



KubeCon



CloudNativeCon

Europe 2020

Save Your Services From Sneaky Snoops With SPIFFE

Virtual

Daniel Feldman
SPIFFE & SPIRE Projects

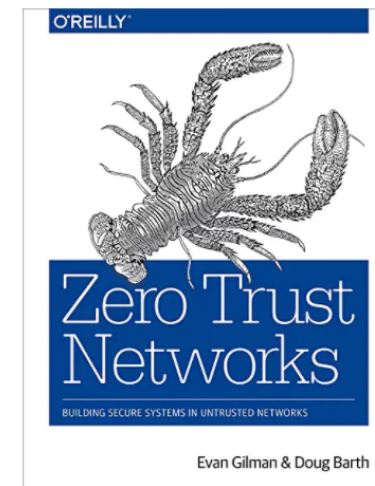
About Me



Daniel Feldman

Cloud security engineering
Veritas -> Scytale -> HPE

And a huge team with security experience from a variety of companies!





KubeCon



CloudNativeCon

Europe 2020

Virtual

Why Service Identity

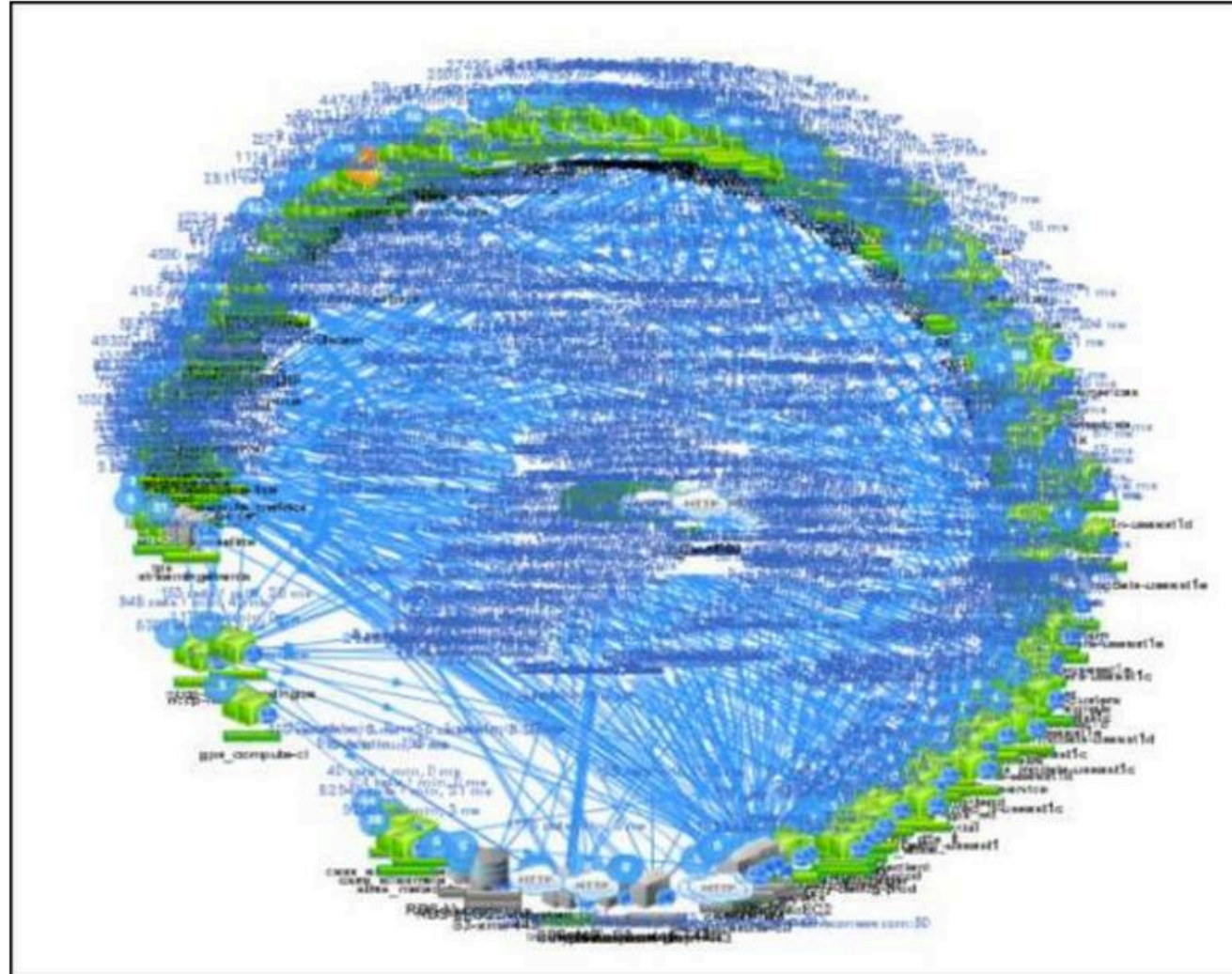
Service Identity Approaches

SPIFFE (the standard)

SPIRE (the implementation)

Next Steps

Why Service Identity



Why Service Identity



ENCRYPTION



INTEGRITY



AUTHENTICATION



AUTHORIZATION

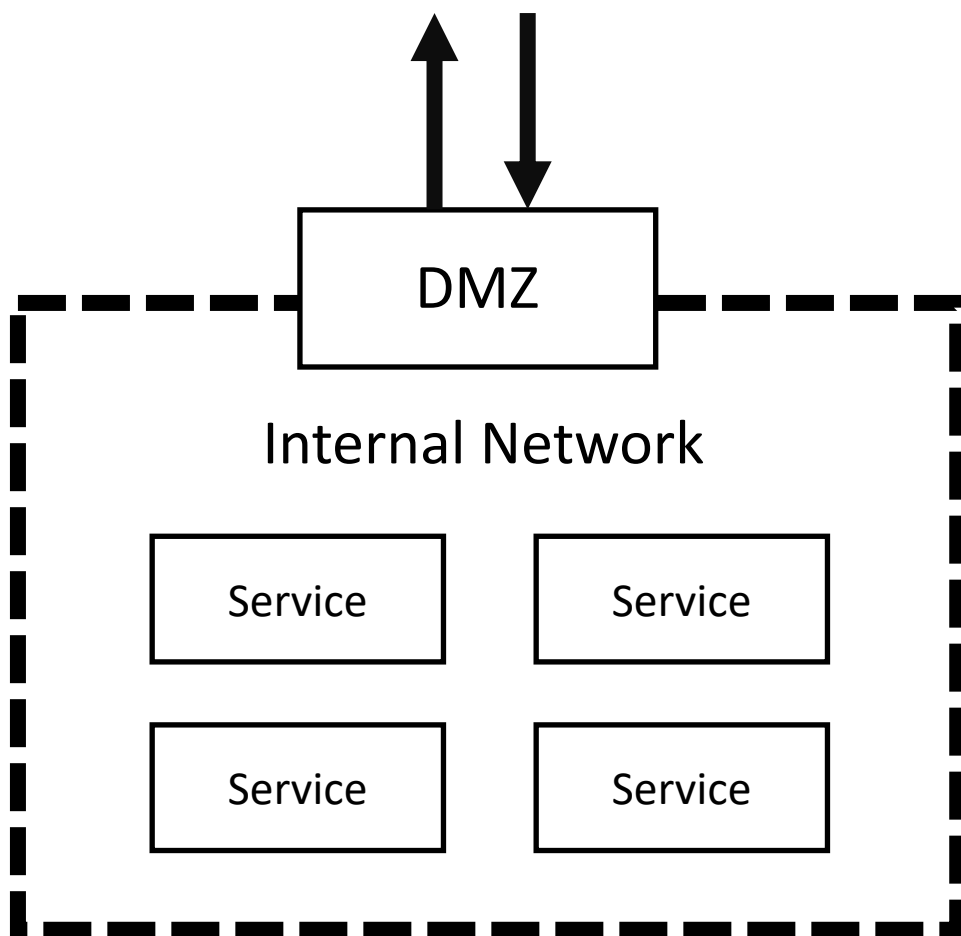
All security rests on a foundation of **identity**

For humans, identity is (mostly) straightforward

For services...

Service identity approaches

Can we just use... **perimeter security**?



- In the perimeter security model, **everything “inside” is trusted** and everything “outside” is **untrusted**

Why Service Identity



KubeCon

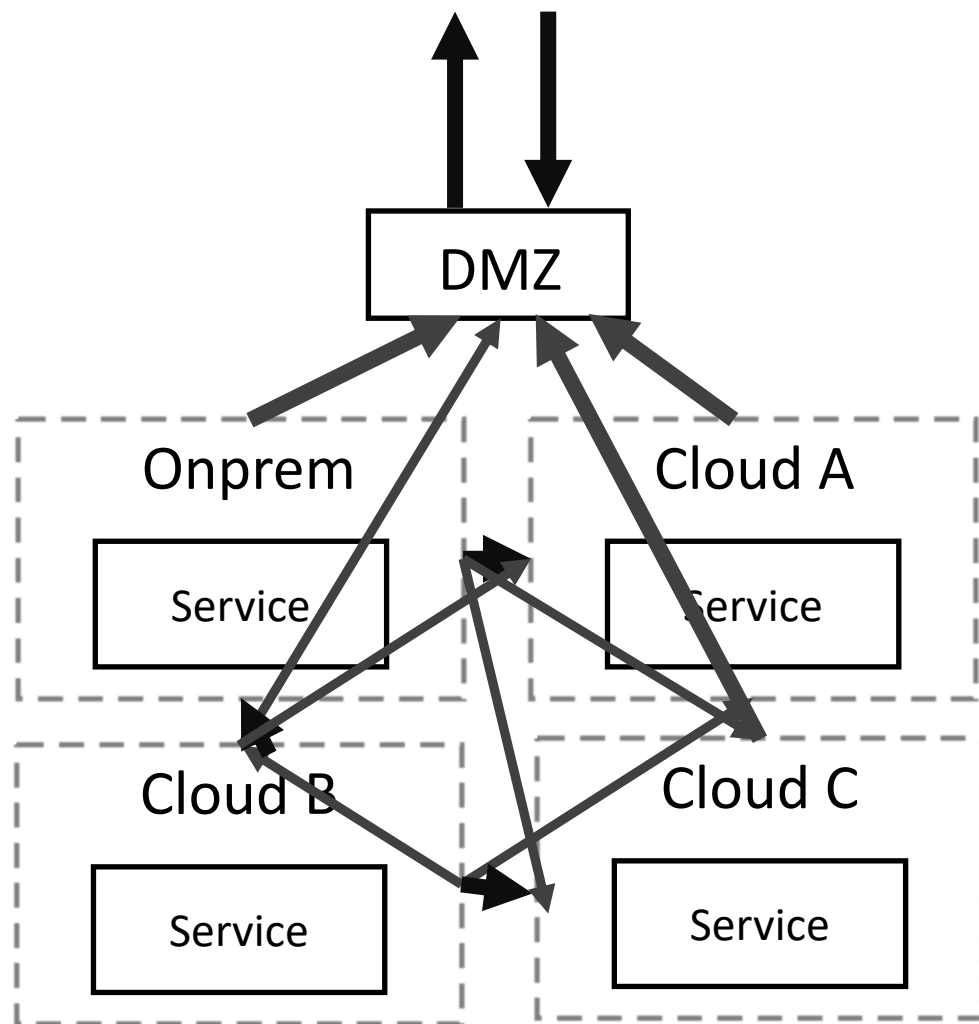


CloudNativeCon

Europe 2020

Virtual

Can we just use... **perimeter security**?



- In the perimeter security model, everything “inside” is trusted and everything “outside” is untrusted
- As you add multiple datacenters, clouds and regions this becomes **increasingly complex**

Why Service Identity



KubeCon

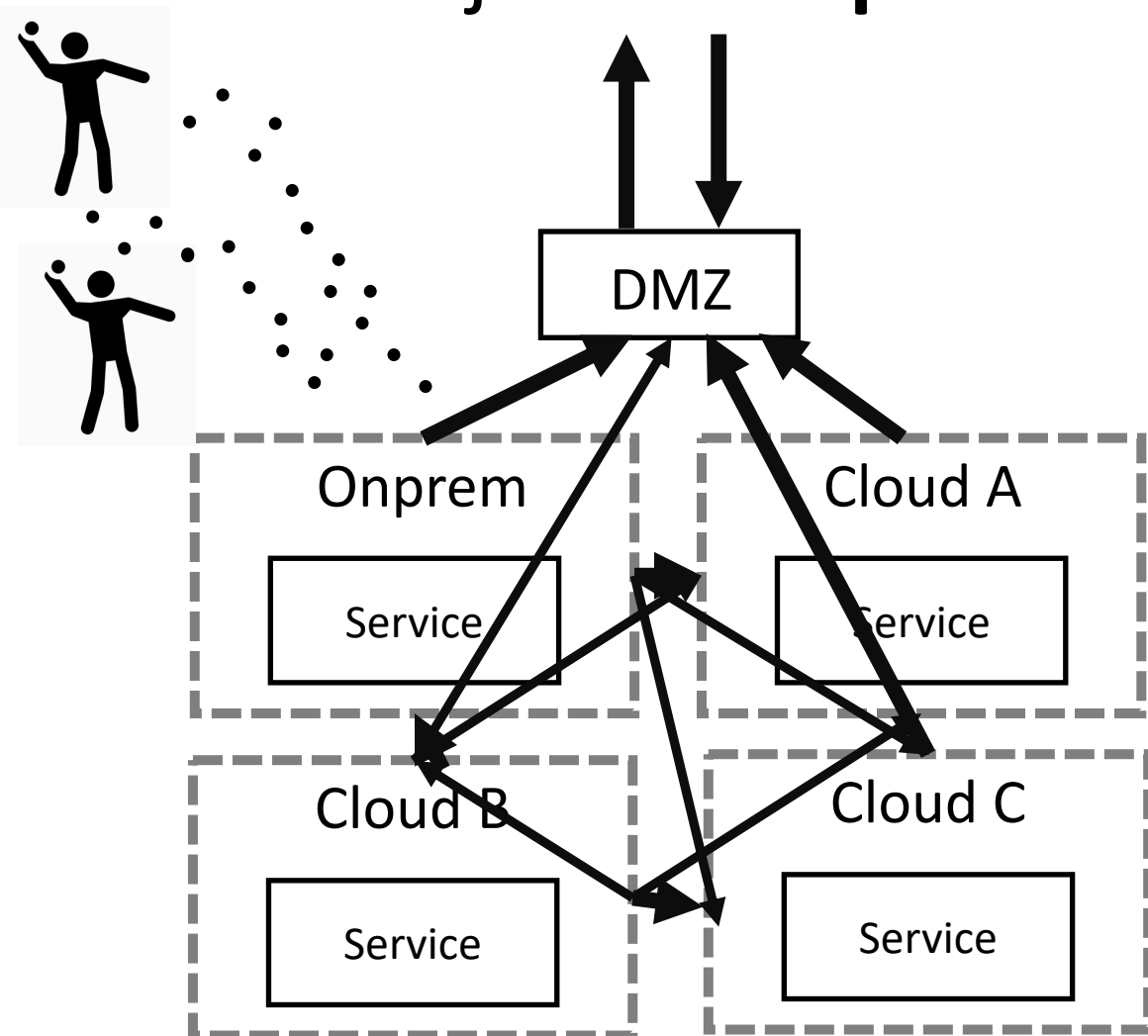


CloudNativeCon

Europe 2020

Virtual

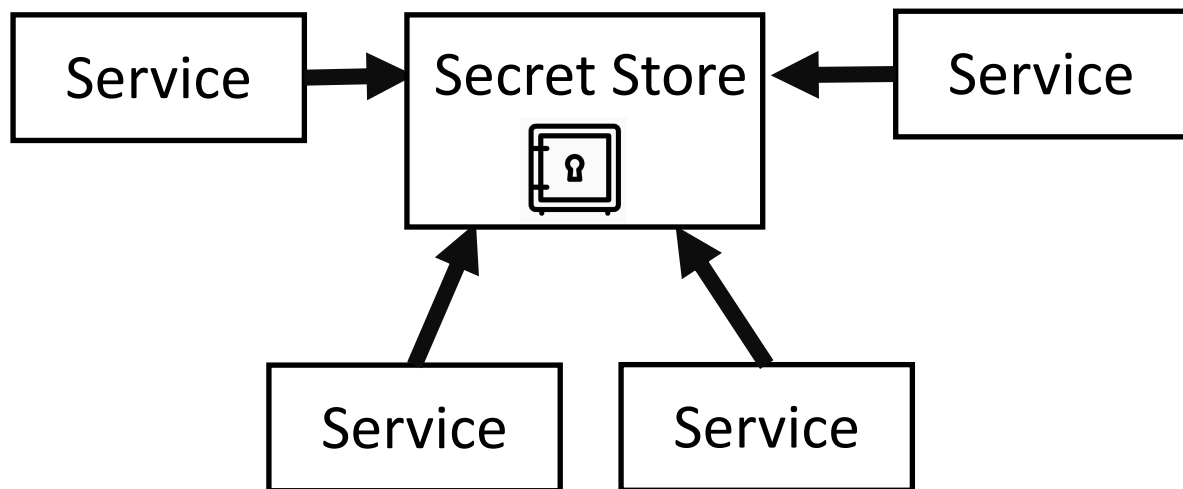
Can we just use... **perimeter security**?



- In the perimeter security model, everything “inside” is trusted and everything “outside” is untrusted
- As you add multiple datacenters, clouds and regions this becomes increasingly complex
- CI/CD makes it almost impossible

Why Service Identity

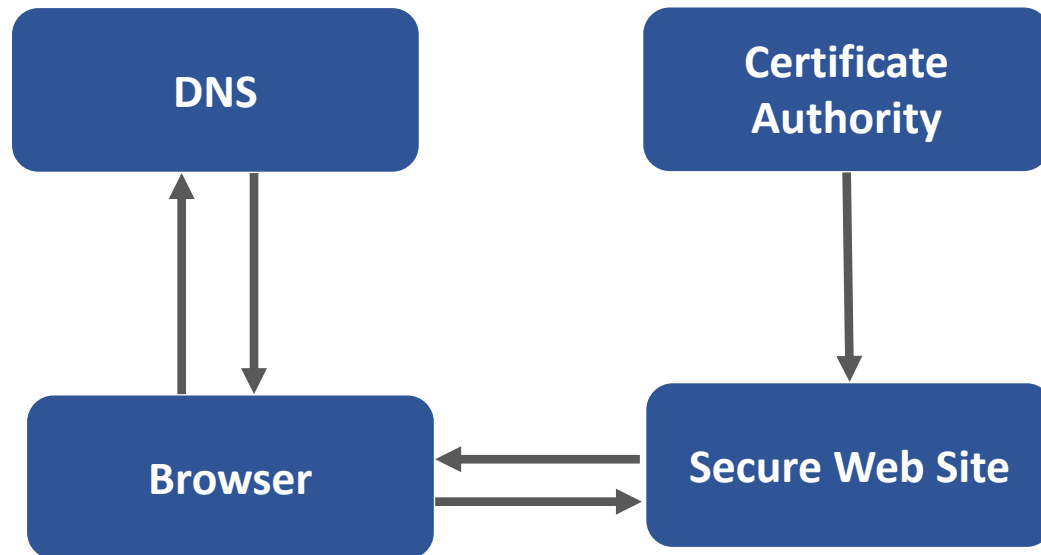
Can we just use... **shared secrets**?



- In the **shared secrets** model, every service has credentials/certificates used to access other services
 - (Hopefully) stored in a secret store
- Maintaining secrets at scale is hard work
- How do you initially authenticate to the secret store?

Why Service Identity

Can we just use... **web PKI**?



- Web Public key infrastructure (PKI) lets you access web sites securely
- But services aren't web sites:
 - Services don't all have hostnames
- Also, no simple way to check the client's identity



We need a way to **securely distribute identities to services** without relying on manual effort

Secure Production Identify Framework for Everyone



- SPIFFE is a **platform-agnostic standard** for implementing service identity
- Inspired by Google, Netflix, and Facebook
- It gives your service a “passport” for communicating with other services
- It is partially implemented by several service meshes, and fully implemented in SPIRE

SPIFFE (the standard)



KubeCon



CloudNativeCon

Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
`spiffe://trustdomain/service`

SPIFFE (the standard)



KubeCon



CloudNativeCon

Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
spiffe://trustdomain/service

SVIDs

Cryptographically verifiable
documents asserting a SPIFFE ID

SPIFFE (the standard)



KubeCon



CloudNativeCon

Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
spiffe://trustdomain/service

SVIDs

Cryptographically verifiable
documents asserting a SPIFFE ID

Trust Bundles

Set of certificates used to
verify SVIDs

SPIFFE (the standard)



KubeCon



CloudNativeCon

Europe 2020

Virtual

SPIFFE IDs

Standard format for a service ID
spiffe://trustdomain/service

SVIDs

Cryptographically verifiable
documents asserting a SPIFFE ID

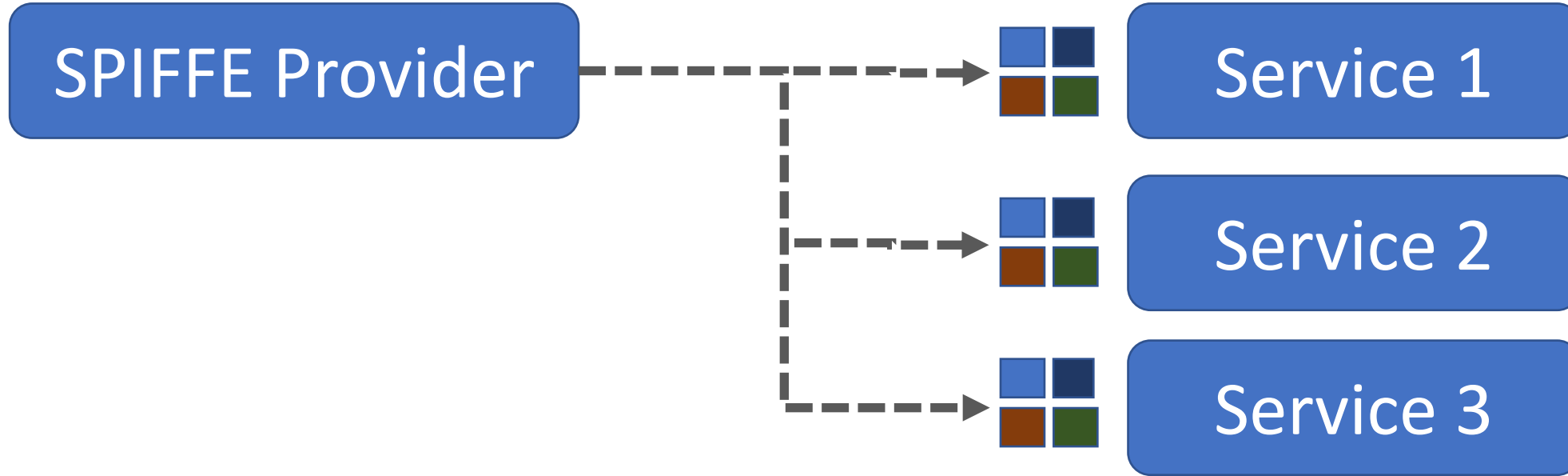
Trust Bundles

Set of certificates used to
verify SVIDs

Workload API

Local gRPC API for workloads to
obtain SPIFFE IDs, SVIDs, and
Trust Bundles

SPIFFE (the standard)

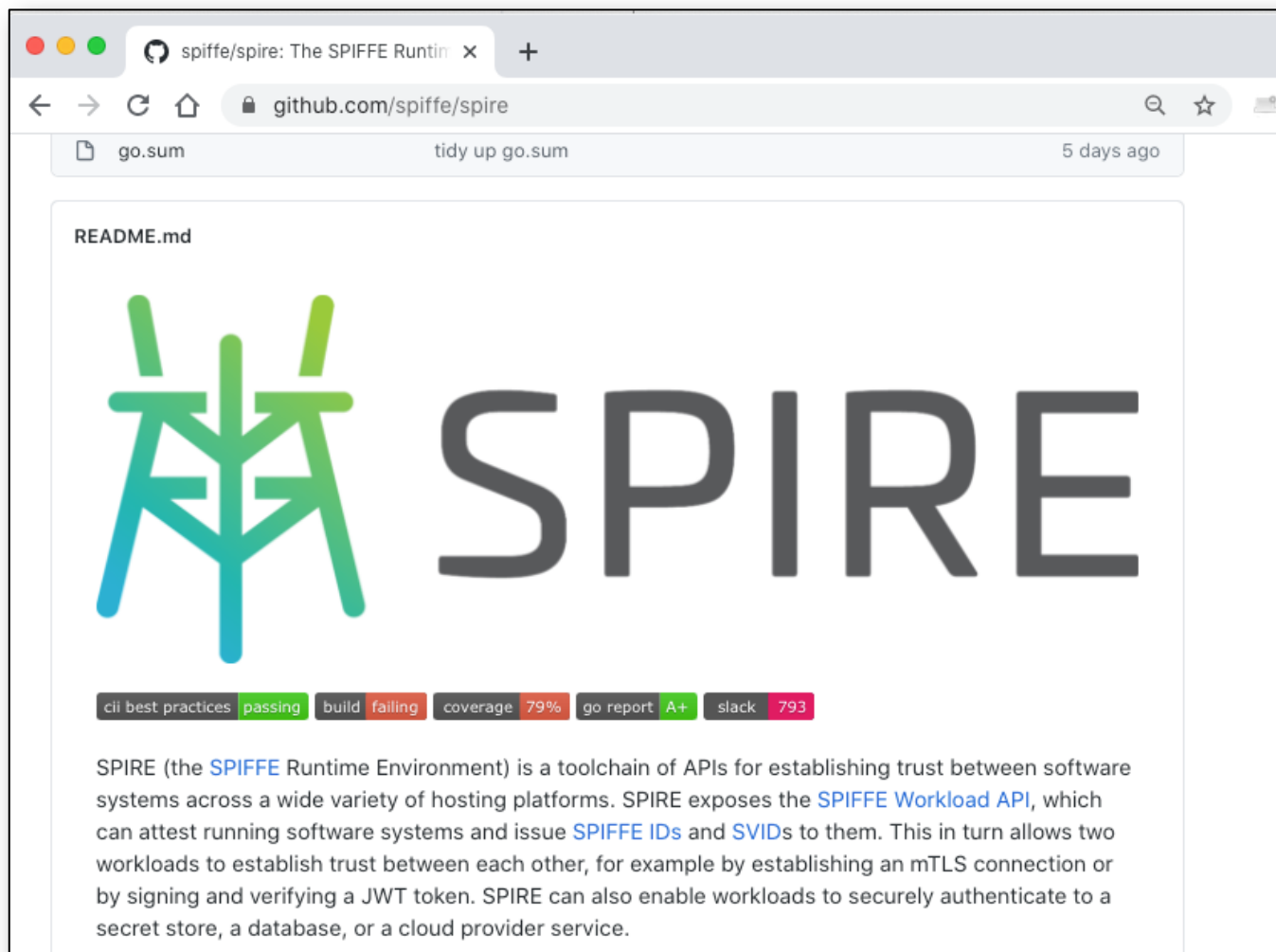


Network Service Mesh



SPIRE

SPIRE (our implementation)



The screenshot shows a web browser window displaying the GitHub repository page for SPIRE. The browser's address bar shows the URL `github.com/spiffe/spire`. The page title is "spiffe/spire: The SPIFFE Runtime Environment". The main content area features the SPIRE logo, which consists of a stylized tree-like structure in shades of green and blue, followed by the word "SPIRE" in large, bold, grey capital letters. Below the logo, there is a row of status indicators: "cii best practices" (passing), "build" (failing), "coverage" (79%), "go report" (A+), and "slack" (793). The README text describes SPIRE as a toolchain of APIs for establishing trust between software systems across various hosting platforms. It mentions the SPIFFE Workload API, SPIFFE IDs, and SVIDs, and notes that SPIRE can enable workloads to securely authenticate to a secret store, a database, or a cloud provider service.

SPIRE (our implementation)

SPIRE Server



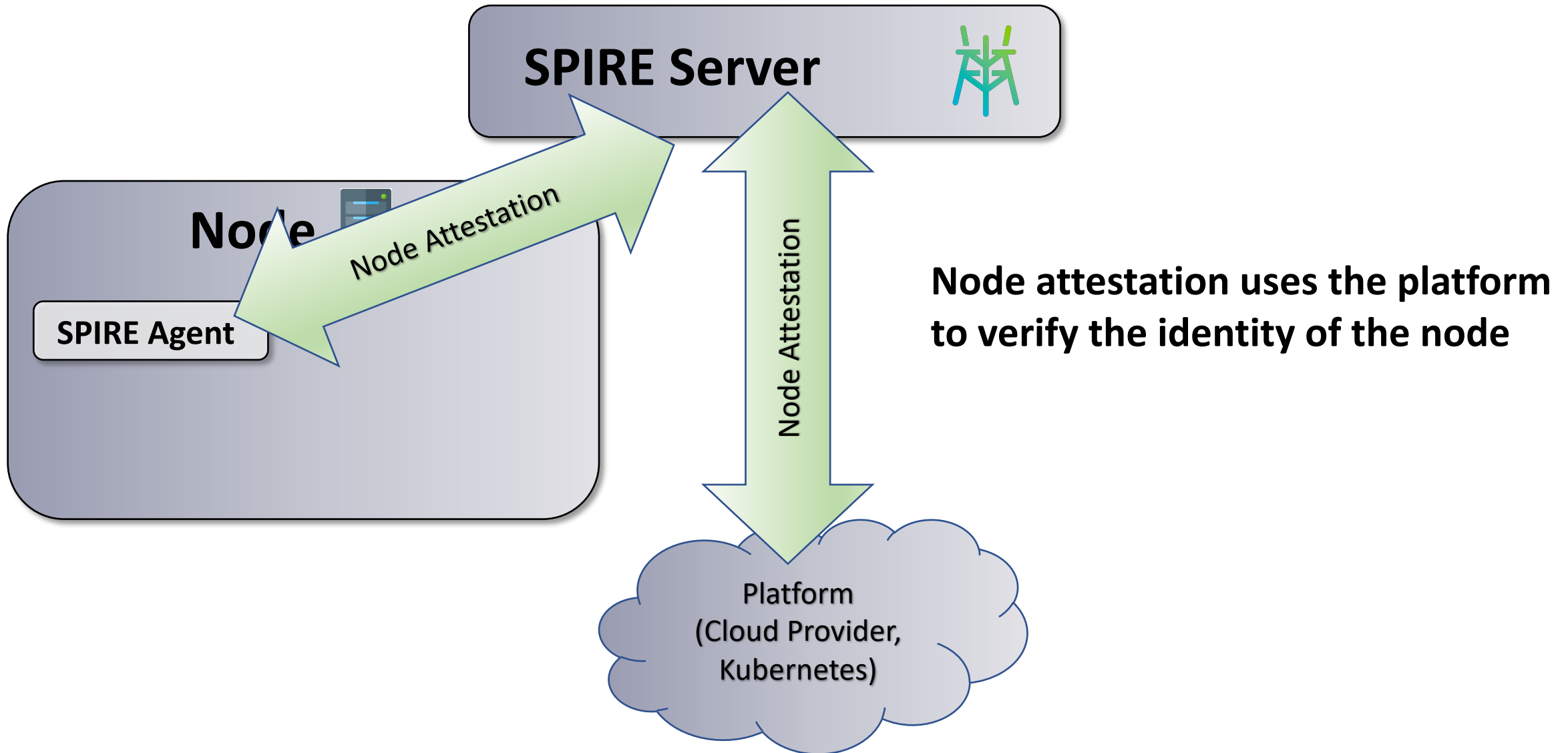
Node



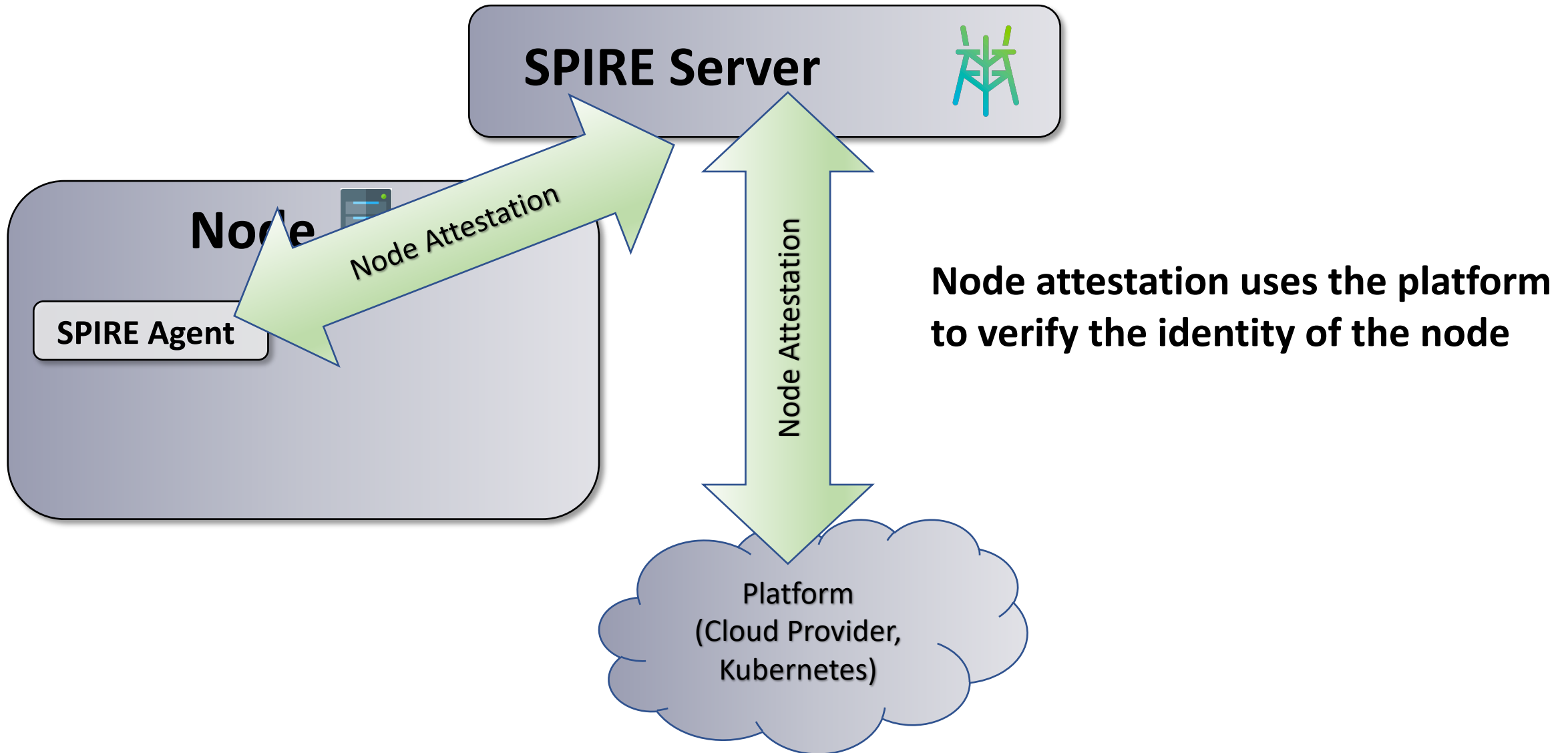
SPIRE Agent

Platform
(Cloud Provider,
Docker, or
Kubernetes)

SPIRE (our implementation)



SPIRE (our implementation)

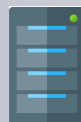


SPIRE (our implementation)

SPIRE Server



Node



SPIRE Agent

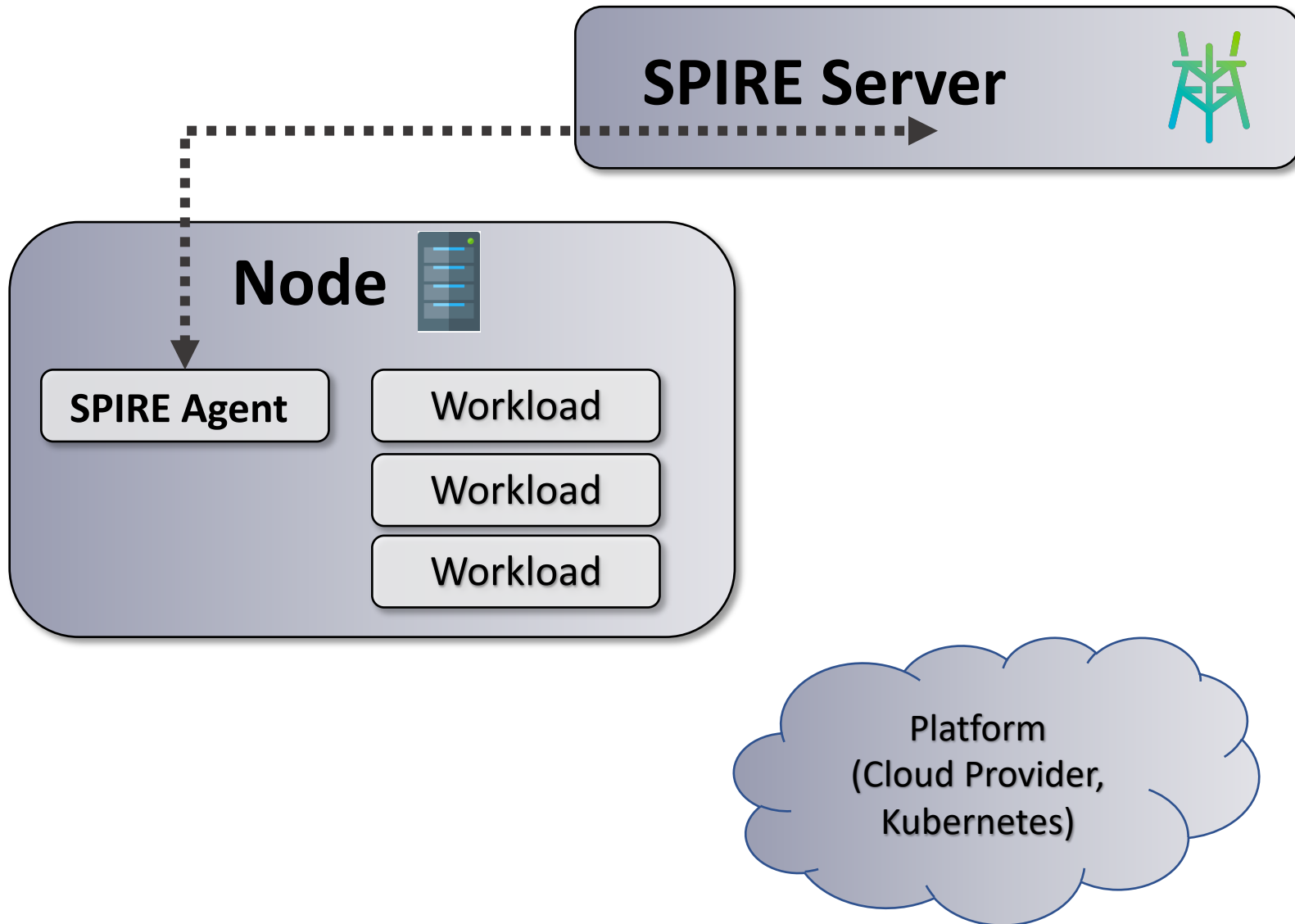
Workload

Workload

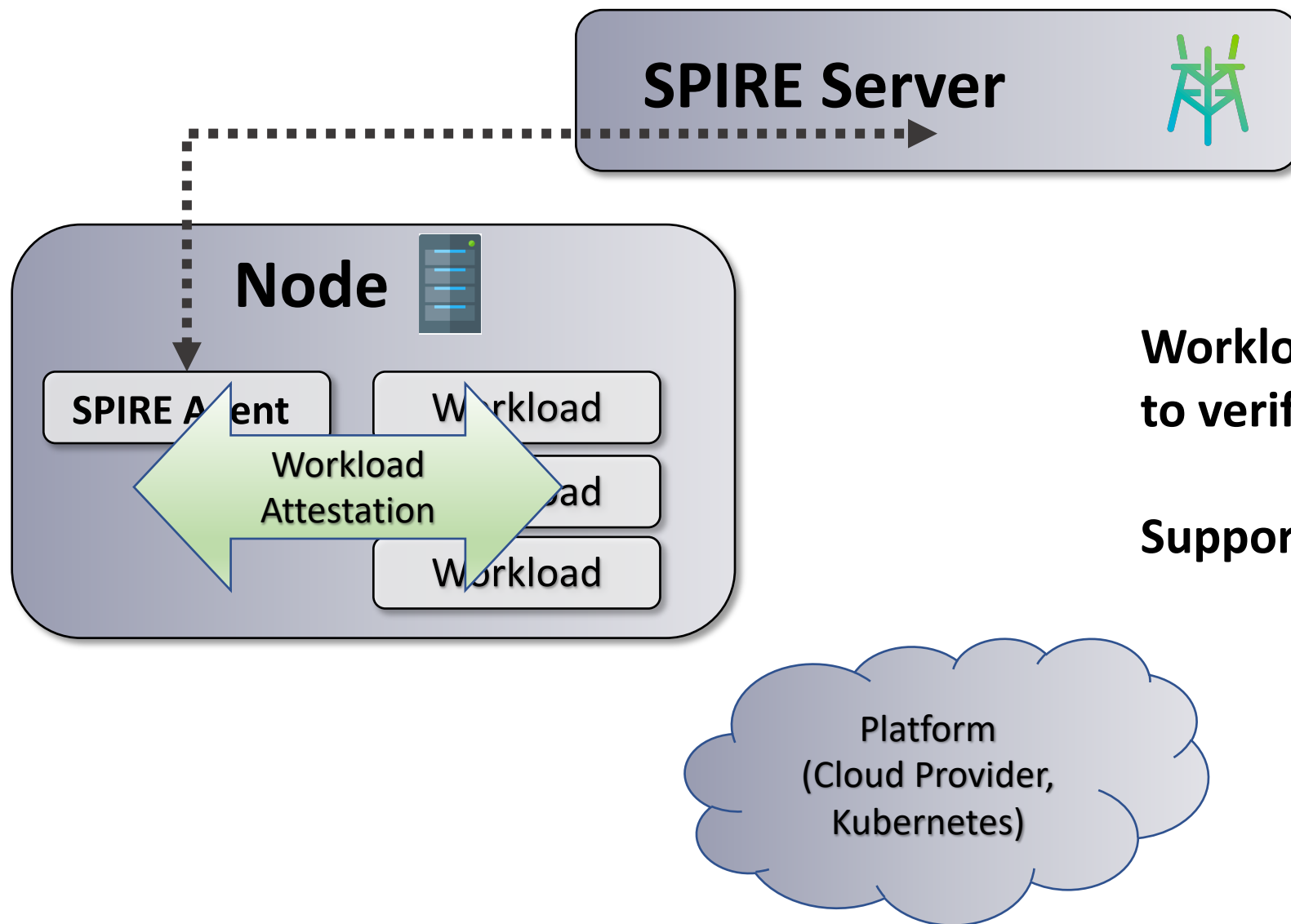
Workload

Platform
(Cloud Provider,
Kubernetes)

SPIRE (our implementation)



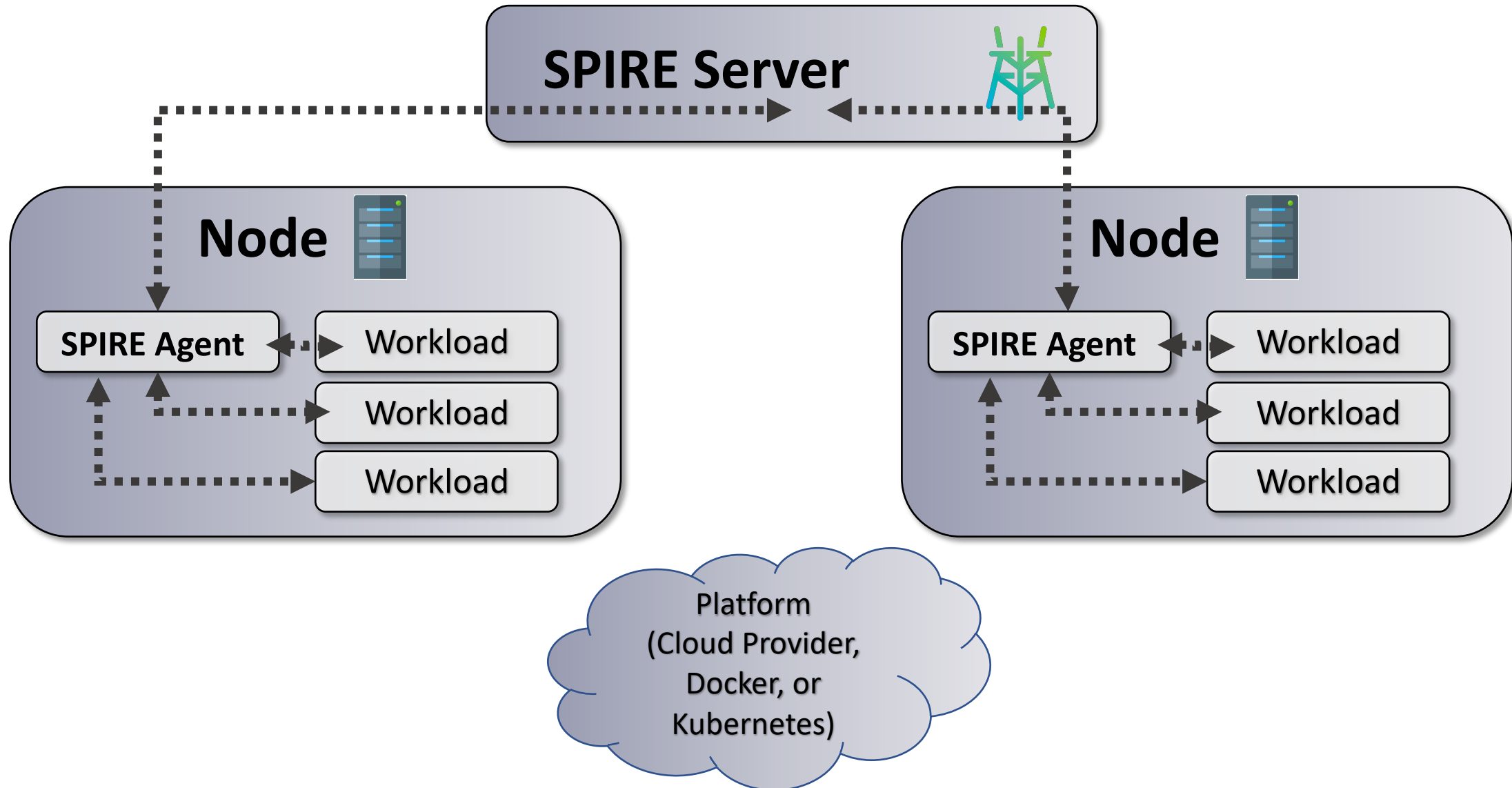
SPIRE (our implementation)



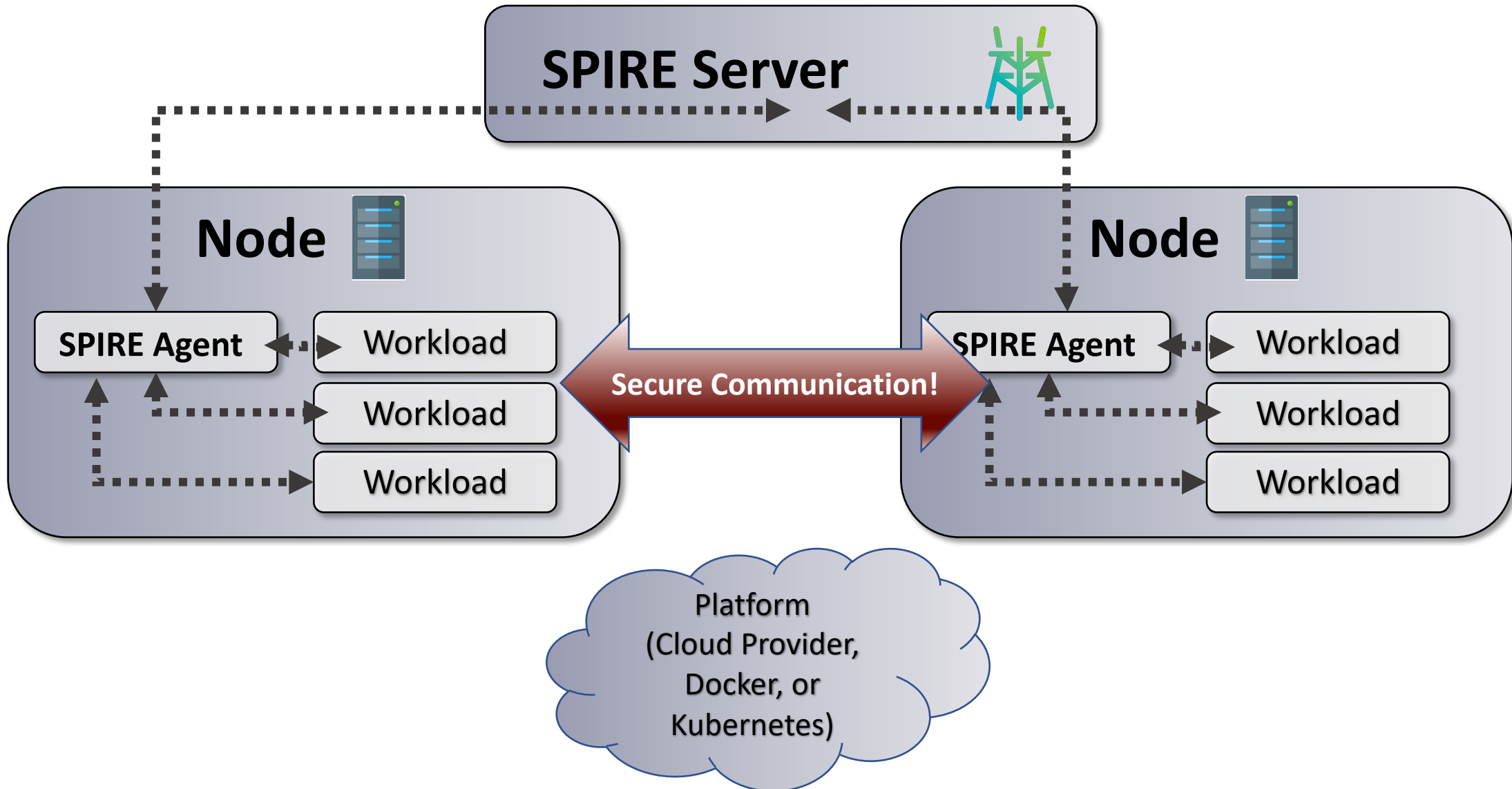
Workload attestation uses the kernel to verify the identity of the process

Supports Linux, BSD, Kubelet

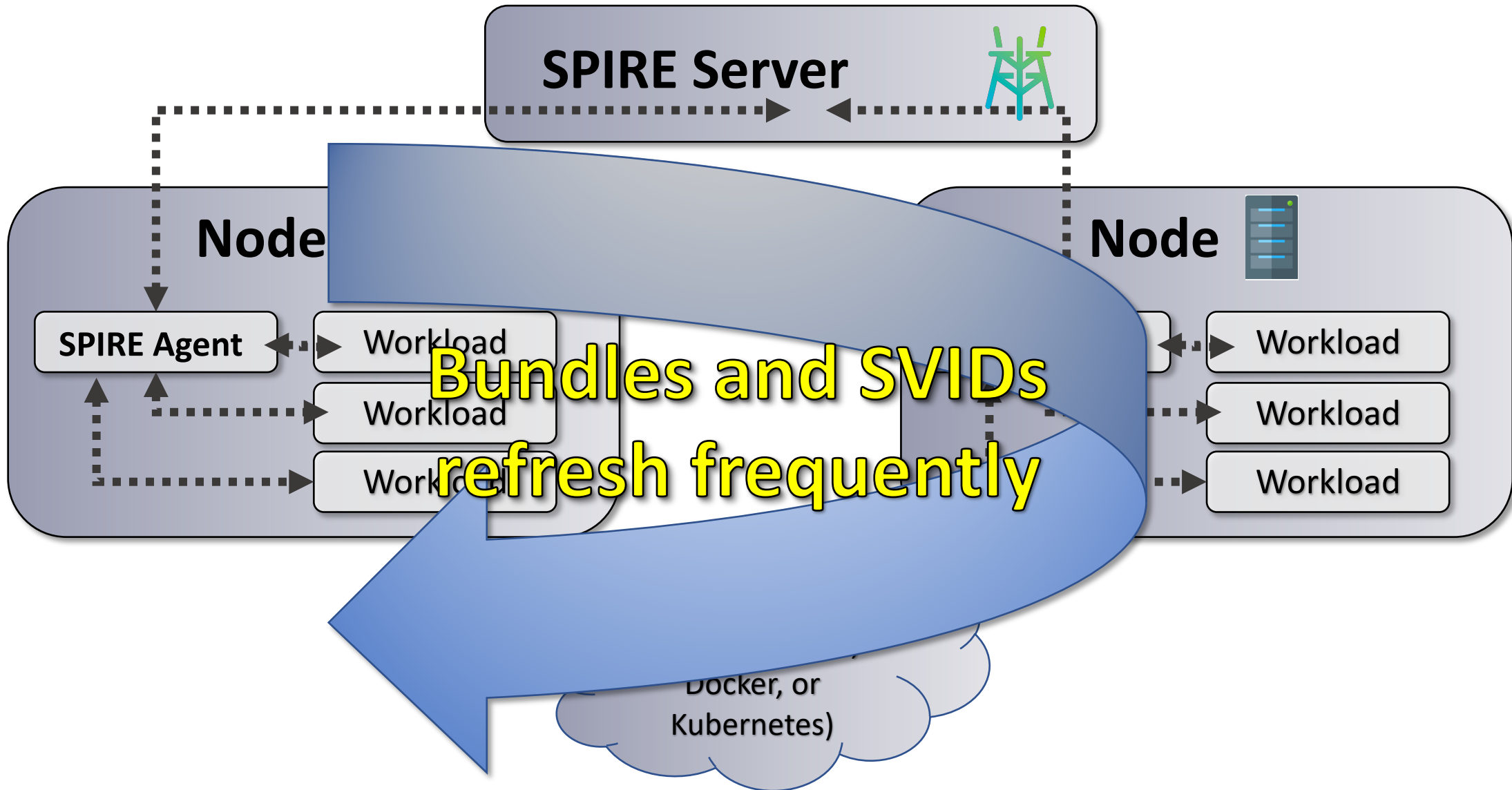
SPIRE (our implementation)



SPIRE (our implementation)



SPIRE (our implementation)



SPIRE (our implementation)



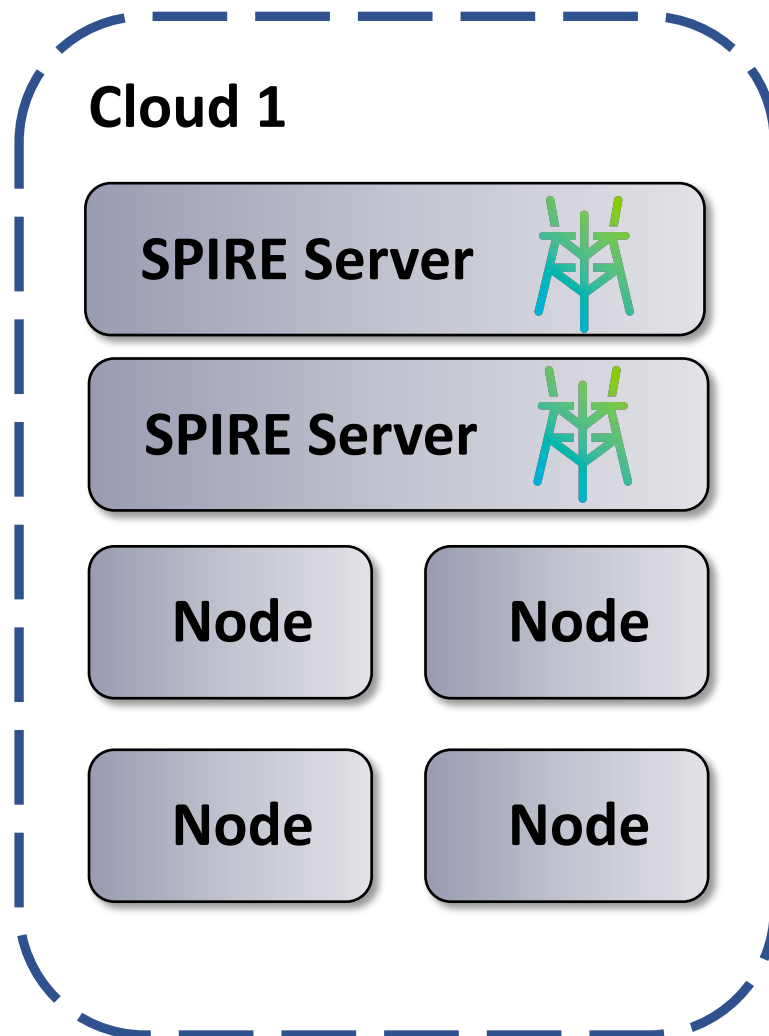
KubeCon



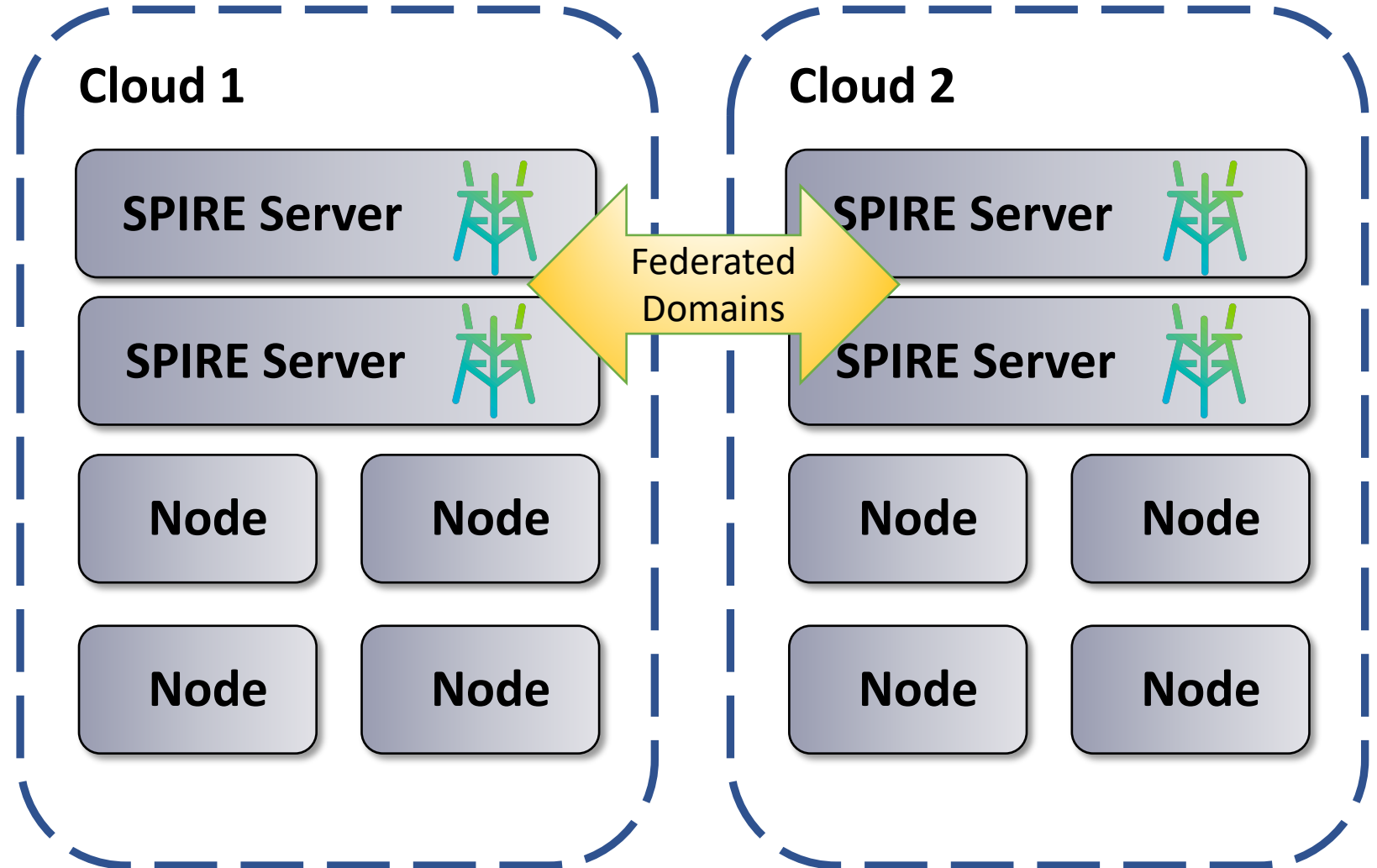
CloudNativeCon

Europe 2020

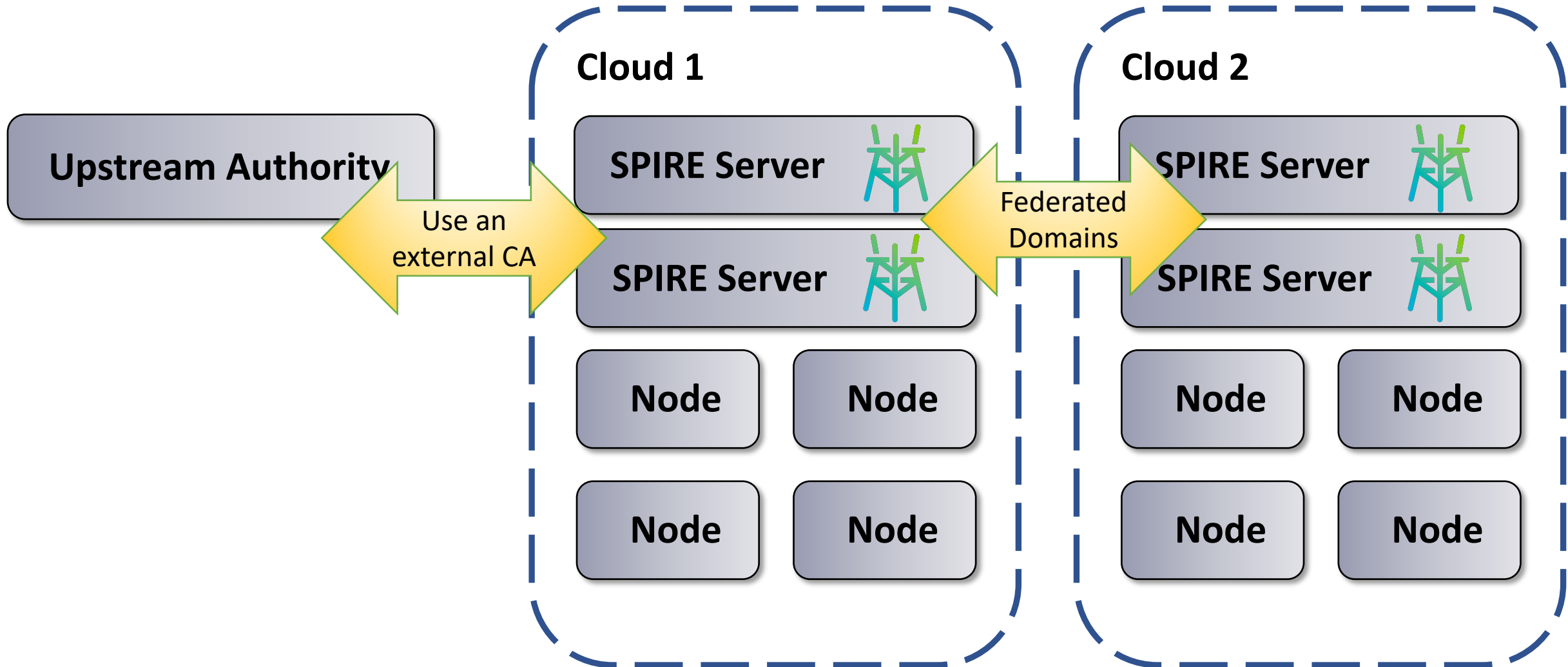
Virtual



SPIRE (our implementation)



SPIRE (our implementation)



SPIRE (our implementation)



KubeCon



CloudNativeCon

Europe 2020

Virtual

- **Why do I need one SPIRE Agent per node?**

SPIRE (our implementation)



- **Why do I need one SPIRE Agent per node?**
- **What if the SPIRE Agent is compromised?**

SPIRE (our implementation)



- **Why do I need one SPIRE Agent per node?**
- **What if the SPIRE Agent is compromised?**
- **What about my old workload that I don't want to change?**

SPIRE (our implementation)



KubeCon



CloudNativeCon

Europe 2020

Virtual

- **Why do I need one SPIRE Agent per node?**
- **What if the SPIRE Agent is compromised?**
- **What about my old workload that I don't want to change?**
- **How do I specify which workloads get which SPIFFE IDs?**



Registration Entries

Node Registration Entry

If a node has:

The aws tag “database”

Then give it the SPIFFE ID:

`spiffe://mycompany/database`

Registration Entries

Node Registration Entry

If a node has:

The aws tag “database”

Then give it the SPIFFE ID:

`spiffe://mycompany/database`

Workload Registration Entry

If a workload has:

The parent ID `spiffe://mycompany/database`

The UID “payments”

Then give it the SPIFFE ID:

`spiffe://mycompany/database/payments`

SPIRE (our implementation)



- **Why do I need one SPIRE Agent per node?**
- **What if the SPIRE Agent is compromised?**
- **What about my old workload that I don't want to change?**
- **How do I specify which workloads get which SPIFFE IDs?**
- **What if the SPIRE Server goes down?**

SPIRE Ecosystem



bloomberg / spire-tpm-plugin

Watch 6 Star 29 Fork 4

Code Issues 2 Pull requests 1 Actions Security Insights

master Go to file Add file Code

About
Provides agent and server plugins for SPIRE to allow TPM 2-based node attestation.
spiffe spire tpm2 tpm-attestation

pawalt Merge pull request #10 from bloombe... ✓ on May 22 18		
ci	add tests	3 months ago
cmd	move agent/server logic to pkg	3 months ago
pkg	add comments to common_test files	2 months ago

SPIRE Ecosystem



KubeCon



CloudNativeCon

Europe 2020

Virtual

bloomberg / spire-tpm-plugin

Watch 6 Star 29 Fork 4

Code Issues 2 Pull requests 1 Actions Security Insights

master

Go to file

- ci add tests
- cmd move agent/server logic to
- pkg add comments to common

bloomberg / vault-auth-spire

Watch 6 Star 22 Fork 5

Code Actions Security Insights

Bloomberg bloomberg
New York, NY

148 repositories 50 members

Code

About

vault-auth-spire is an authentication plugin for Hashicorp Vault which allows logging into Vault using a Spire provided SVID.

spire plugin authn

dennisgove Updates README with new co... on Nov 8, 2019 21

- cmd/plugin Fixes #7: Properly documents and i... 9 months ago
- internal/common Fixes #7: Properly documents and i... 9 months ago
- .gitignore Added comments, moved things aro... 10 months ago

SPIRE Ecosystem



KubeCon



CloudNativeCon

Europe 2020

Virtual

[bloomberg / spire-tpm-plugin](#) Watch 6 Star 29 Fork 4

Code Issues 2 Pull requests 1 Actions Security Insights

master Go to file

pawalt Merge pull request #10 from bloombe...

- ci add tests
- cmd move agent/server logic to
- pkg add comments to common

[bloomberg / vault-auth-spire](#) Watch 6 Star 22 Fork 5

Code Issues Security Insights

Bloomberg bloomberg New York, N

148 repositories

dennisgove Updates RE

- cmd/plugin Fixe
- internal/common Fixe
- .gitignore Add

[github / emissary](#) Watch 72 Star 20 Fork 0

Code Issues 1 Pull requests Actions Projects Wiki

master Go to file Add file Code

joewilliams Update README.md 6 days ago 3

- cmd/emissary initial commit 7 days ago
- examples initial commit 7 days ago
- mocks initial commit 7 days ago
- pkg initial commit 7 days ago

About

- Envoy External Authorization API
- Bridge To SPIFFE Workload API
- Readme
- MIT License

Next Steps



Who's Using SPIFFE?

Anyone using Istio, Kuma, NSM, Consul Connect, Hamlet, or several other service mesh technologies is using at least part of SPIFFE!

Who's Using SPIRE?

ByteDance (TikTok)

Square

Bloomberg

Anthem (Health Insurance)

Uber

GitHub

Stripe

TransferWise

Others we don't know about....

Next Steps



Learn More:

Find out more at spiffe.io

Regular Community Days

Join the SPIFFE Slack: slack.spiffe.io

More Talks:

Evan Gilman – [Introduction to SPIFFE and SPIRE](#)

Andrew Harding – [Running SPIRE In Large Scale, Enterprise-Grade Environments](#)
[Building Zero Trust based Authentication in Healthcare with SPIRE](#)

SPIRE Deep Dives at [HPE Discover](#)

Contribute!



KubeCon



CloudNativeCon

Europe 2020

Virtual

Why Service Identity

Service Identity Approaches

SPIFFE (the standard)

SPIRE (the implementation)

Next Steps

Thank You!

[@d_feldman](#)

dan.feldman@hpe.com

Time for Questions

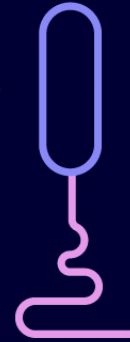
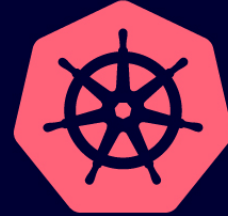


KubeCon



CloudNativeCon

Europe 2020



Virtual



KEEP CLOUD NATIVE

CONNECTED

