DATENSCHUTZ IN DER CLOUD MIT SPRING CLOUD VAULT

25.4.2018

Präsentation und Demos:
https://github.com/andifalk/jax-2018-spring-vault

ANDREAS FALK (@ANDIFALK)

NovaTec Consulting GmbH (Stuttgart/Germany)

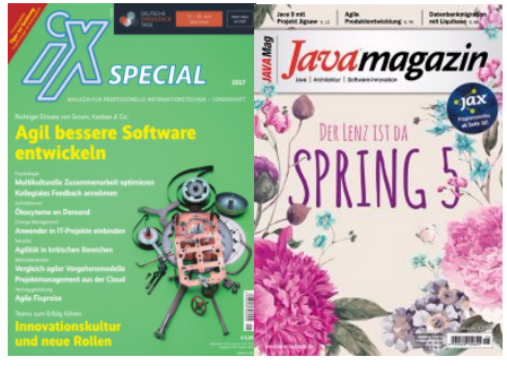
NOVATEC
make IT happen!

jax

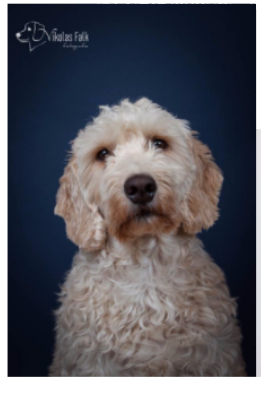
spring I O

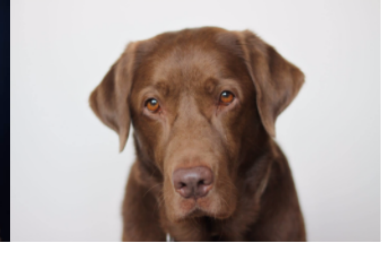
APPSEC EUROPE
ROMA MMXVI

CLOUD FOUNDRY
SUMMIT 2017
OCTOBER 11-12
SWITZERLAND



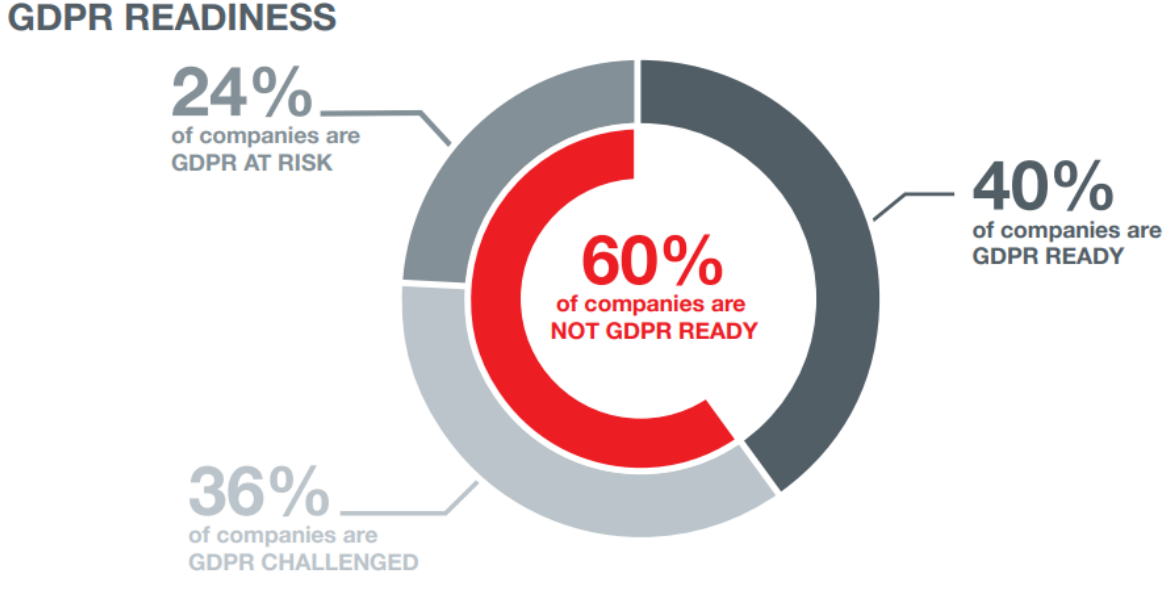
SUPPORTER
OWASP.ORG
2017
owasp.org





EU DATENSCHUTZ GRUNDVERORDNUNG (DSGVO / GDPR)

Ab 25.Mai 2018 geltendes Recht!



Quelle: GDPR's Missing Link Report (senzing.com/gdpr)

ARTIKEL 32

(SICHERHEIT DER VERARBEITUNG)

“ Unter Berücksichtigung des Stands der Technik, ... treffen der Verantwortliche ...geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten... ”

Quelle: eur-lex.europa.eu

A3: SENSITIVE DATA EXPOSURE

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://github.com/OWASP/Top10

TYPICAL SENSITIVE DATA

PASSWORDS

SERVICE CREDENTIALS (DB, MESSAGING, ...)

OAUTH2 CLIENT SECRETS

ENCRYPTION KEYS

CREDIT CARD NUMBERS

PERSONAL DATA

APPLICATION.YAML

DATABASE ACCESS CREDENTIALS

```
spring:
    datasource:
        url: jdbc:postgresql://localhost/test
        username: root
        password: mysupersecretpassword
```

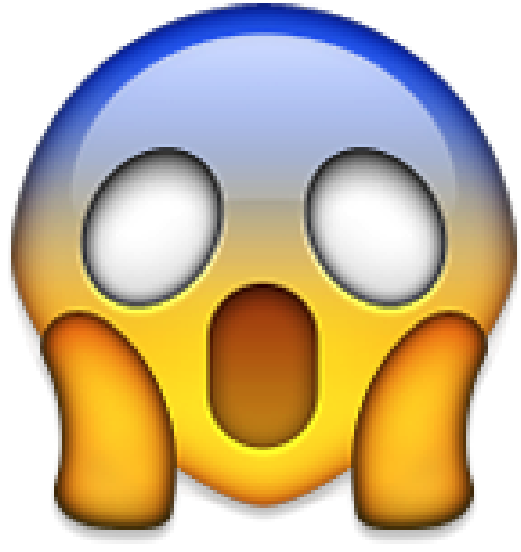
KEY MANAGEMENT

How to protect the key encrypting key?

“THERE IS NO ALIEN TECHNOLOGY TO MITIGATE ALL THE RISKS”

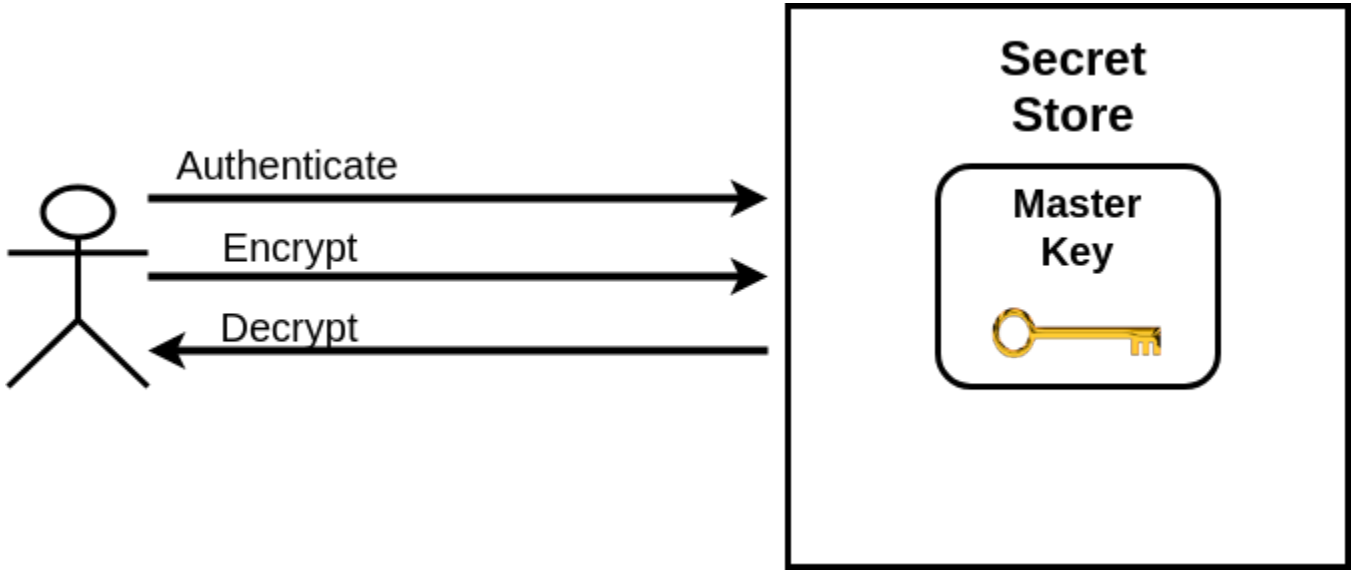
Justin Smith (CSO @ Pivotal)

https://youtu.be/MvPIthr4kXA

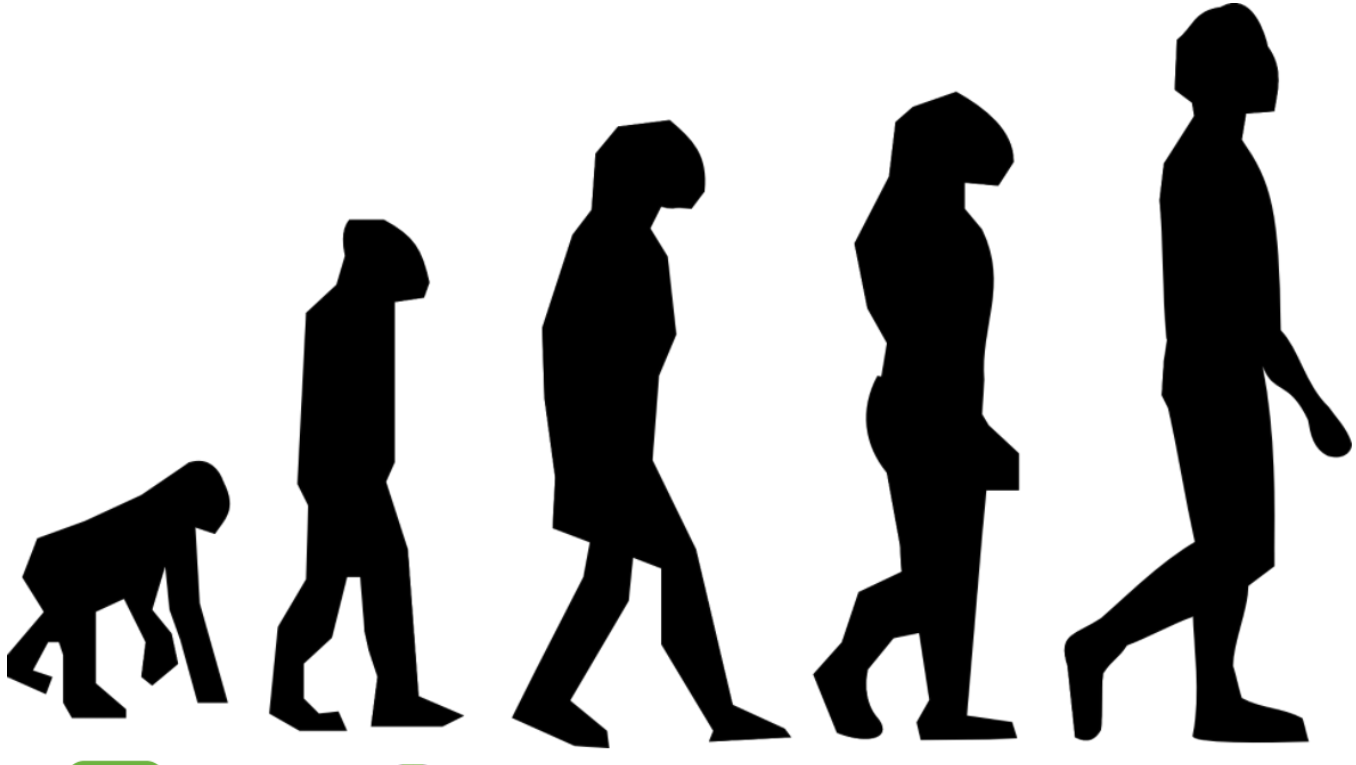


KEY MANAGEMENT

Authentication



DATA SECURITY EVOLUTION



INTRODUCTION

https://www.vaultproject.io

“A Security Swiss Army Knife”

Jeff Mitchell, Vault Lead, HashiCorp

A TOOL FOR MANAGING SECRETS LIKE...

- Tokens
- Passwords
- MFA
- X.509 Certificates
- API keys
- DB credentials

KEY FEATURES

SECURE SECRET STORAGE

DYNAMIC SECRETS

DATA ENCRYPTION (AES CYPHER)

LEASING, RENEWAL & REVOCATION

OPERATIONAL FEATURES

AUTHENTICATION

AUTHORIZATION (ACL)

AUDIT LOGS

HIGH AVAILABILITY MODE (HA)

WEB UI (SINCE V.0.10)

AUTHORIZATION (ACL)

my-policy.json

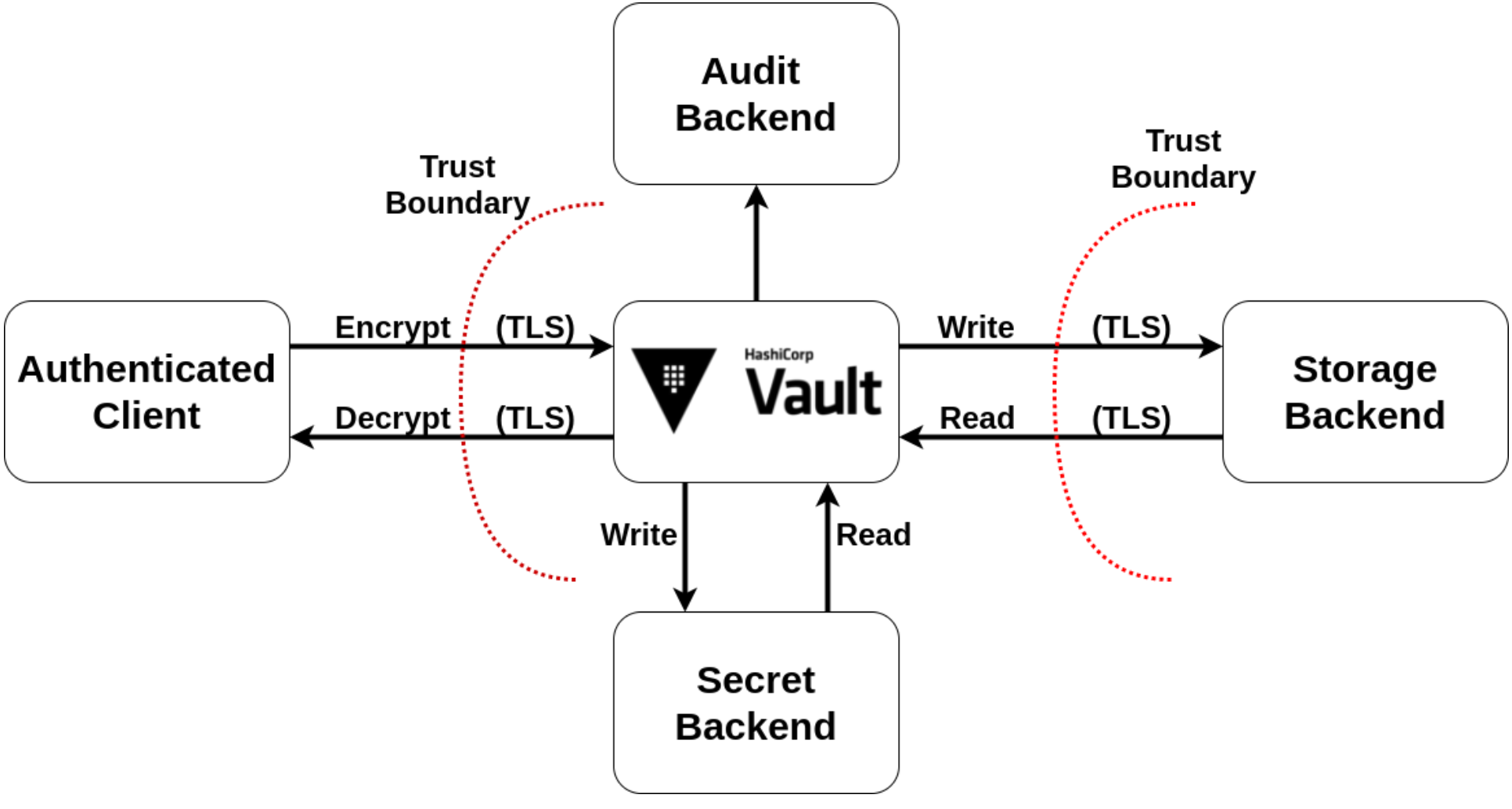
```
path "secret/*" {
  capabilities = [
    "create", "read", "update",
    "delete", "list"
  ]
}

path "secret/super-secret" {
  capabilities = ["deny"]
}
```

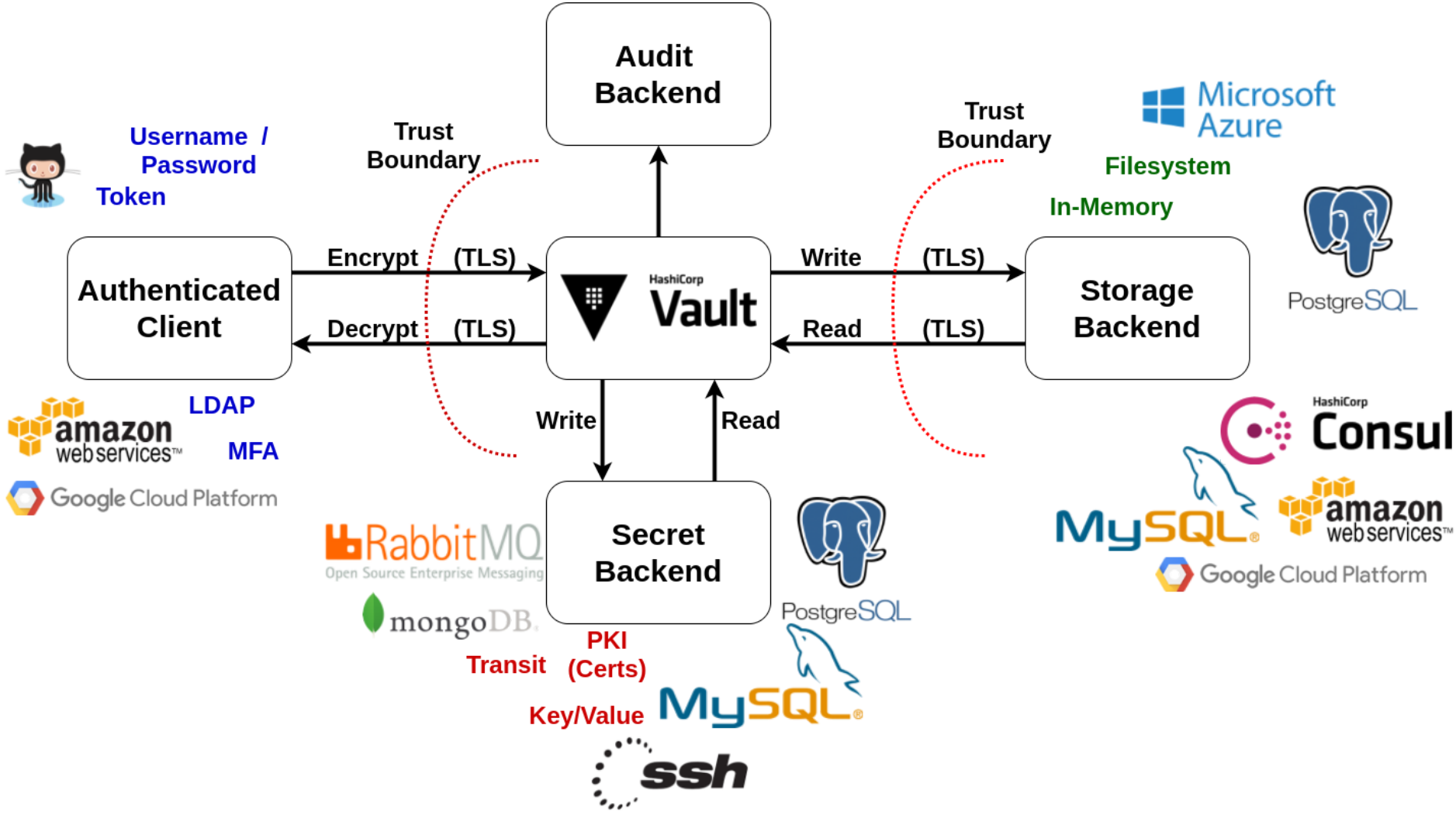
```
$ vault write sys/policy/my-policy policy=@my-policy.json
```

```
$ vault token create -policy=my-policy ...
```

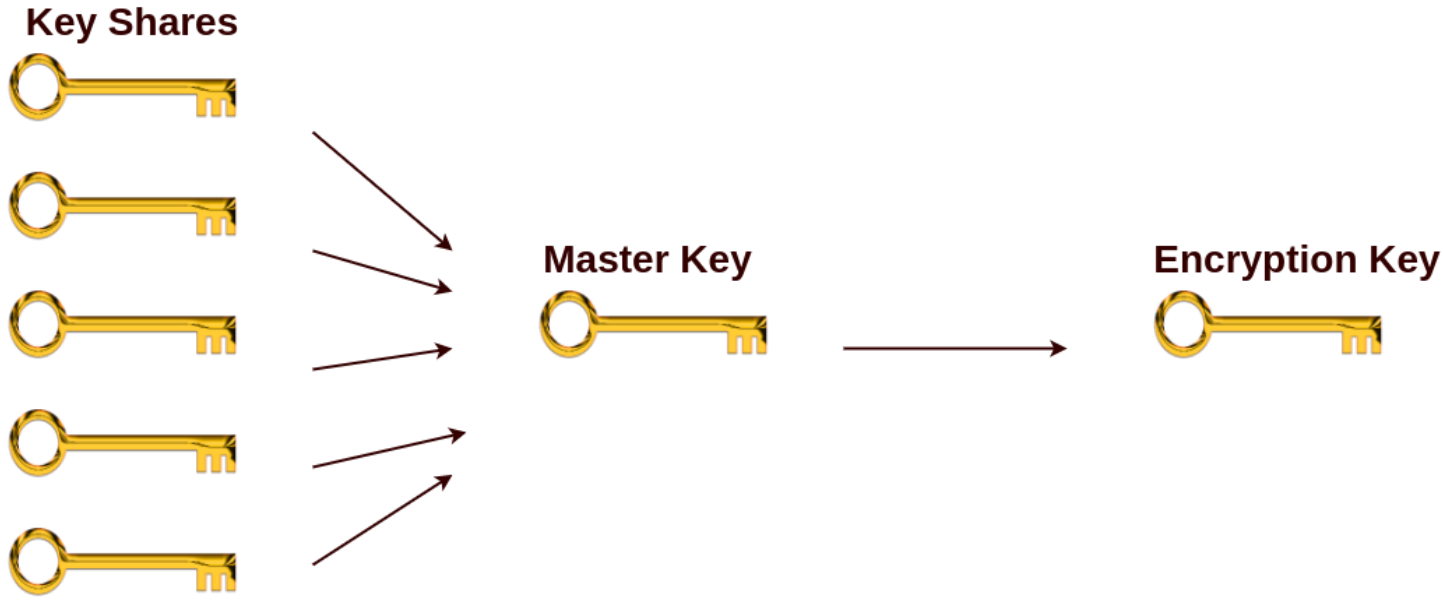
ARCHITECTURE I



ARCHITECTURE II



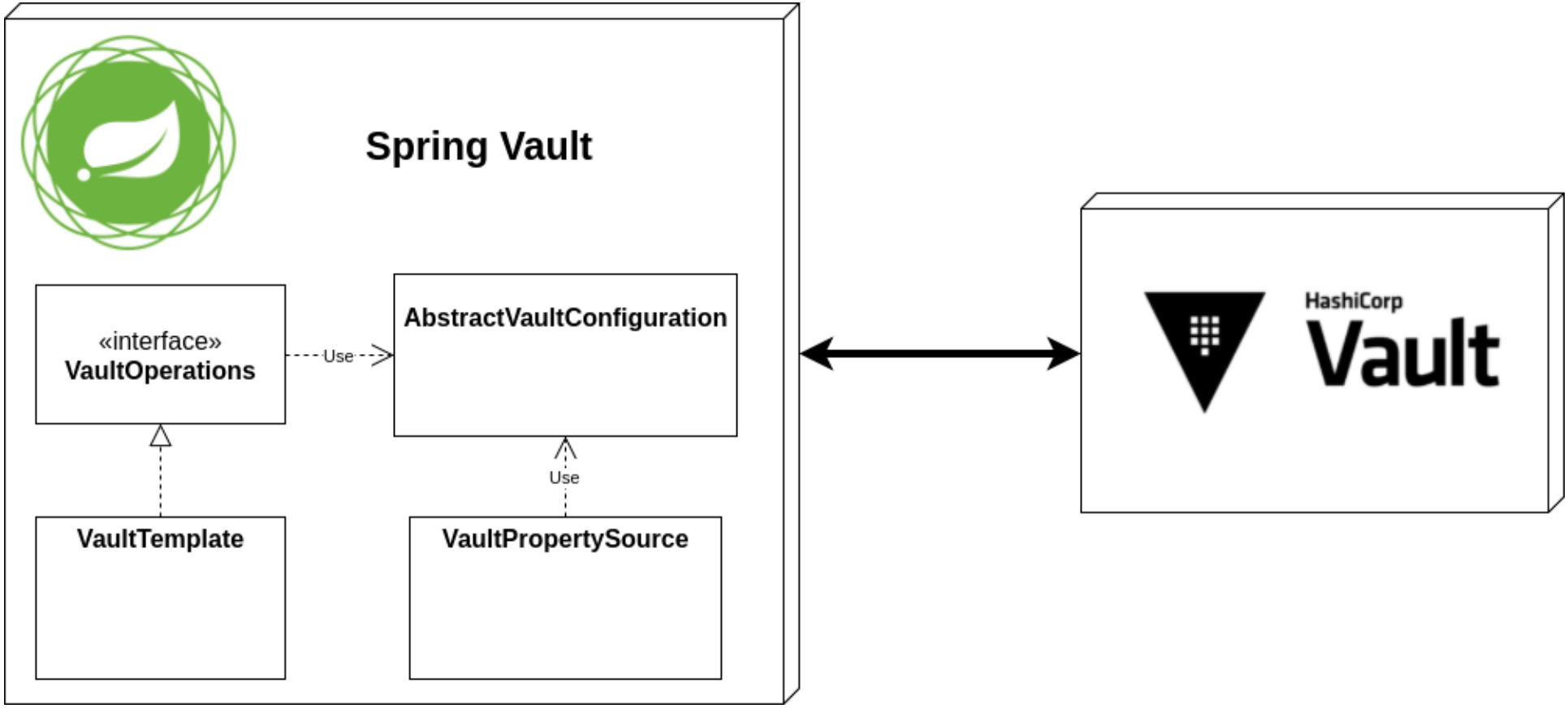
KEY SHARES



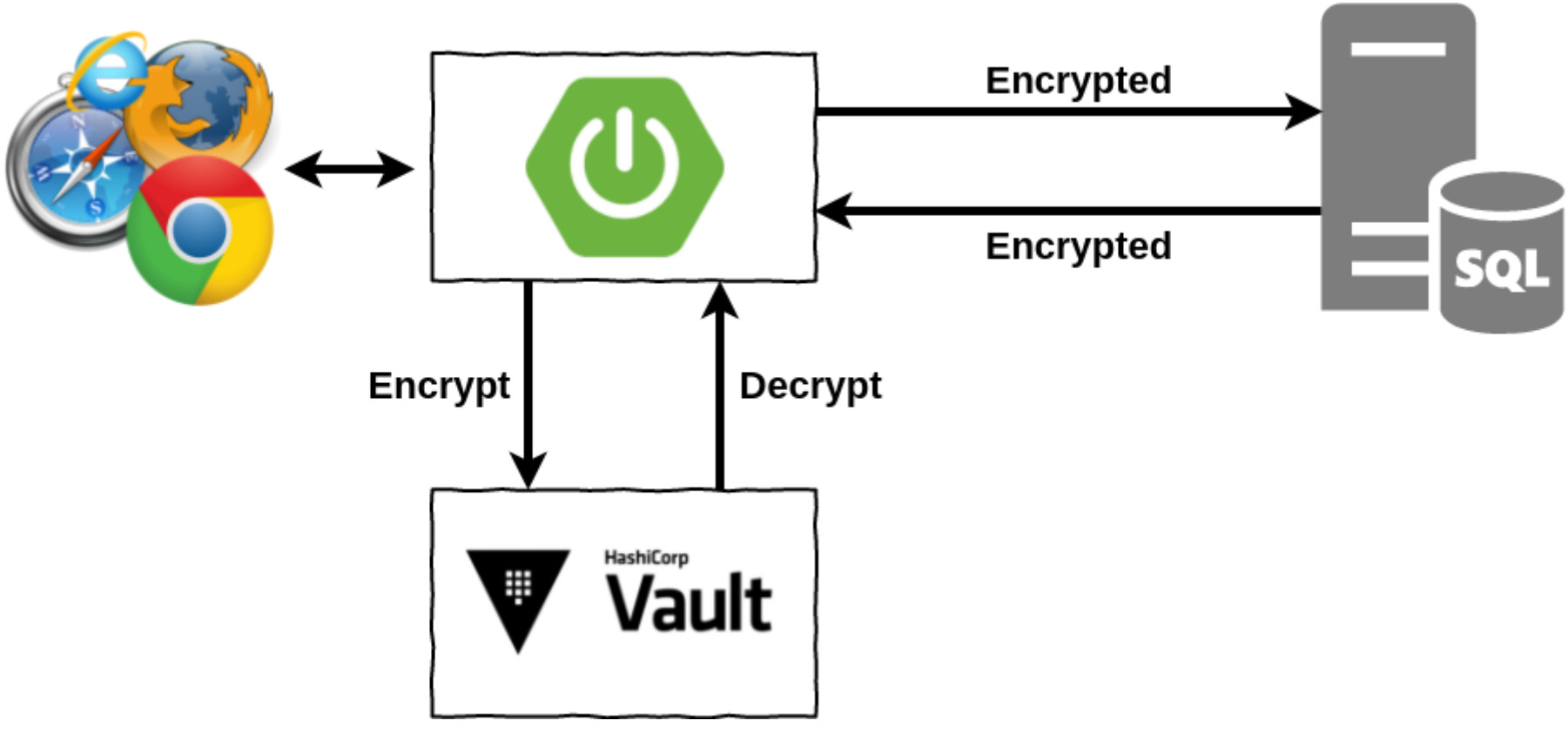
https://www.cs.tau.ac.il/~bchor/Shamir.html

SPRING VAULT

https://projects.spring.io/spring-vault

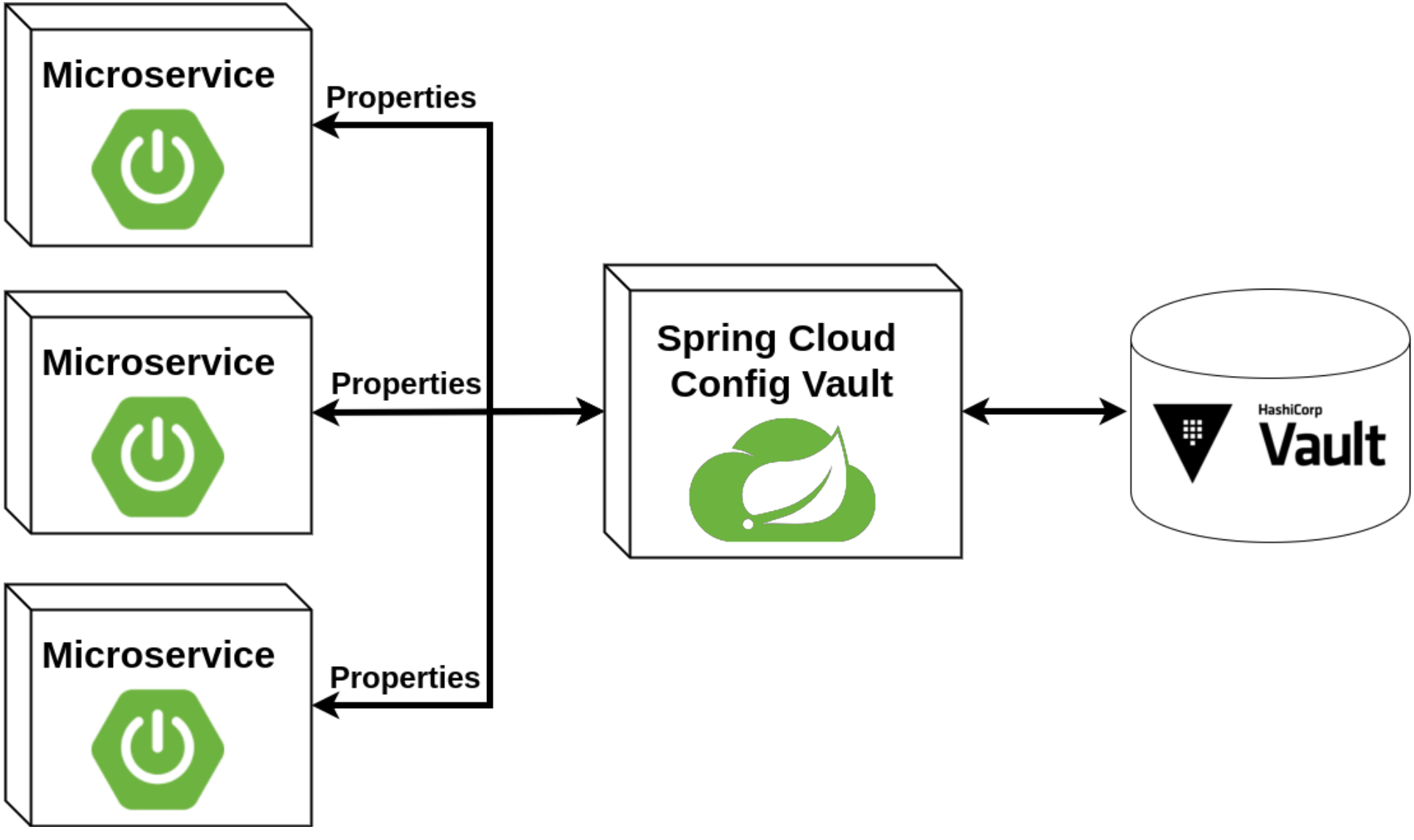

Spring Vault
«interface»
VaultOperations
Use
AbstractVaultConfiguration
Use
VaultTemplate
VaultPropertySource
HashiCorp
Vault

ENCRYPTION AS A SERVICE



SPRING CLOUD VAULT

https://cloud.spring.io/spring-cloud-vault


Microservice
Properties
Microservice
Properties
Microservice
Properties
Spring Cloud
Config Vault
HashiCorp
Vault

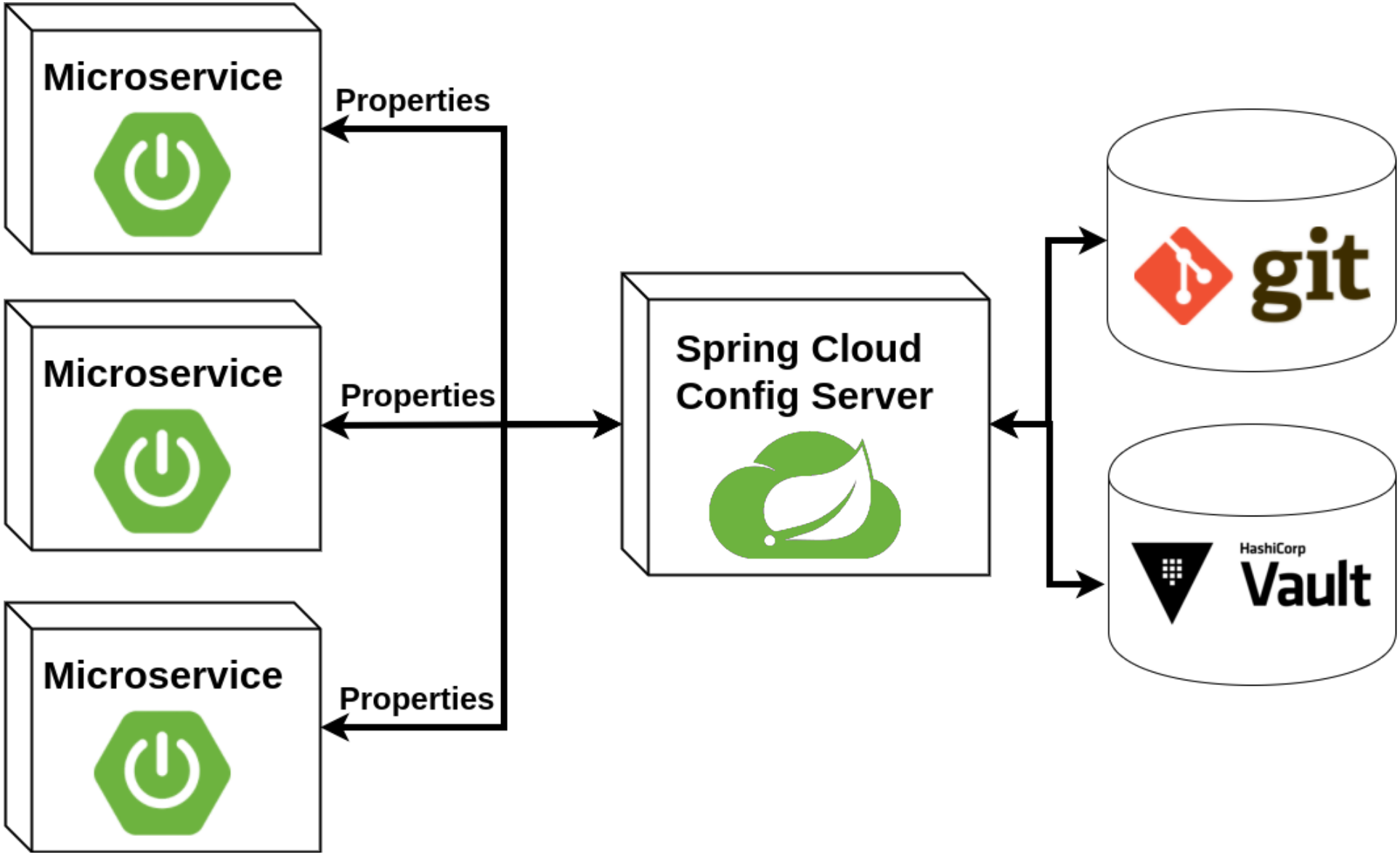
SECRET VAULT MAPPING

BOOTSTRAP.PROPERTIES

```
spring.cloud.vault.generic.application-name =
        application1,additional/keys
#spring.cloud.vault.application-name = ...
#spring.application.name = ...
```

MAPPED SECRET PATHS IN VAULT

```
/secret/application1
/secret/application1/myprofile
/secret/additional/keys
/secret/application
/secret/application/myprofile
```


Microservice
Properties
Microservice
Properties
Microservice
Properties
Spring Cloud
Config Server
git
HashiCorp
Vault

SPRING CLOUD CONFIG VAULT ENVIRONMENT REPOSITORY

APPLICATION.PROPERTIES (CONFIG SERVER)

```
spring.profiles.active=git,vault
spring.cloud.config.server.vault.host=127.0.0.1
spring.cloud.config.server.vault.port=8200
spring.cloud.config.server.vault.scheme=https
```

BOOTSTRAP.PROPERTIES (CLIENT)

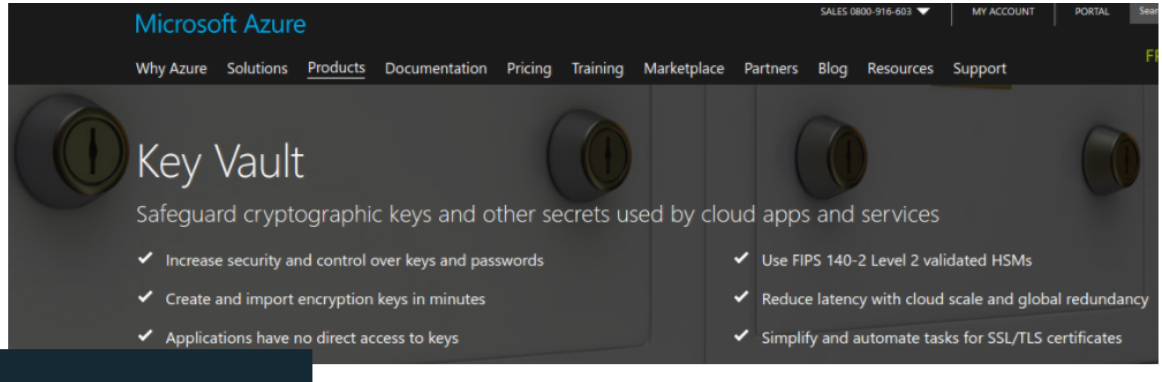
```
spring.cloud.config.token = YourVaultToken
```

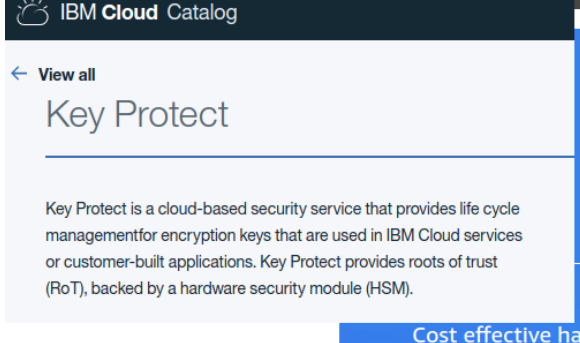
ALTERNATIVES

Azure Key Vault

CredHub (Pivotal)

Hardware Security Modules (HSM)





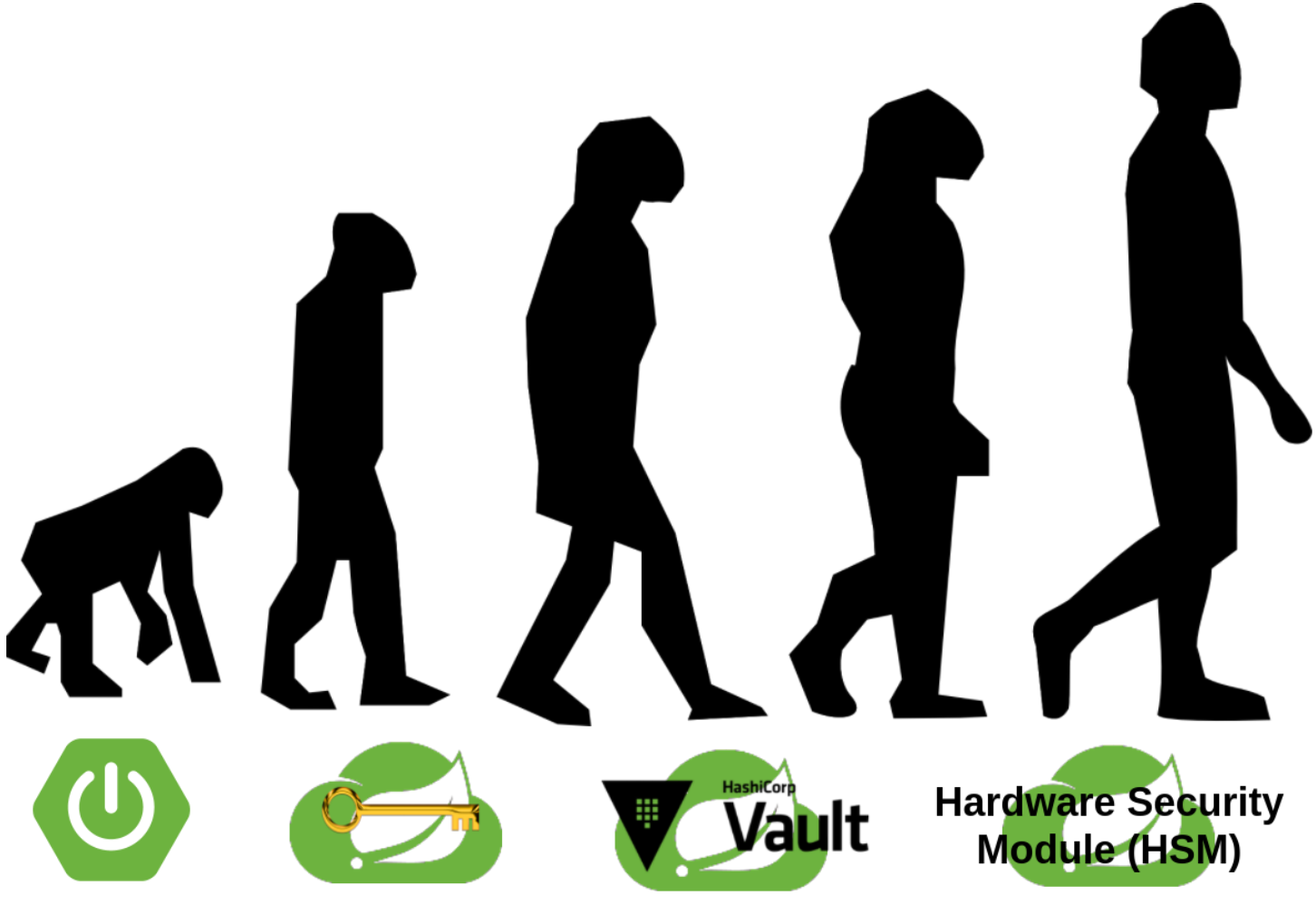
BUT HSM...

...not Cloud Friendly or...

...quite expensive (AWS ~ 18000 $/year)

...and not 100% secure (“Confused Deputy”)

NO SILVER BULLETS!!



Q&A

http://blog.novatec-gmbh.de

andreas.falk@novatec-gmbh.de

@andifalk

@Spring I/O (Barcelona)
24.5.2018
Spring Security 5.0 Hands-On Workshop

REFERENCES

- Vault (https://www.vaultproject.io)
- Shamir's secret sharing (https://en.wikipedia.org/wiki/Shamir's_Secret_Sharing)
- Spring Cloud Config (https://cloud.spring.io/spring-cloud-config/)
- Spring Vault (https://projects.spring.io/spring-vault)
- Spring Cloud Vault (https://cloud.spring.io/spring-cloud-vault)
- Sources and Presentation (https://github.com/andifalk/jax-2018-spring-vault)