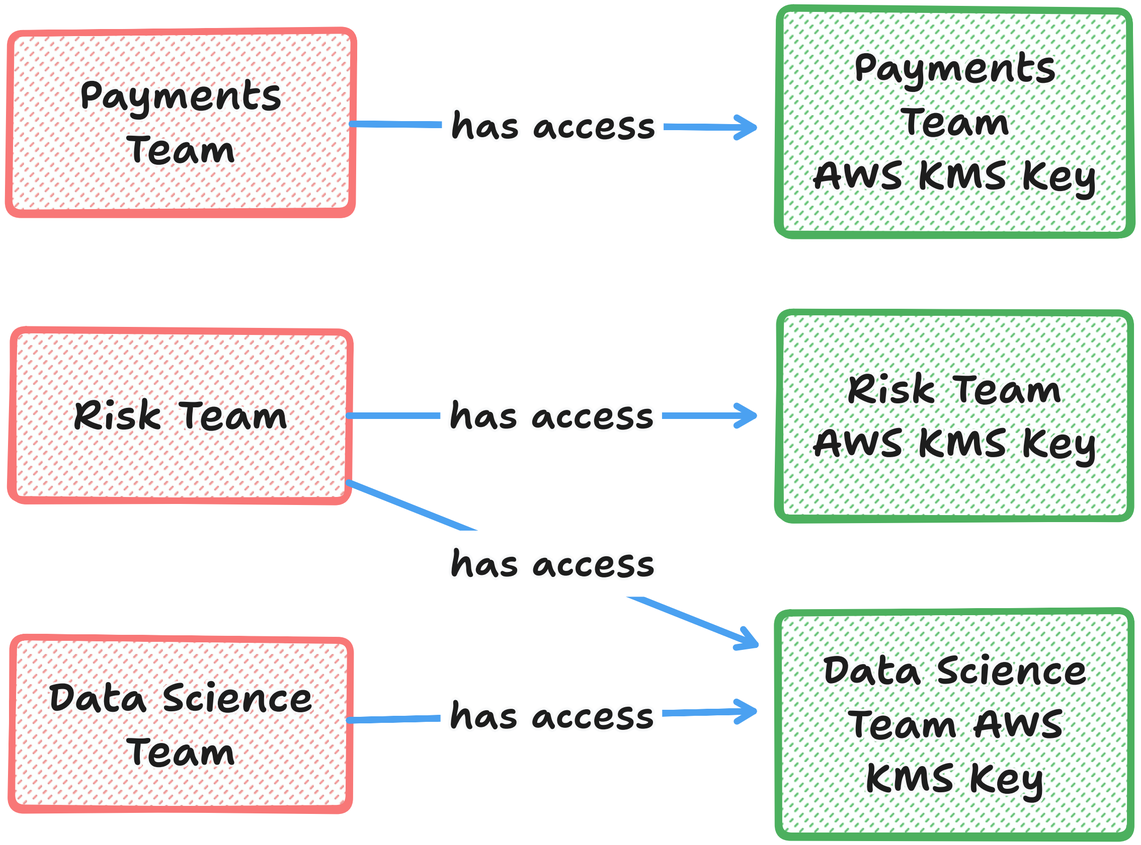
Demo

How it works

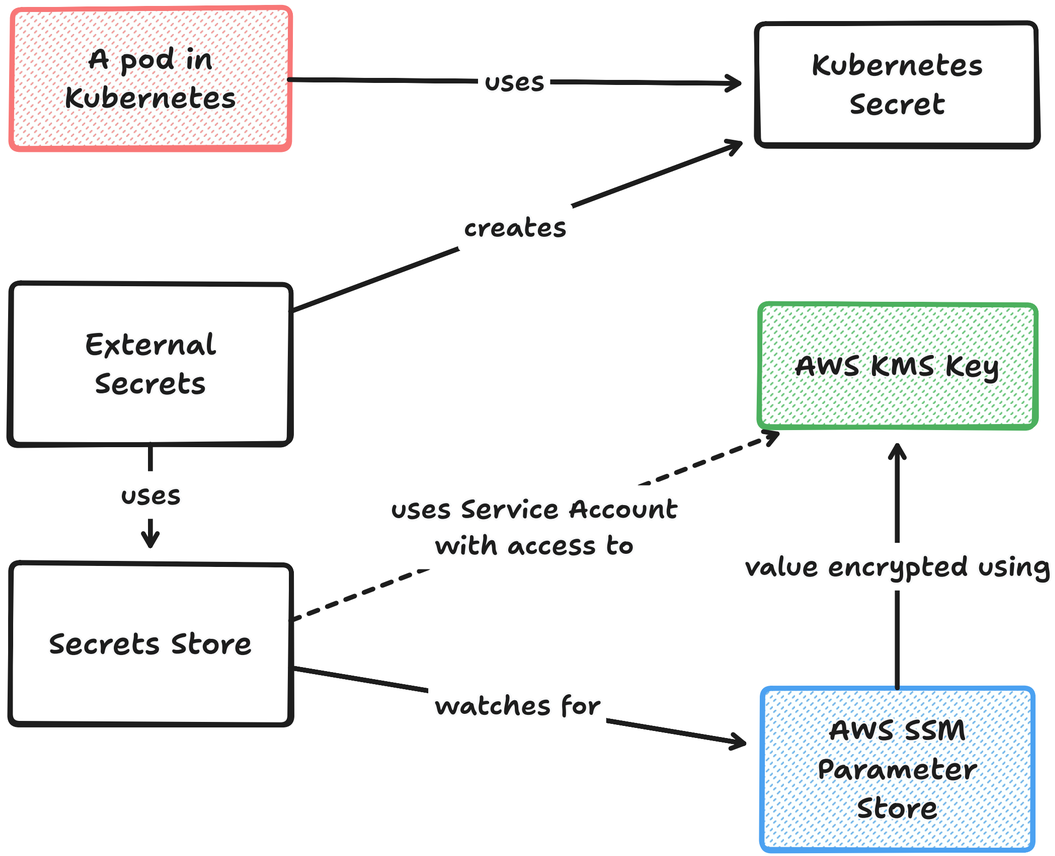

GitHub repository
creates a PR with a secret
watches commits and comments in PR
User
Atlantis
has access to
AWS KMS Key
applies a change
value encrypted using
AWS SSM Parameter Store
populates parameter
Terraform

Permissions Management

Teams / Keys



Kubernetes Secrets



Benefits

- It works and it's Cloud-native!
- Ansible compatible
- Same X as a Code benefits: rollback, audit, discussion
- AI 🤖 friendly

Downsides

- Pay attention to S3 Bucket access
- Maybe OpenTofu instead of Terraform for Encryption
- Still has lots of moving parts

Q/A

- Questions

Follow Me 👨‍🔧

- Blog https://prokopov.me
- LinkedIn: https://www.linkedin.com/in/max-prokopov/
- Twitter/X: @mprokopov