

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 🙈

Conversation 0 | Commits 1 | Checks 0 | Files changed 2

Changes from all commits | File filter | Conversations | 0 / 2 files viewed

Filter changed files

group_vaults

- all-prod.yml
- production.yml

```
... @@ -1,1334 +1,1343 @@
1 1  $ANSIBLE_VAULT;1.1;AES256
2  - 62336265613133393431366333306133303533346661373838343937366431373034323164636236
3  - 3432666263623666376662393866636133346132366238390a616463333937616234386635626135
4  - 34393932393761396634613461373931363362643533343261646635373339346362396162373839
5  - 3833653762363931390a636565316530613838646139323165386563303264366231346366383364
6  - 38376565316461393531303932613739383766373232366163306439383666336430396436336534
7  - 30623666323132636136663635643262643266653164313137633462633638376236353864313061
8  - 62616434353731306434343661666663613732393363343762623735336163333565353438333666
9  - 39383833323835343739353438343433653034633332363138636131373530636630373733353562
10 - 65343134313364366661343963323633626666306165666463613239373331386539626133633866
11 - 37316630633332326633663636616435656635633135613636306264313131646437313330303766
12 - 35663436633338643535303933336531633337366534353664346531363034633264653337303461
13 - 64323230356237343665333331376566393135393137356561653935303839333039633263653039
14 - 30323034633664616137323563616334326566626164626637316131343735306261333963623236
15 - 34613039626564343738313332336238323538373537336234323161383833623530616432306564
16 - 3065366364303331326334343236383430353337366566663396161626663323430363335373136
17 - 31396237626533393537656330326163623133663265383737393737616532313331646335316361
18 - 62336335343138386366346562646666666634656566383764396162313966363166646664346534
19 - 32633032393461363431303663636161353761656534653735393930636235396130333136646435
20 - 64373363343237623162656334633762636633396564613534623035613463643836396137346234
21 - 37323636663935333738306136616166663139313461613863646236326666613031316339386264
22 - 35376530636537646465383864336363656139306464373565393338643562363937616634356539
```

The Old Way

Ansible Vault

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

```
215 217 risky_e_crefo_secret_at: !vault |
216 218 $ANSIBLE_VAULT;1.2;AES256;neo
217 - 65383362396130373066663233343531363135656365653764326237343366326438353035383136
218 - 3436613531336161623437336230663339313665636530330a313238303536333866363638666566
219 - 31343630336634326438383366633063636531336231366363306165626530313366656230346634
220 - 3465613164613861650a316435363132323066613336666564396263643236383937383834346231
221 - 6166
219 + 65363634666436396164326638666566386464353434383037656436336233346133353734323138
220 + 3135373063393661353233373032616533373134666562310a663962356534303234353030323764
221 + 63356339336534663766663366656439326534333033663937393233636431363962306365383637
222 + 3265303131393631360a343335346132343438653435363535343733633634333334353639383261
223 + 6637
```

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/>

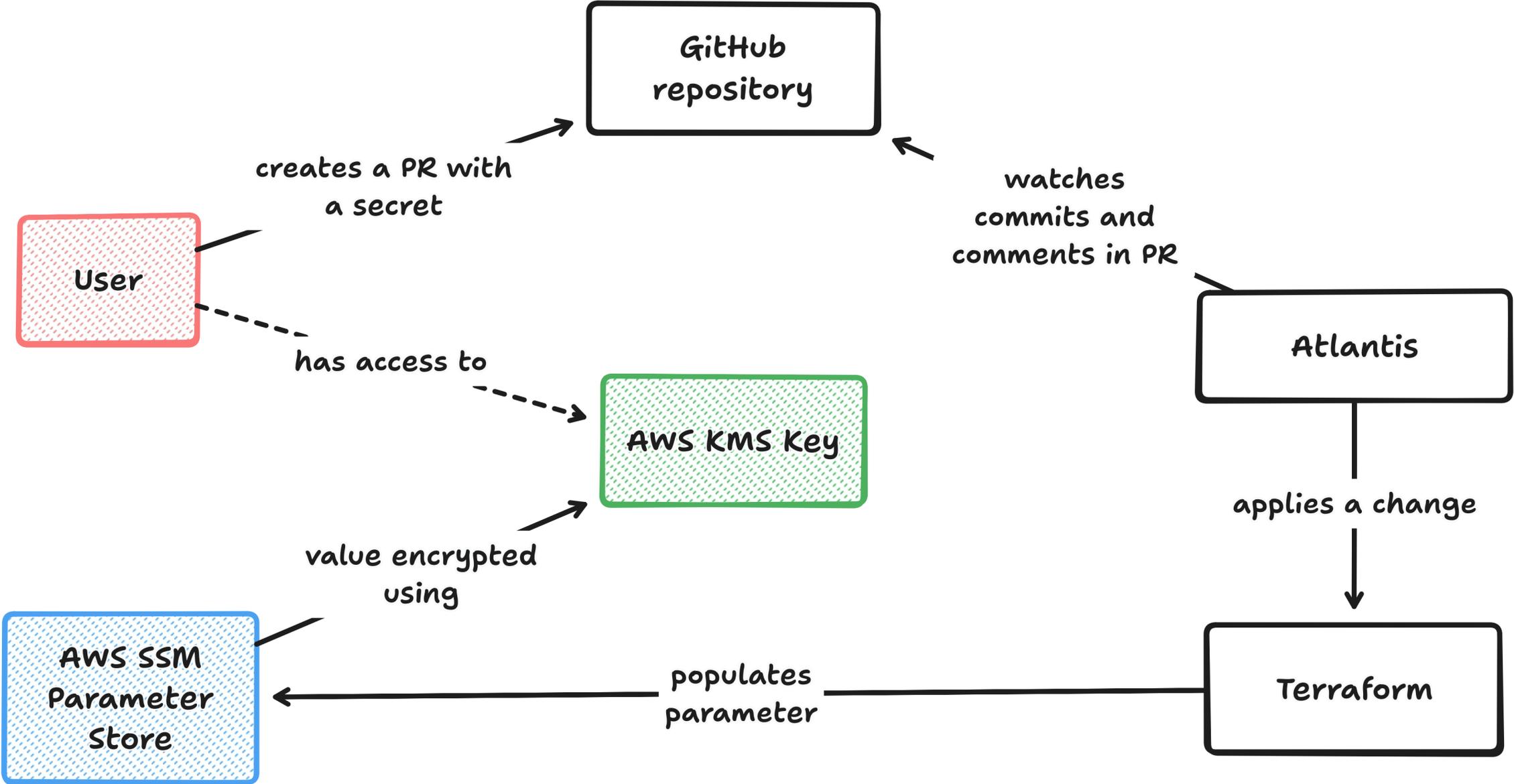
- Ansible support
- Kubernetes support
- Cloud integration

Developer-friendly

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

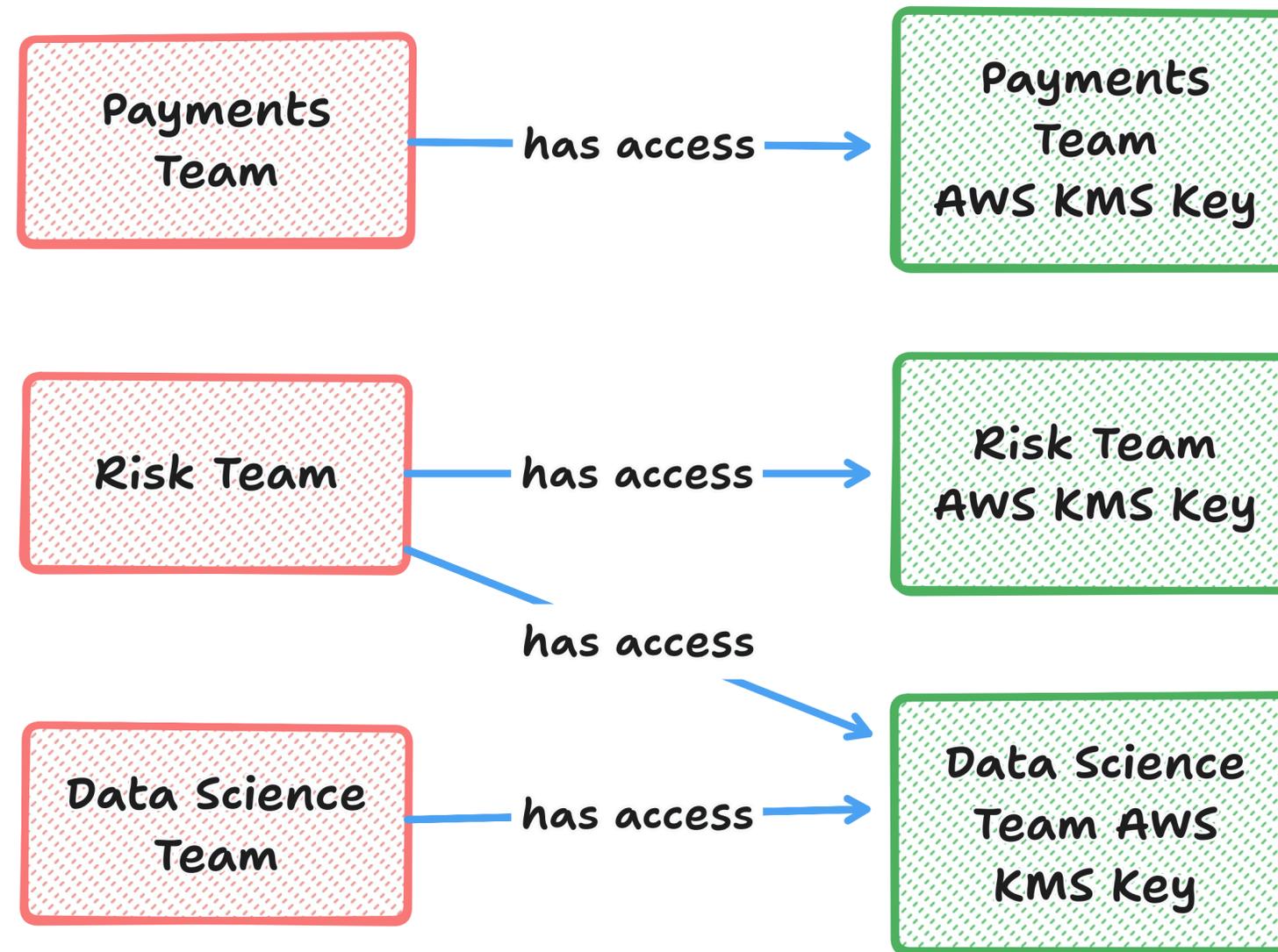
Demo

How it works

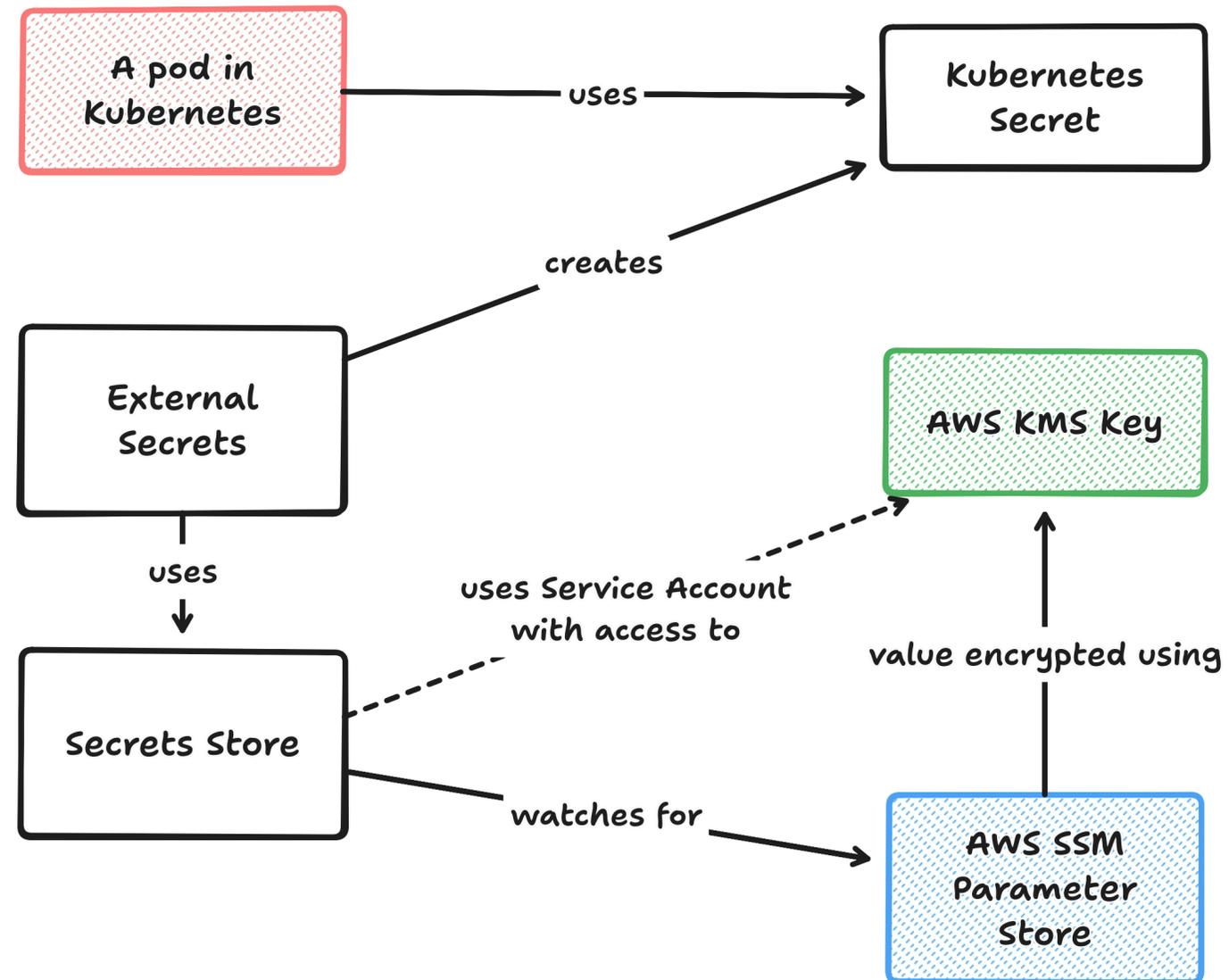


Permissions Management

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