SCYTALE

spiffe

Intro: SPIFFE
A developer's tour of the SPIFFE project

Andrew and Dan from Scytale
KubeCon North America, December 2018

SCYTALE

About us...

SCYTALE

Andrew Jessup

Recovering engineer @ Scytale

@whenfalse

Dan Feldman

Software engineer @ Scytale

@d_feldman

Today

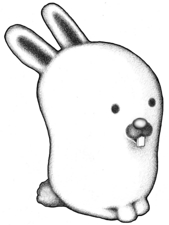
A short history of SPIFFE

What SPIFFE solves for

SVIDs, Workload API and Federation

How to use SPIFFE

What’s Next & Get Involved



11th USENIX Security Symposium (2002)

Plan9 security design published

GlueCon 2016

Joe Beda proposes SPIFFE

April 2018

CNCF welcomes SPIFFE & SPIRE

Circa 2005

Google rolls-out LOAS

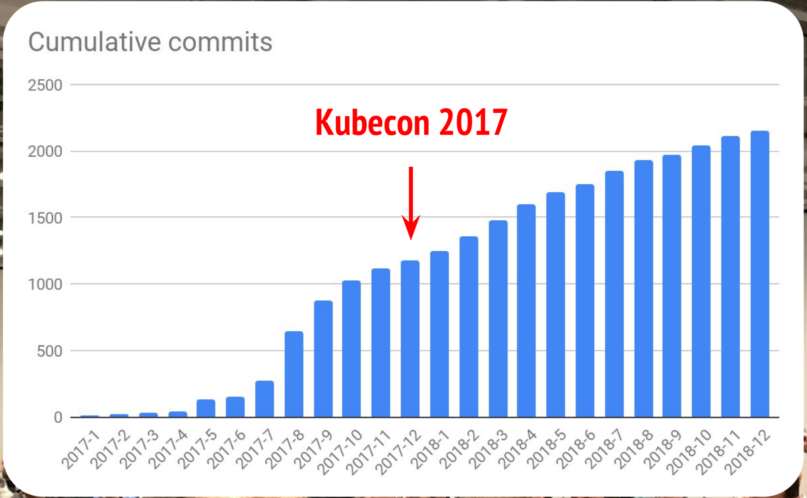
KubeCon NA 2017

SPIFFE & SPIRE 0.1 are released

spiffe

SCYTALE

Project growth



With thanks to our fantastic open-source community

Mark Lakewood Twilio	**Matthew McPherrin** Square	**Matt Moyer** Heptio	**Andreas Zitzelsberger** QAware
Spike Curtis Tigera	**Neel Shah** VMWare	**Guy Templeton** Skyscanner	**John Gelsey** Xnor.ai
Jon Debonis Blend	**Adam Bozanich** Overclock Labs	**Enrico Schiattarella** Pensando	**And many more!**

Today

SCYTALE

A short history of SPIFFE

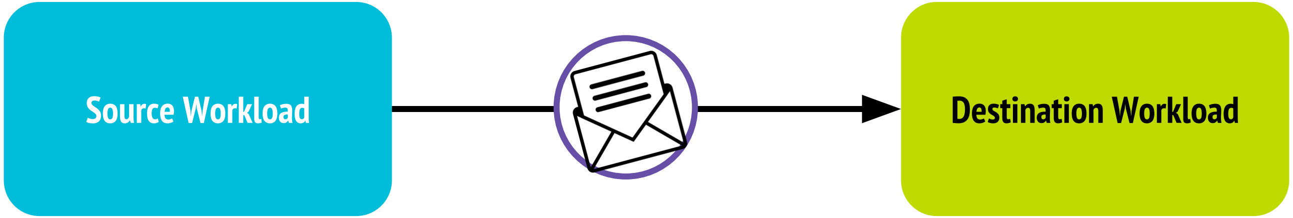
What SPIFFE solves for

SVIDs, Workload API and Federation

How to use SPIFFE

What’s Next?

SPIFFE delivers trusted identities to software systems

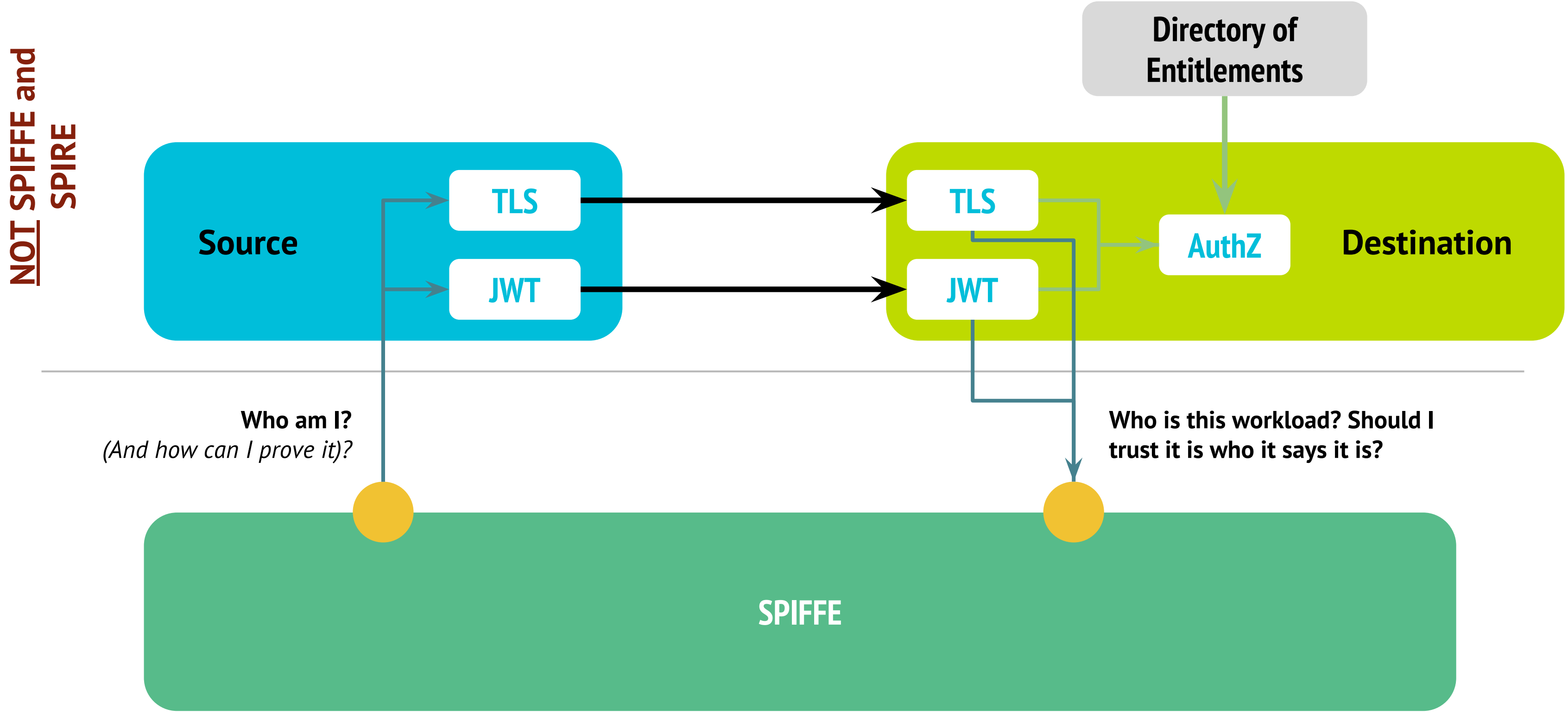


“Do I believe the source workload is who it says it is?”

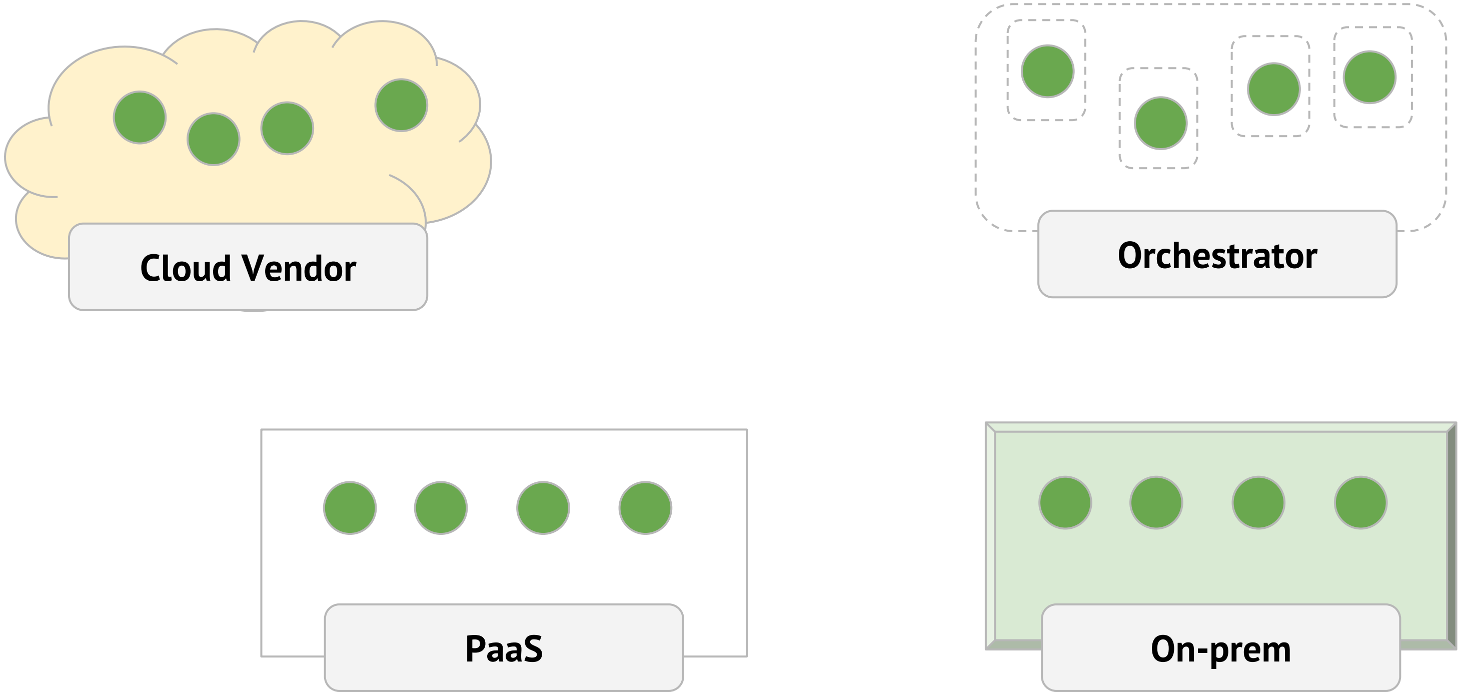
“Do I believe the legitimacy of the message I received?”

Identity is the *basis for* AuthN and AuthZ

SCYTALE


NOT SPIFFE and SPIRE
Directory of Entitlements
Source
TLS
JWT
TLS
JWT
AuthZ
Destination
Who am I?
(And how can I prove it)?
Who is this workload? Should I trust it is who it says it is?
SPIFFE

Modern software is complex and heterogeneous



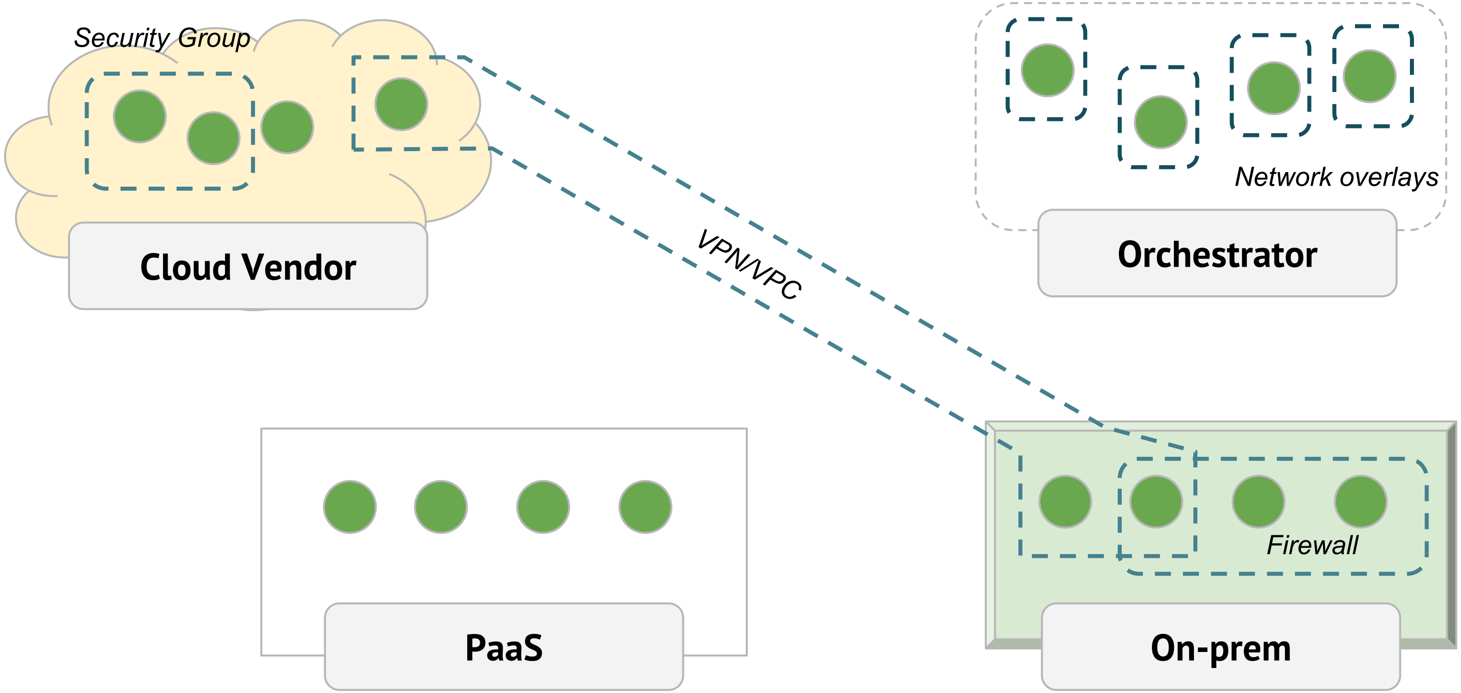
Cloud Vendor

Orchestrator

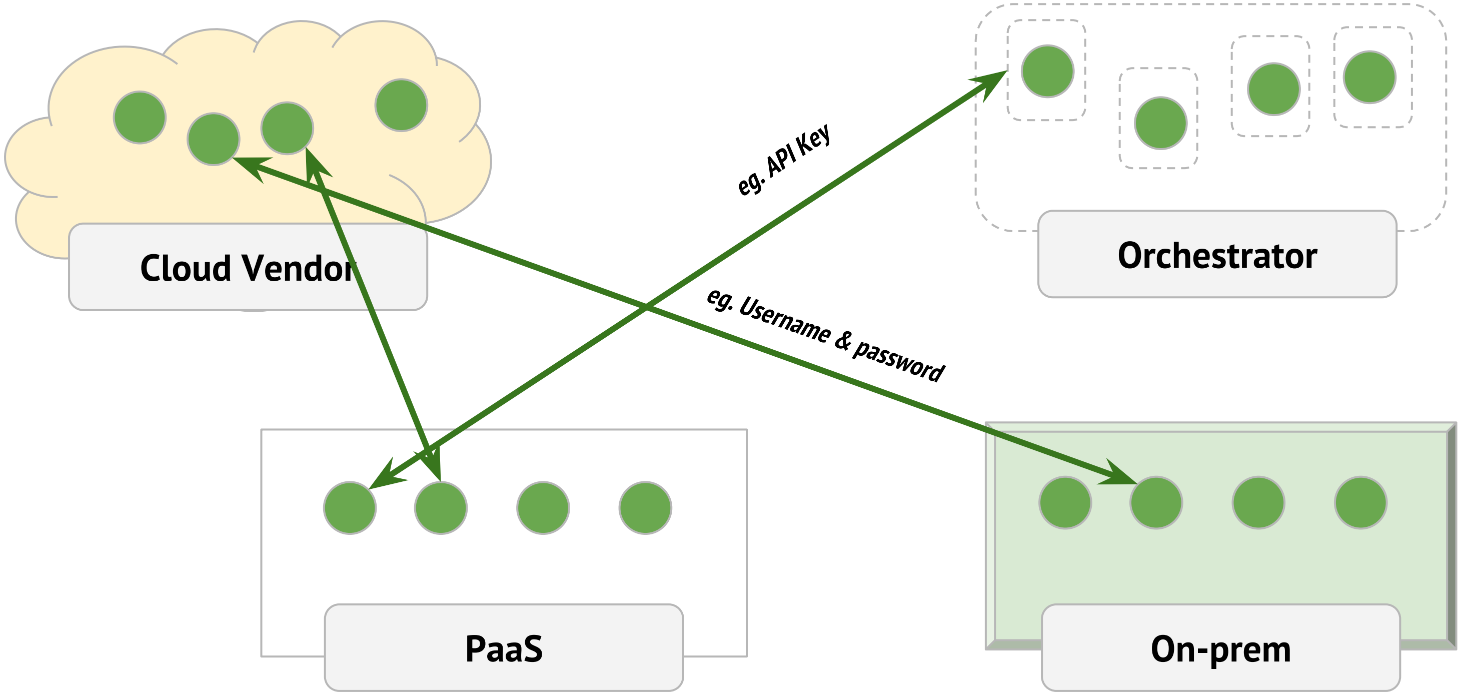
PaaS

On-prem

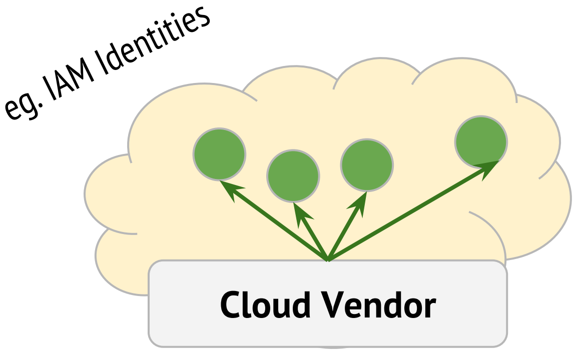
Workload identity? Use the network?

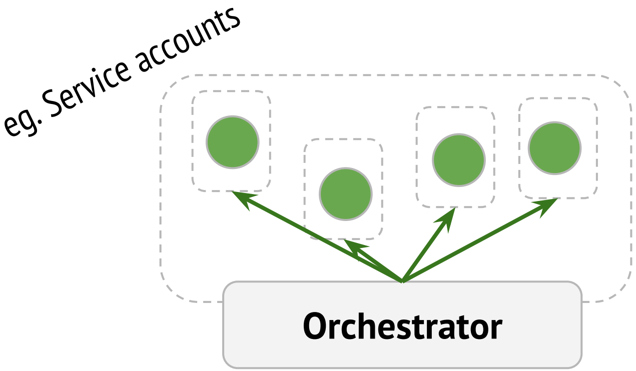


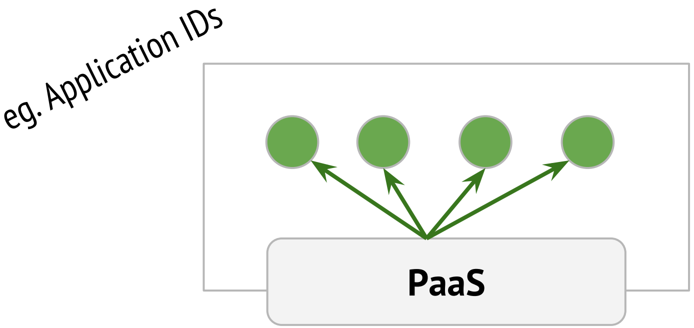
Workload identity? Shared secrets?

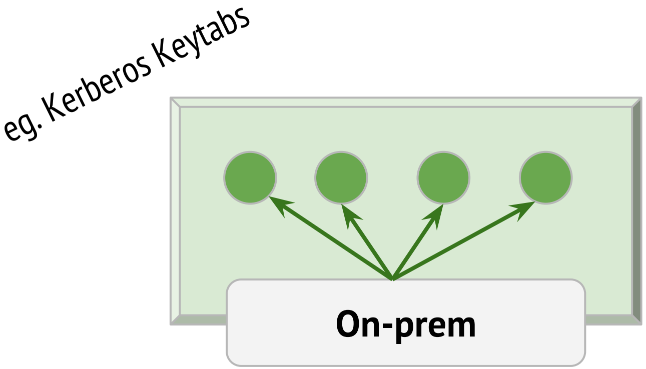


Workload identity? Ask my platform?

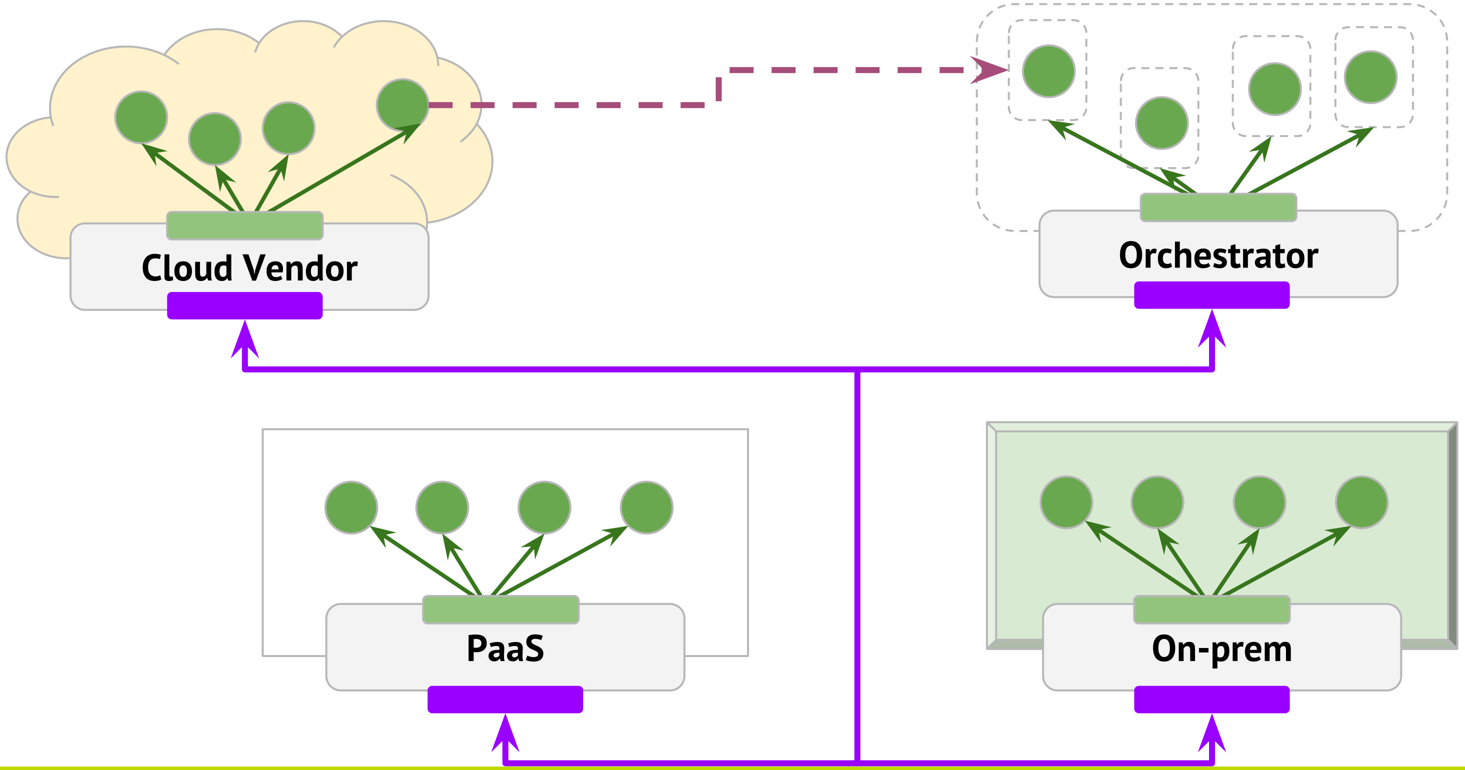




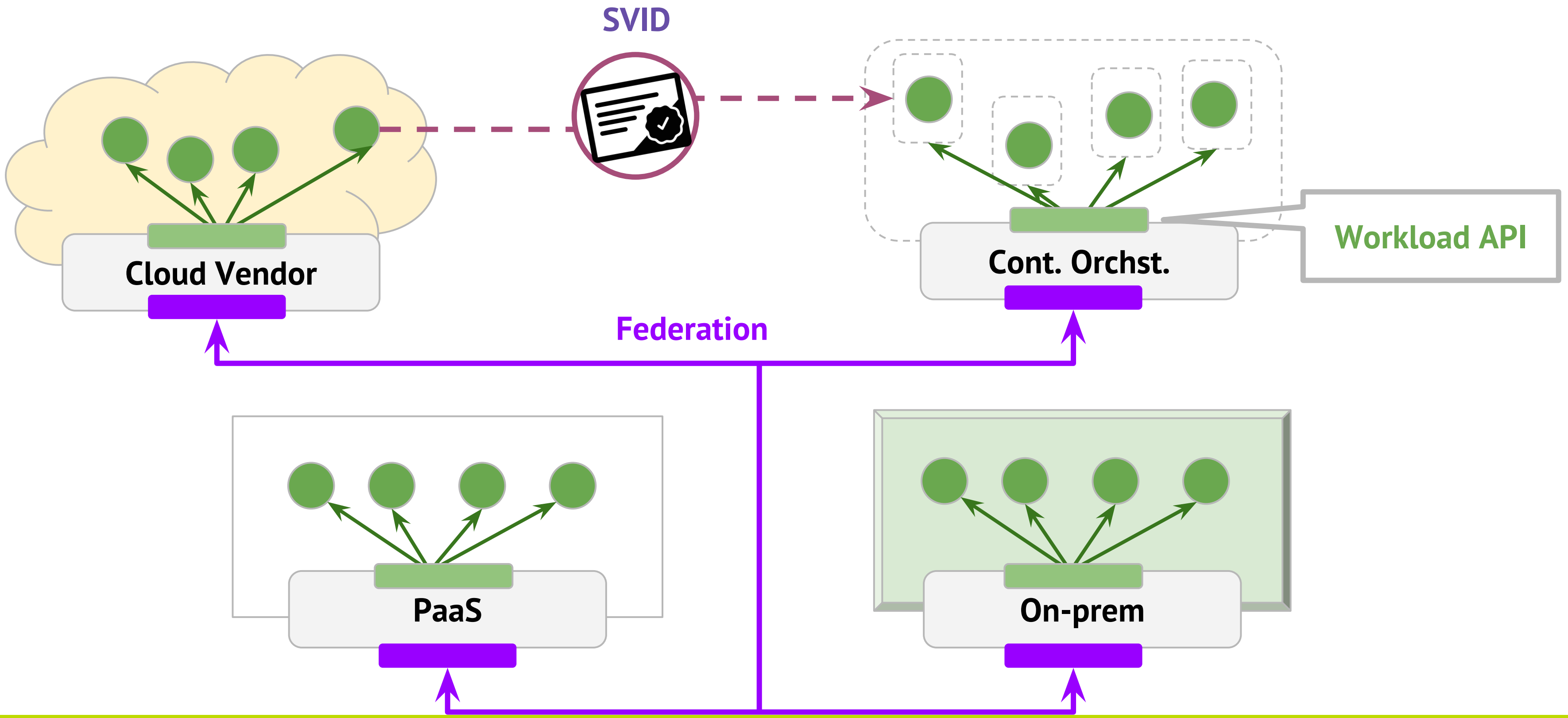




SPIFFE: Federated, platform-mediated, vendor neutral identity



SPIFFE: Federated, platform-mediated, vendor neutral identity



SPIFFE Issuers

SPIRE
(Full implementation)

HashiCorp Consul Connect
(Partial implementation)

Istio Citadel
(Partial implementation)

SPIFFE Consumers

HashiCorp Vault
Secret store

Knox
Secret store

Ghostunnel
Proxy

nginx
Web server and proxy

Envoy
Proxy

?

Your code
Using libraries

Today

A short history of SPIFFE

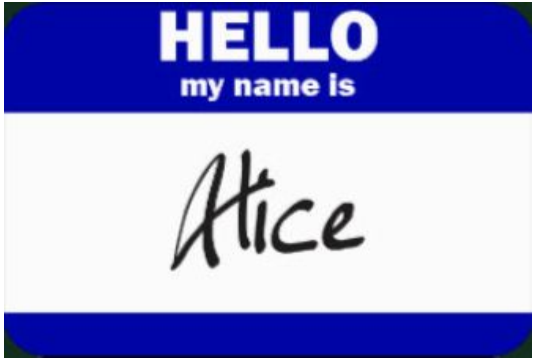
What SPIFFE solves for

SVIDs, Workload API and Federation

How to use SPIFFE

What's Next?

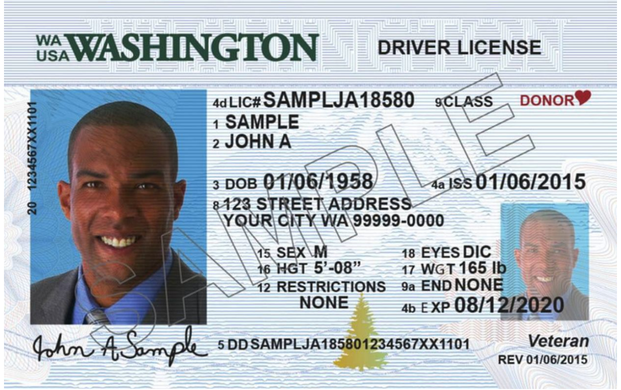
What is an SVID?



HELLO

my name is

Alice



WA USA WASHINGTON DRIVER LICENSE

4d LIC# SAMPLJA18580 9 CLASS DONOR

1 SAMPLE

2 JOHN A

3 DOB 01/06/1958 4a ISS 01/06/2015

8 123 STREET ADDRESS

YOUR CITY WA 99999-0000

15 SEX M 18 EYES DIC

16 HGT 5'-08" 17 WGT 165 lb

12 RESTRICTIONS NONE 9a END NONE

4b EXP 08/12/2020

20 1234567XX1101

John A Sample

5 DD SAMPLJA185801234567XX1101

Veteran

REV 01/06/2015

Identity documents are:

- Unique
- Static
- Verifiable
- Attested by a trusted authority

What is an SVID?

spiffe://acme.com/billing/payments

A SPIFFE ID

X.509-SVID describes exactly how to encode a SPIFFE ID in an X.509 certificate

JWT-SVID describes exactly how to encode a SPIFFE ID in an JWT bearer token

SPIFFE Verifiable Identity Document

Certificate of Achievement

Awarded to

for superior achievement and excellence in

this ____ day of ________________

in the year ________________

Signed ________________________

Excellence

SPIFFE
Verifiable Identity Document
(SVID)

Trust Bundle

SPIFFE Verifiable Identity Document

Certificate of Achievement

Awarded to

for superior achievement and excellence in

this ___ day of ___

in the year ___

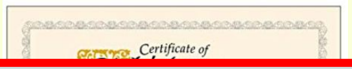
Signed ___

SPIFFE
Verifiable Identity Document
(SVID)

Trust Bundle

spiffe://acme.com/billing/payments

SPIFFE Verifiable Identity Document



⚠ **SVID comes from the SPIFFE implementation, not from the workload itself**

(SVID)

SPIFFE Verifiable Identity Document

Certificate of Achievement

Awarded to

for superior achievement and excellence in

this ___ day of ___

in the year ___

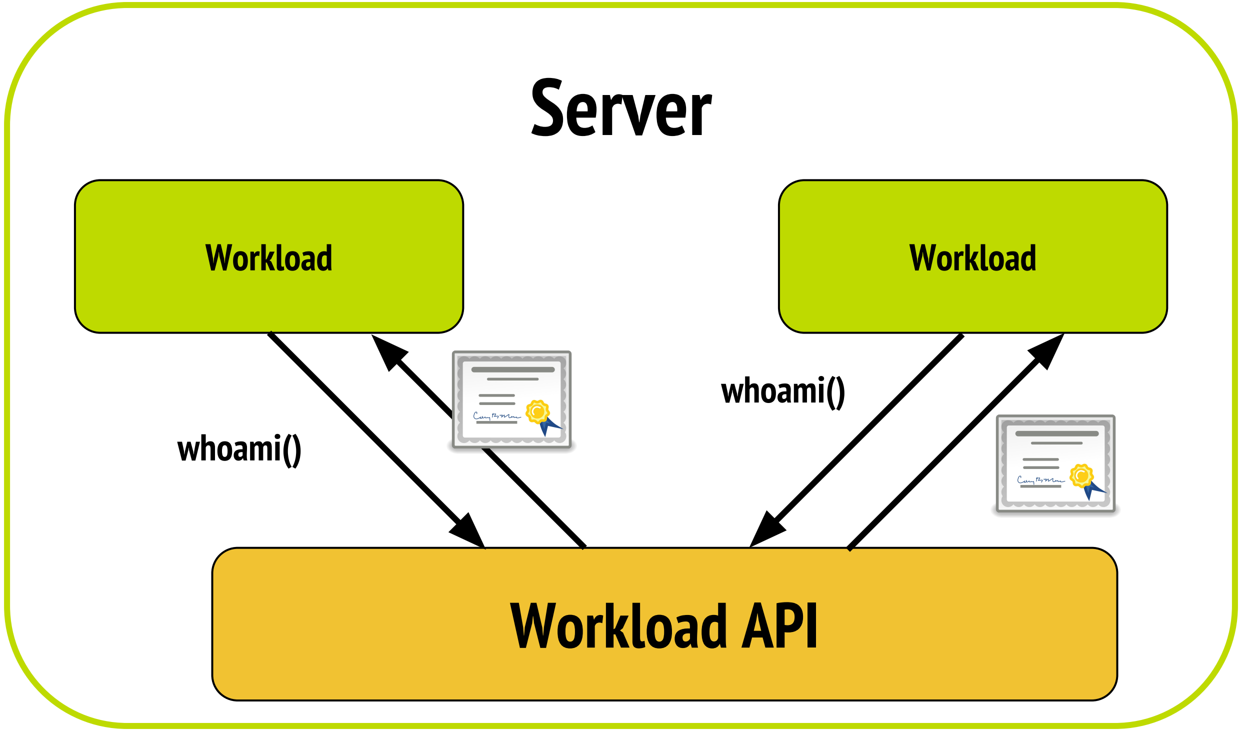
Signed ___

Excellence

SPIFFE
Verifiable Identity Document
(SVID)

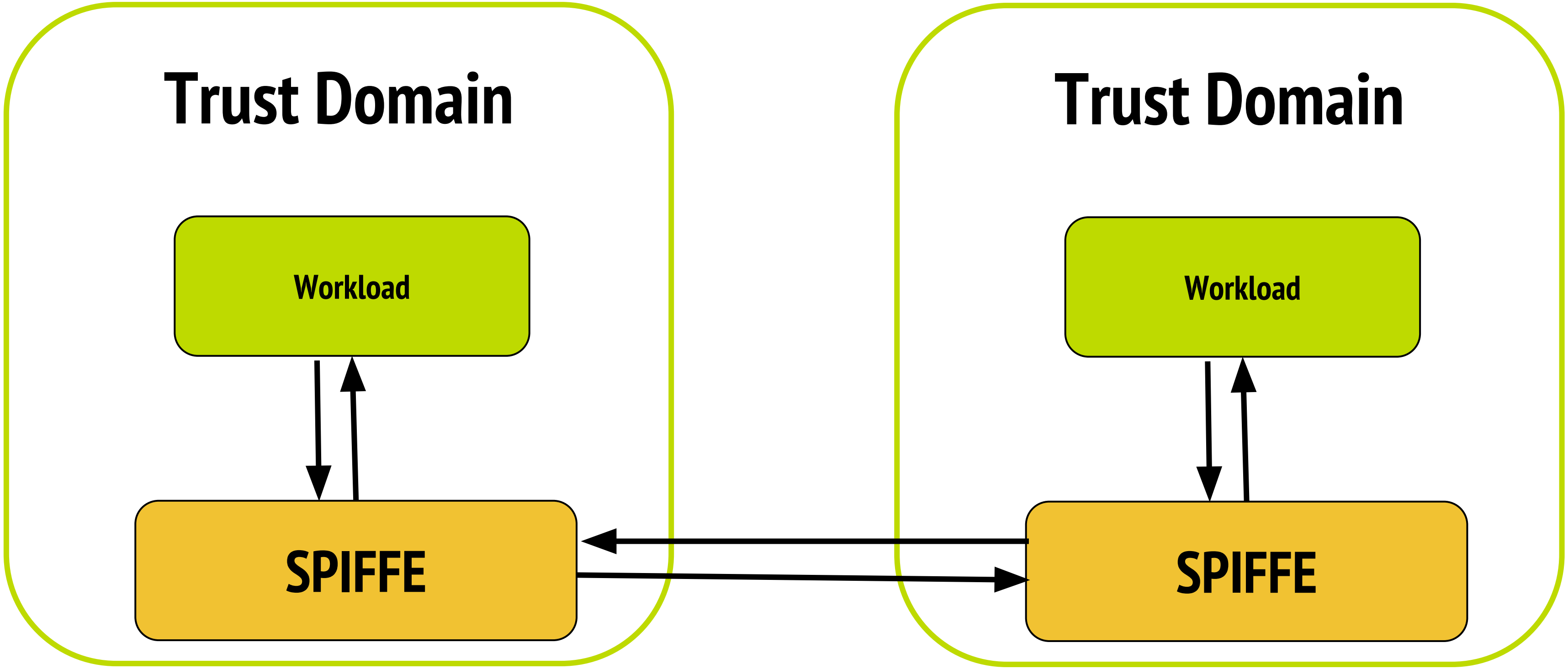
Trust Bundle

SPIFFE Workload API



SPIFFE Federation API

SCYTALE



Today

A short history of SPIFFE

What SPIFFE solves for

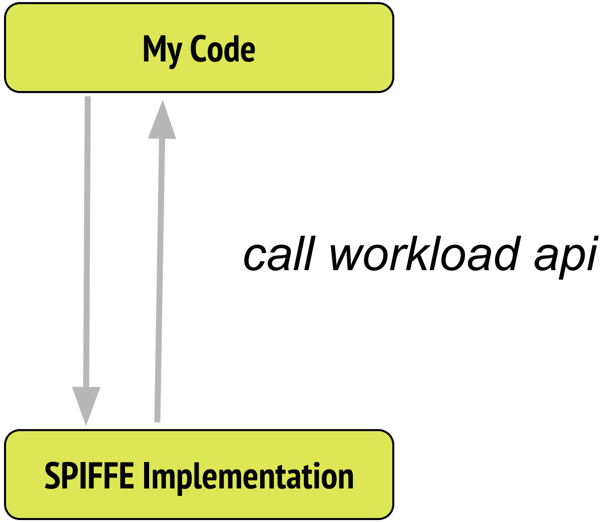
SVIDs, Workload API and Federation

How to use SPIFFE

What's Next?

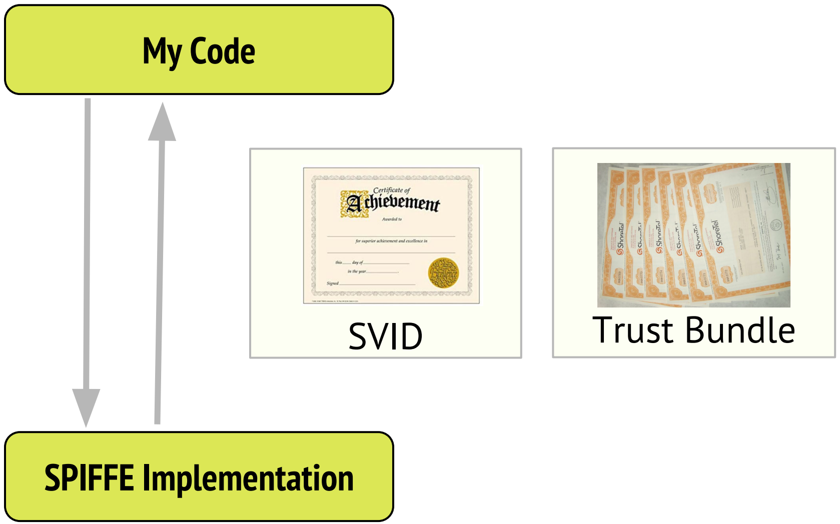
How do I get an SVID?

My Code
Library
Proxy
spiffe-helper
Service Mesh



How do I get an SVID?

- My Code
- Library
- Proxy
- spiffe-helper
- Service Mesh



My Code

SVID

Trust Bundle

SPIFFE Implementation

How do I get an SVID?

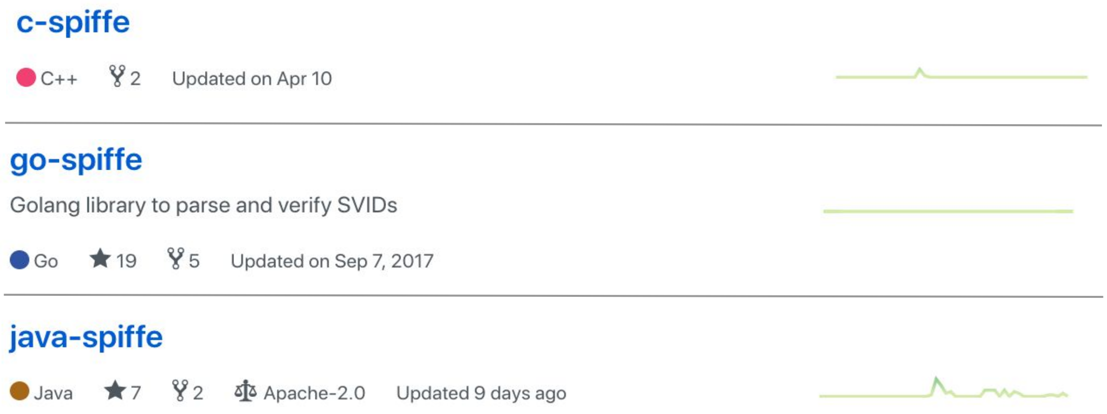
My Code

Library

Proxy

spiffe-helper

Service Mesh



c-spiffe

● C++ ⑂ 2 Updated on Apr 10

go-spiffe

Golang library to parse and verify SVIDs

● Go ★ 19 ⑂ 5 Updated on Sep 7, 2017

java-spiffe

● Java ★ 7 ⑂ 2 ⚖ Apache-2.0 Updated 9 days ago

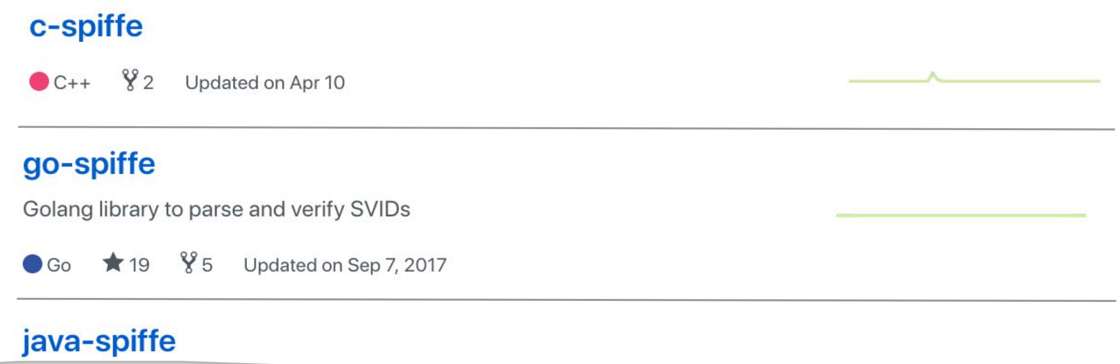
How do I get an SVID?

My Code

Library

Proxy

Service Mesh



c-spiffe

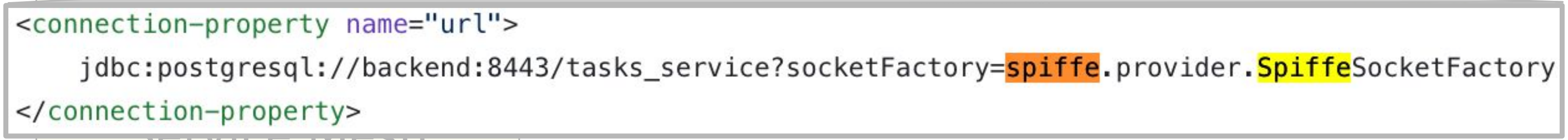
● C++ 2 Updated on Apr 10

go-spiffe

Golang library to parse and verify SVIDs

● Go ★ 19 5 Updated on Sep 7, 2017

java-spiffe

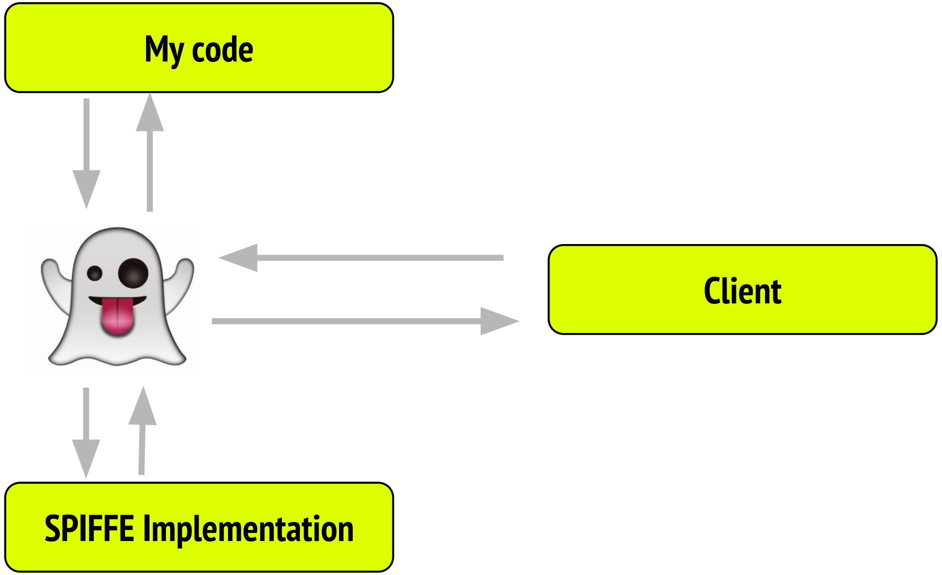


```
<connection-property name="url">
    jdbc:postgresql://backend:8443/tasks_service?socketFactory=spiffe.provider.SpiffeSocketFactory
</connection-property>
```

How do I get an SVID?

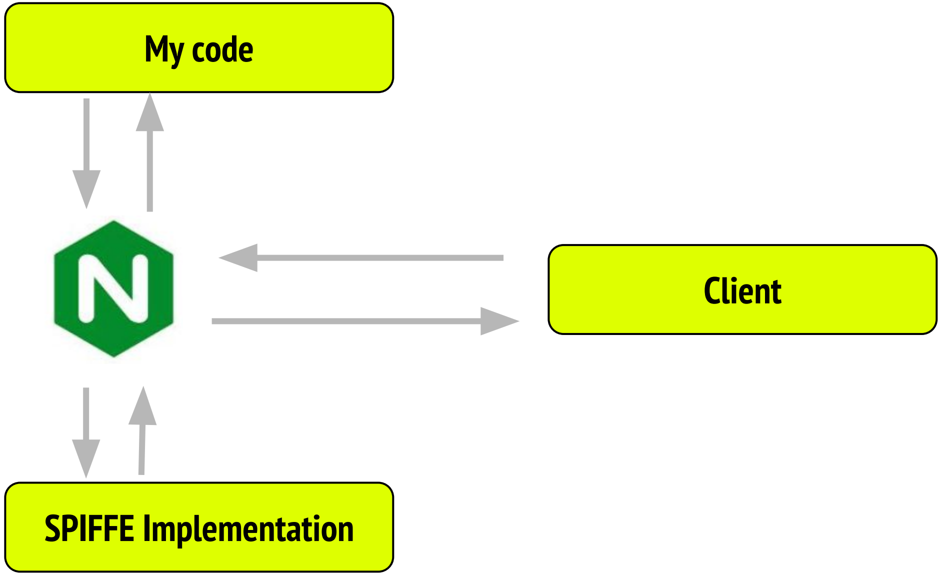
SCYTALE

- My Code
- Library
- **Proxy**
- spiffe-helper
- Service Mesh



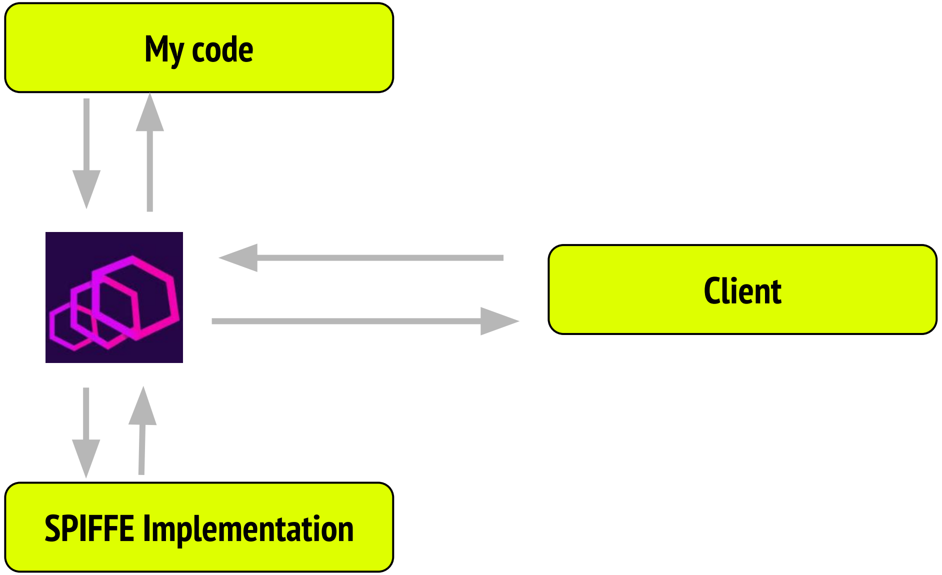
How do I get an SVID?

- My Code
- Library
- Proxy
- spiffe-helper
- Service Mesh



How do I get an SVID?

- My Code
- Library
- Proxy
- spiffe-helper
- Service Mesh



How do I get an SVID?

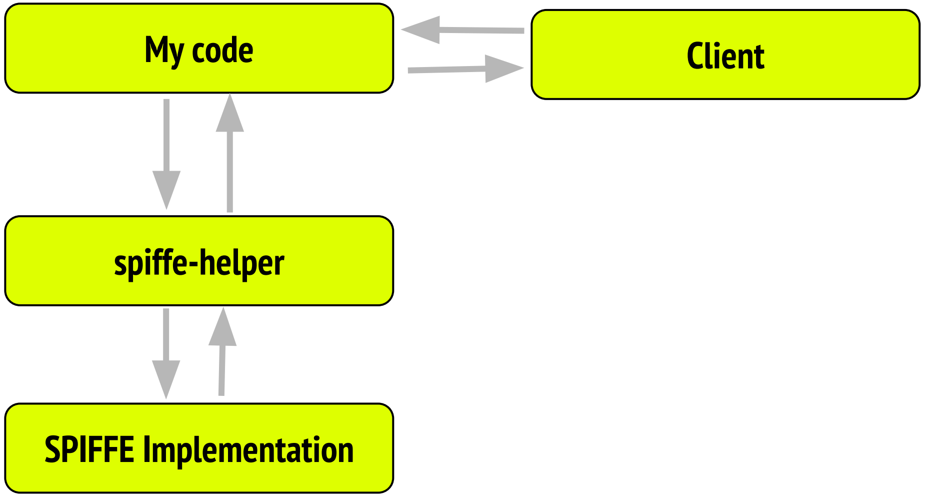
My Code

Library

Proxy

spiffe-helper

Service Mesh



How do I get an SVID?

SCYTALE

My Code

Library

Proxy

spiffe-helper

Service Mesh

Today

A short history of SPIFFE

What SPIFFE solves for

SVIDs, Workload API and Federation

How to use SPIFFE

What's Next?

SCYTALE

Thank you!

Where to find us

slack.spiffe.io

github.com/spiffe

spiffe.io

Today at KubeCon

1.45pm ***Correlating metrics with SPIFFE and SPIRE*** *(Gitlab)*

3.40pm ***SPIFFE and SPIRE Security*** *(Scytale & Heptio)*

Tomorrow at KubeCon

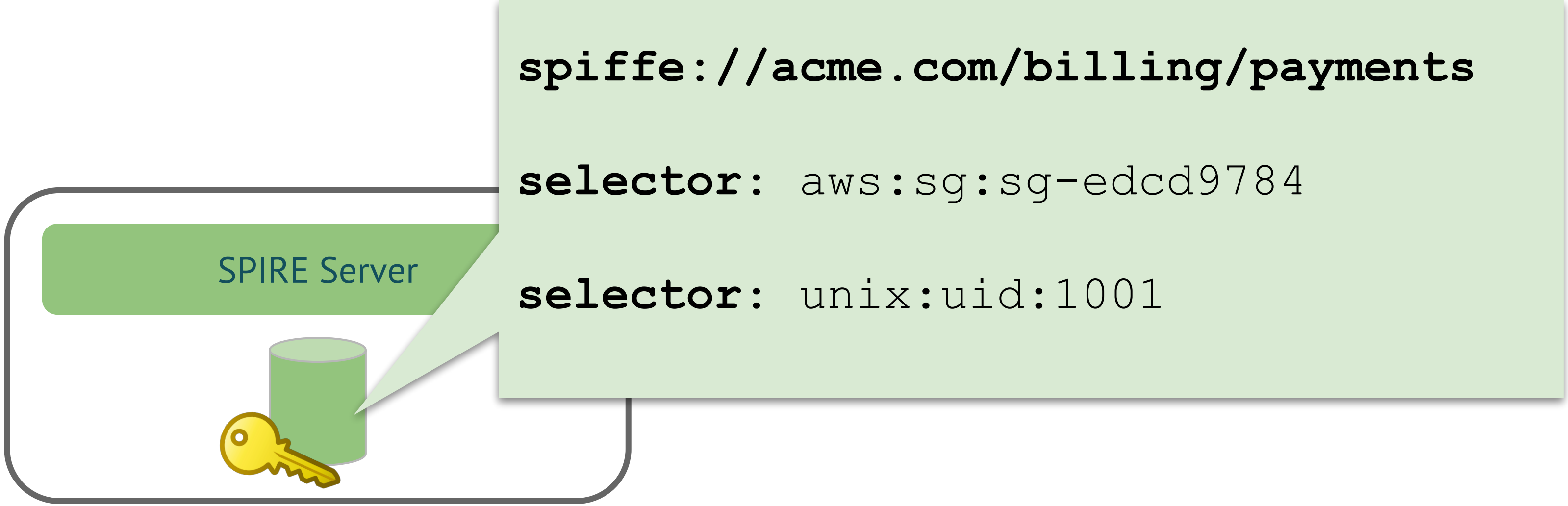
1.45pm ***SPIFFE Deep Dive*** *(Scytale)*

(Lots of details about Federation and JWT)

SCYTALE

Thank you!

A day in the life of an SVID (using SPIRE)

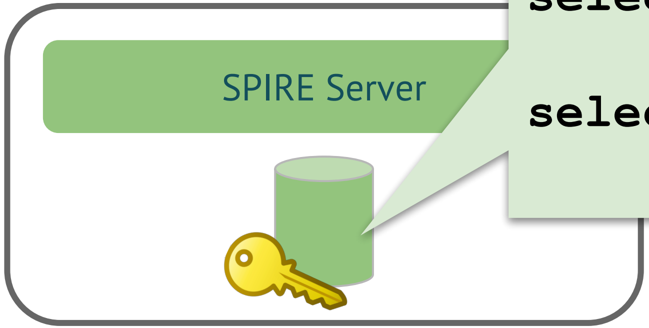


```
spiffe://acme.com/billing/payments

selector: aws:sg:sg-edcd9784

selector: unix:uid:1001
```

A day in the life of an SVID (using SPIRE)

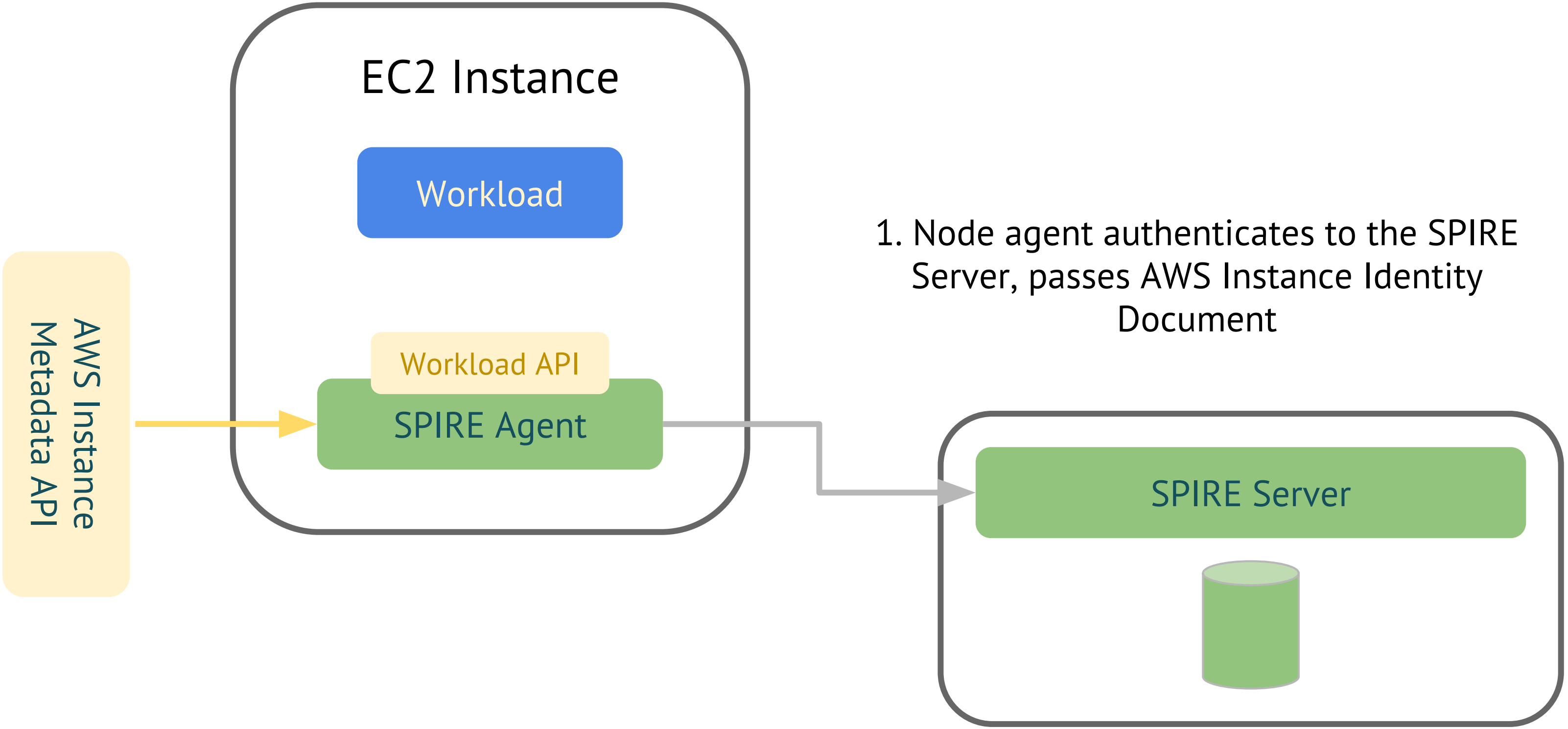


```
spiffe://acme.com/billing/payments

selector: aws:sg:sg-edcd9784

selector: unix:uid:1001
```

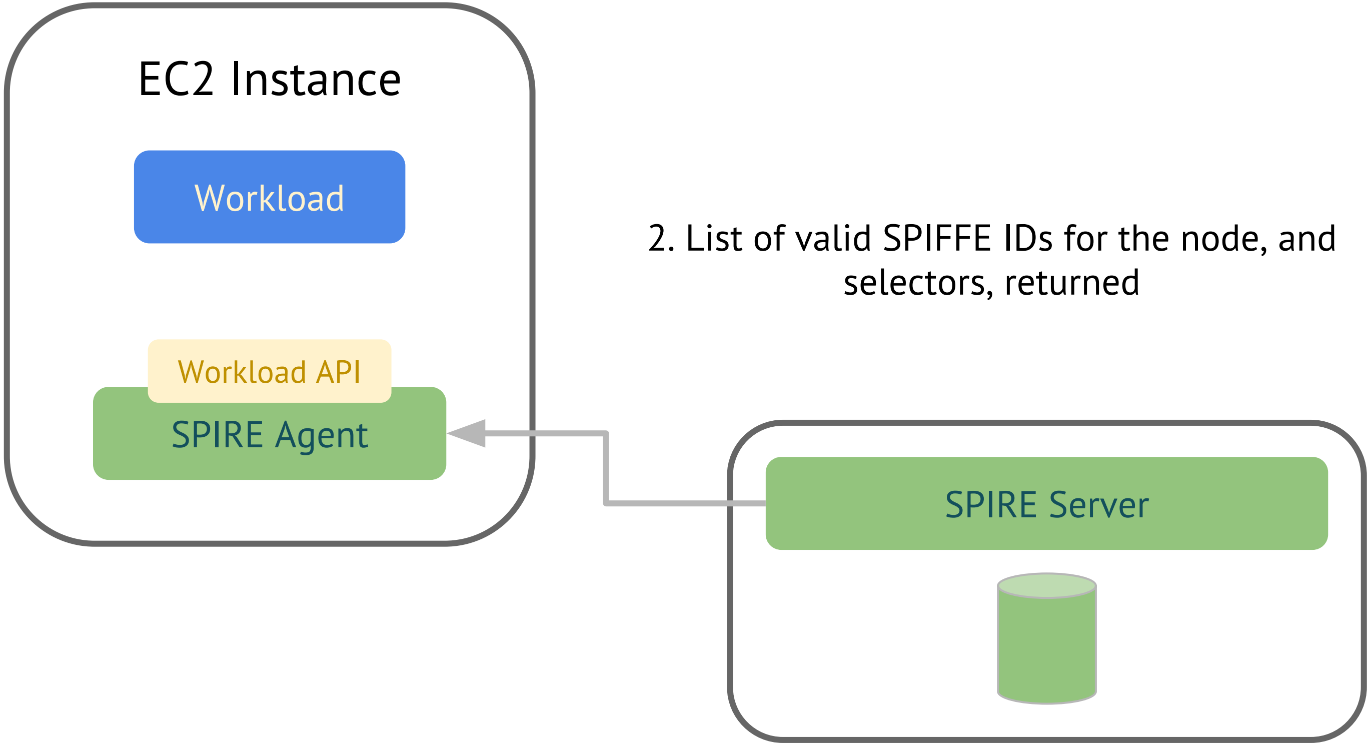
A day in the life of an SVID (using SPIRE)



1. Node agent authenticates to the SPIRE Server, passes AWS Instance Identity Document

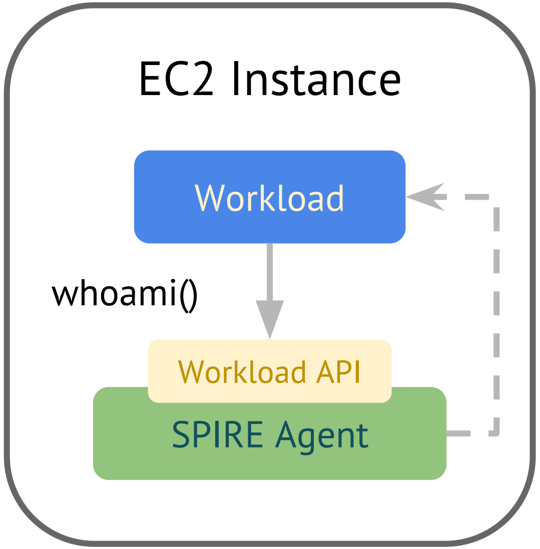
A day in the life of an SVID (using SPIRE)

SCYTALE



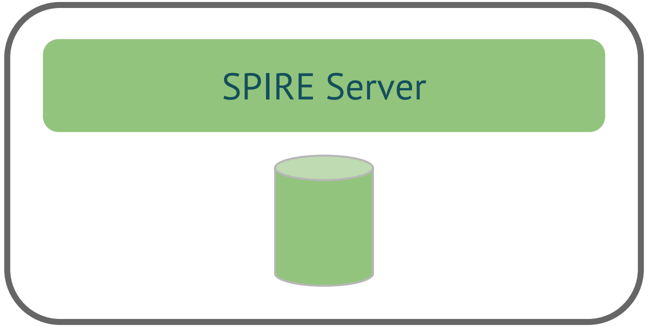
2. List of valid SPIFFE IDs for the node, and selectors, returned

A day in the life of an SVID (using SPIRE)



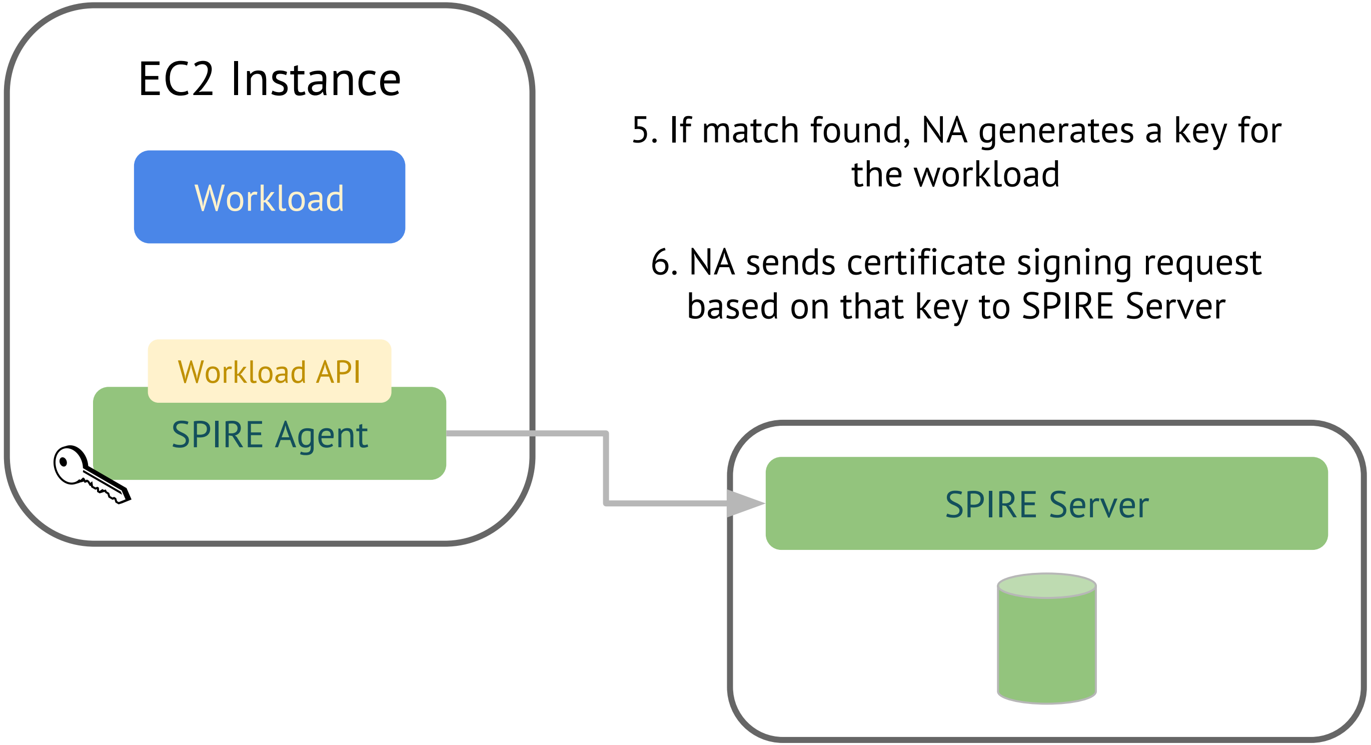
3. Workload requests identity

4. Node agent performs an out-of-band check of the workload process metadata, compares to known selectors



A day in the life of an SVID (using SPIRE)

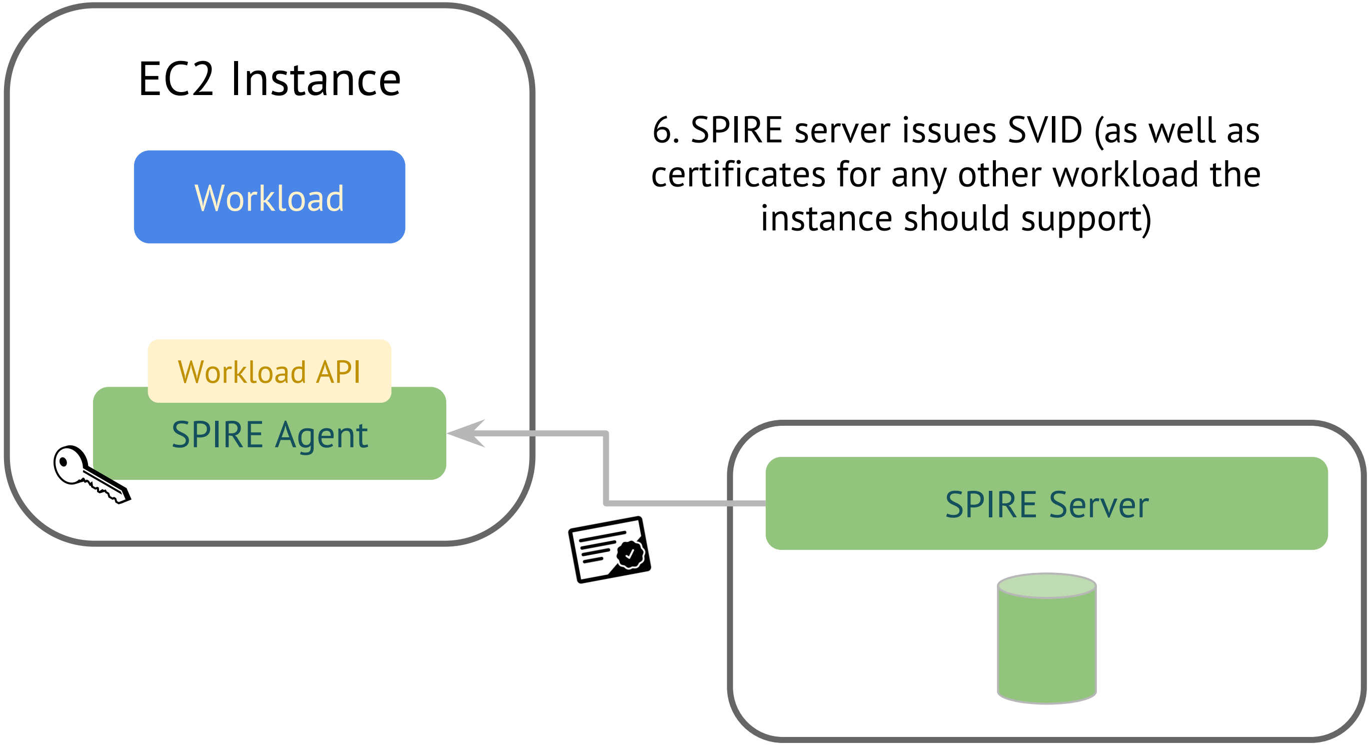
SCYTALE



5. If match found, NA generates a key for the workload

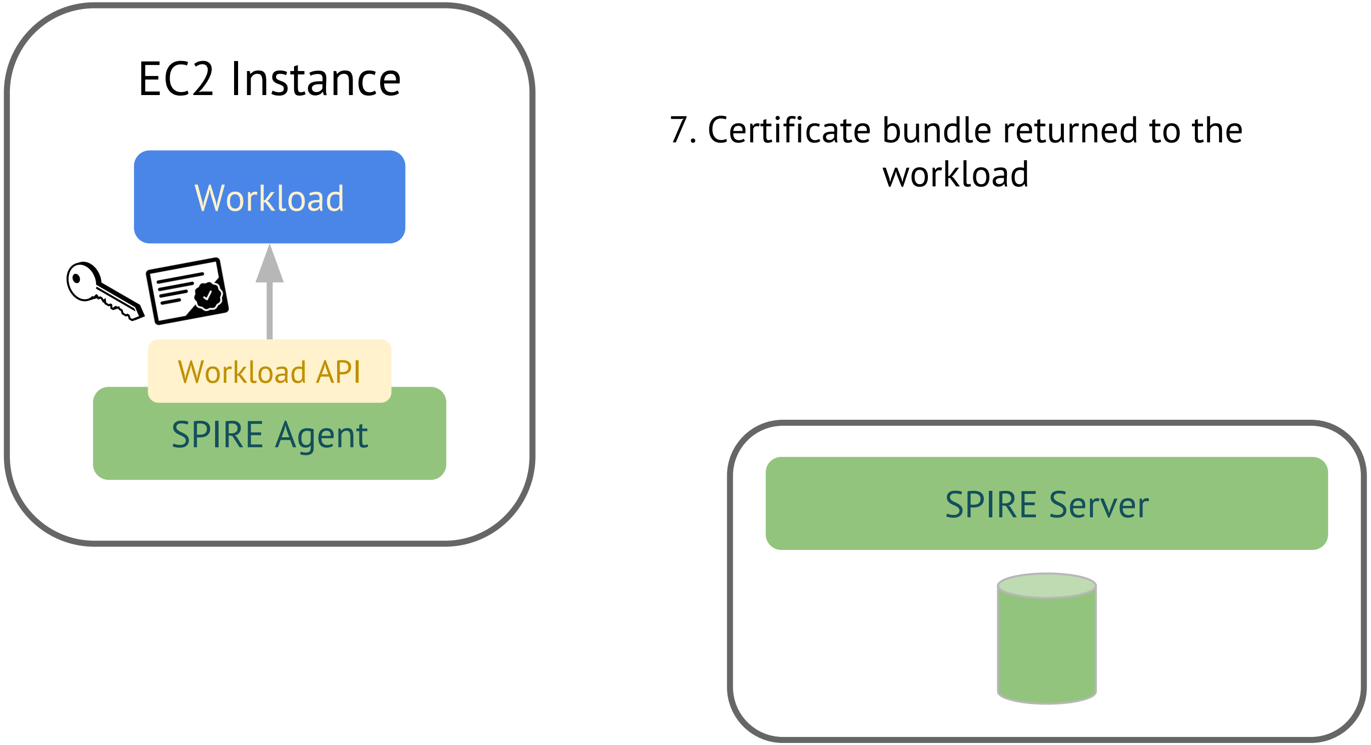
6. NA sends certificate signing request based on that key to SPIRE Server

A day in the life of an SVID (using SPIRE)



6. SPIRE server issues SVID (as well as certificates for any other workload the instance should support)

A day in the life of an SVID (using SPIRE)



7. Certificate bundle returned to the workload