Working with Secrets

Ned Bellavance
MICROSOFT AZURE MVP

@ned1313 | nedinthecloud.com

Summary

Secret lifecycle

Key value secrets

Secrets engines

Dynamic secrets

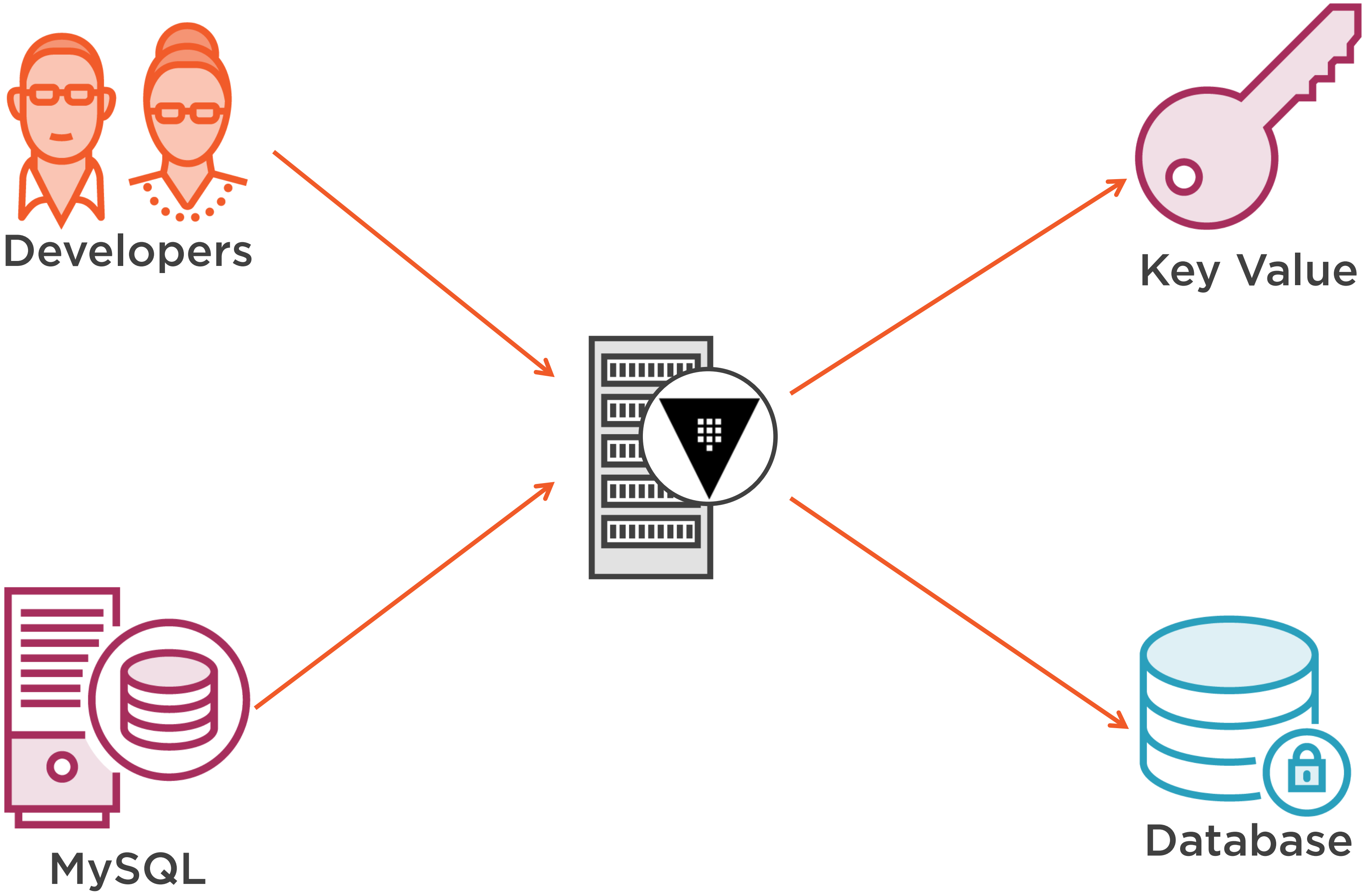
Secrets Lifecycle

- Create
- Read
- Update
- Delete
- Destroy
- Metadata Destroy

Key Value Secrets

Version 1	Version 2
No versioning, last key wins	Versioning of past secrets
Faster with fewer storage calls	Possibly less performant
Deleted items are gone	Delete items and metadate retained
Can be upgraded to version 2	Cannot be downgraded
Default version on creation	Can be specified at creation

Globomantics Scenario



Secrets Engines

Store, generate, encrypt data

AWS, Database, Active Directory, PKI, SSH

Lifecycle: Enable, Disable, Move, Tune

Vault Paths

API rules everything

Everything is a path

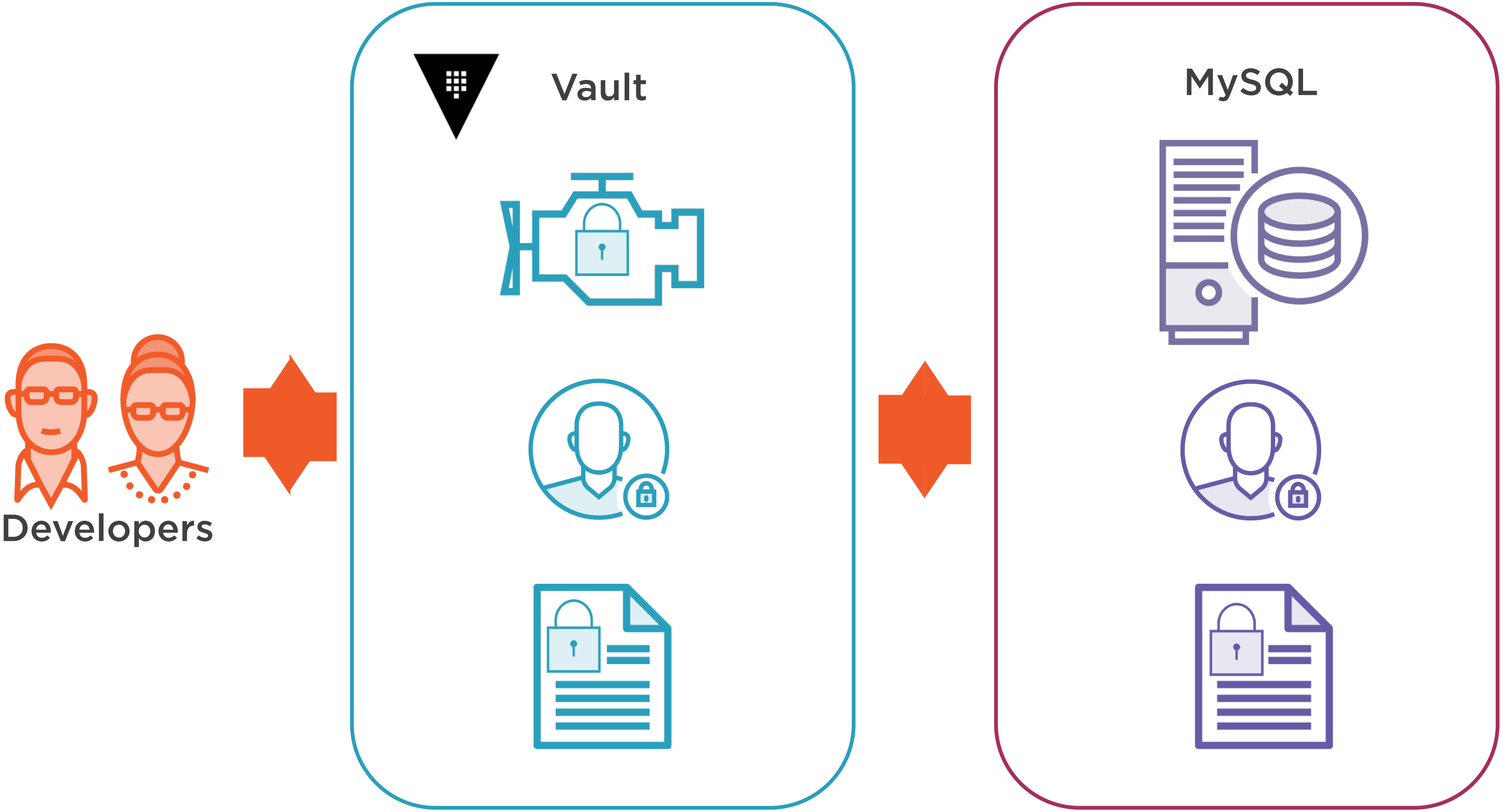
Enables path-help

API docs or bust

Working with Secrets Engines

```
#Enable a secrets engine

vault secrets enable [options] TYPE

#Disable a secrets engine

vault secrets disable [options] PATH

#Move a secrets engine

vault secrets move [options] SOURCE DESTINATION

#Tune a secrets engine

vault secrets tune [option] PATH
```

Database Secrets Engine



Dynamic Secrets

Create secrets on demand

Lease issued for each secret

Lease sets validity period

Control renewal and revocation

Conclusion

Secrets are more than key/value pairs

Secrets engines make Vault extensible

Dynamic secrets are kinda awesome

Coming up:

- Controlling Access in Vault