Introduction to SPIFFE/SPIRE

Emiliano Berenbaum
and Scott Emmons

SCYTALE

AGENDA

- What is SPIFFE
- What is SPIRE
- Announcements since last KubeCon
- SPIRE 0.8

SCYTALE

SPIFFE talks at KubeCon 2019

Introduction to SPIFFE	Tuesday, May 21 11:55
Zero Trust Service Mesh with Calico, SPIRE and Envoy	Wednesday, May 22 11:05
Deep Dive: SPIFFE	Wednesday, May 22 14:50
Securing Multi-Cloud Cross-Cluster Communication with SPIFFE and SPIRE	Thursday, May 23 14:00
Uber x Security: Why and How we Built Our Workload Identity Platform	Thursday, May 23 16:45

SPIFFE

SCYTALE

SPIFFE

- SPIFFE ID
- SPIFFE Verified Identity Document
- Workload API
- Federation API

SPIFFE ID

spiffe://example.org/foo

SCYTALE

SPIFFE ID

spiffe://example.org/foo

Scheme: SPIFFE

Trust Domain

Workload Name

SCYTALE

SPIFFE Verifiable Document

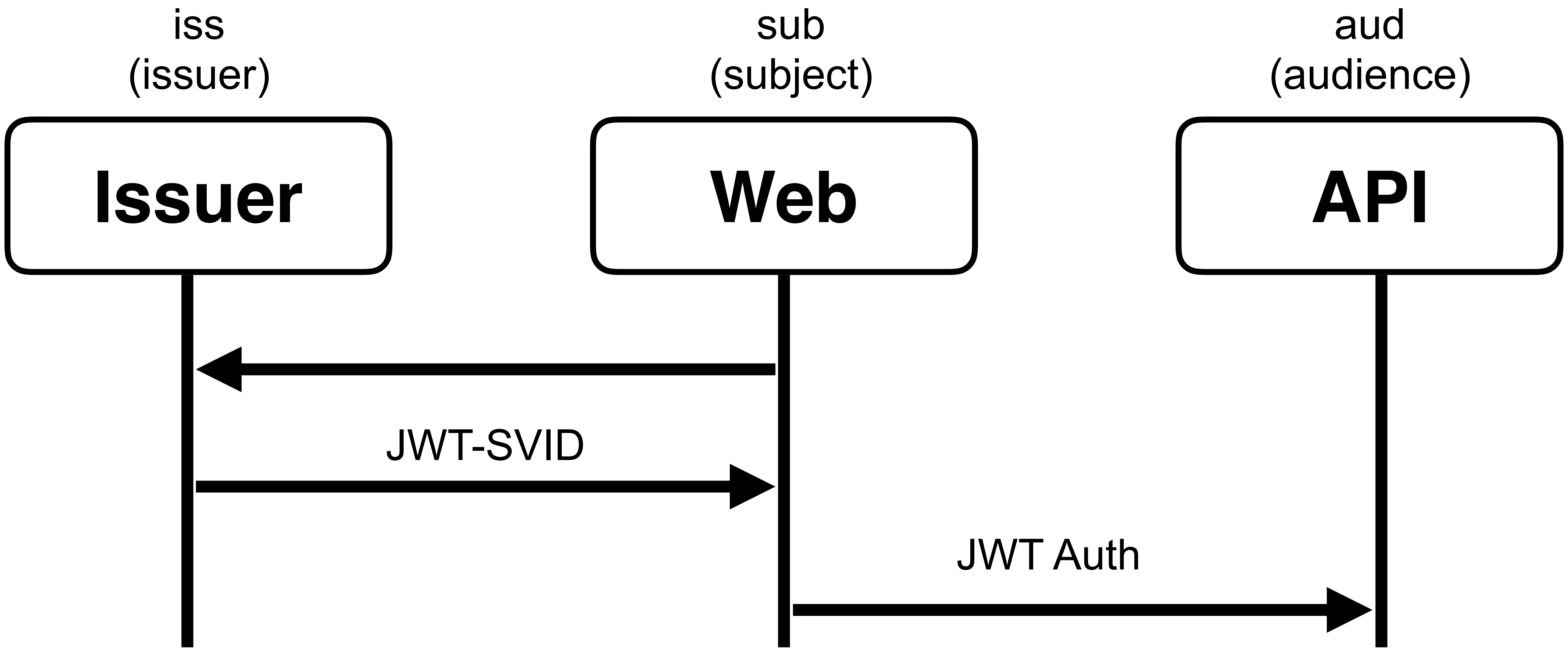
spiffe://example.org/foo

X.509 SVID

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=SPIFFE
        Validity
            Not Before: Dec  1 15:30:54 2017 GMT
            Not After : Dec  1 16:31:04 2017 GMT
        Subject: C=US, O=SPIRE
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (521 bit)
                pub:
                    04:01:….
                ASN1 OID: secp521r1
                NIST CURVE: P-521
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Key Agreement
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Alternative Name:
                URI:spiffe://example.org/host/workload
    Signature Algorithm: sha256WithRSAEncryption
```

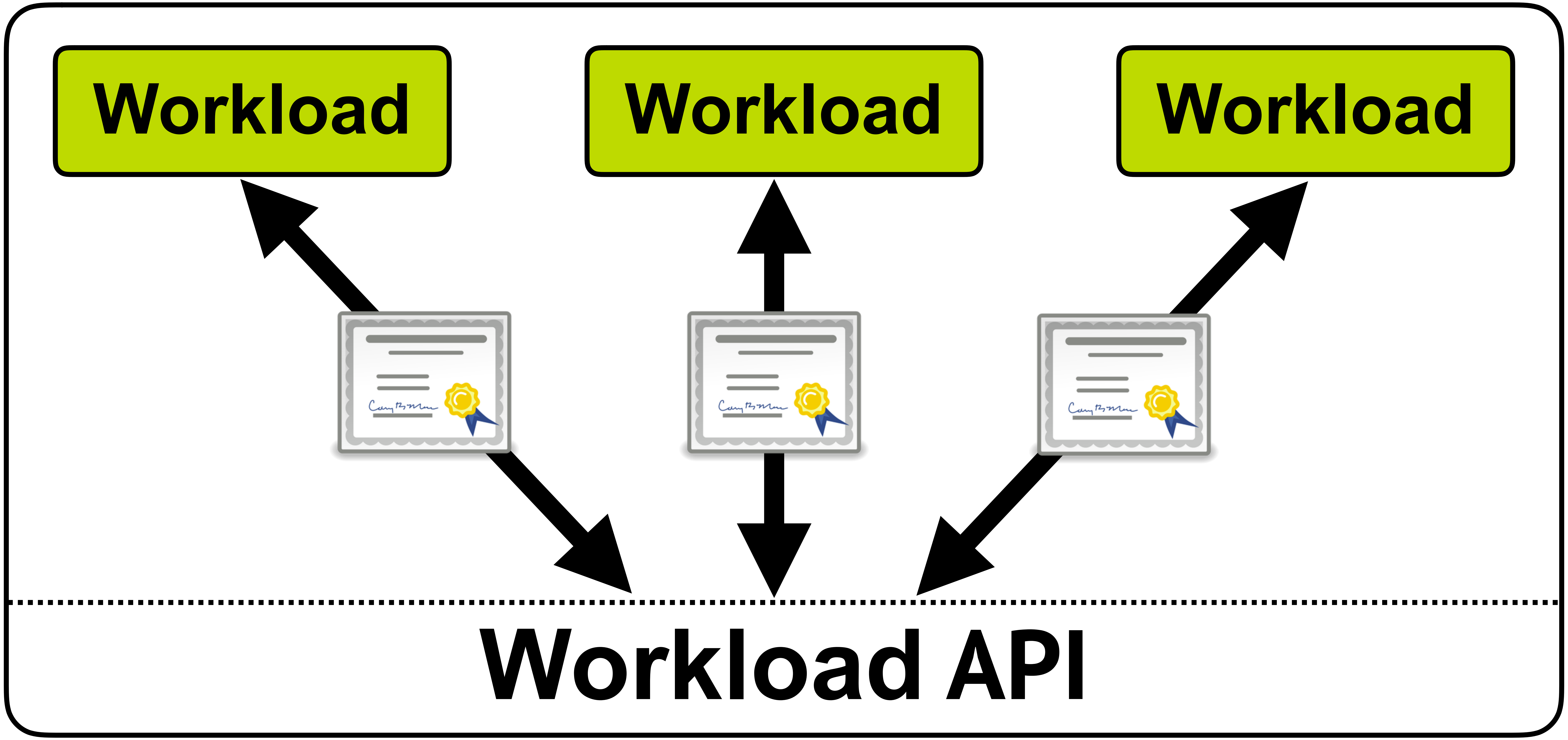
JWT SVID

```
{
    “aud”:  “sidecar”,
    “exp”:   1551170050,
    “iat”:    1551169760,
    “sub”:    “spiffe://staging1.acme.com/payments/web"
}
```



SCYTALE

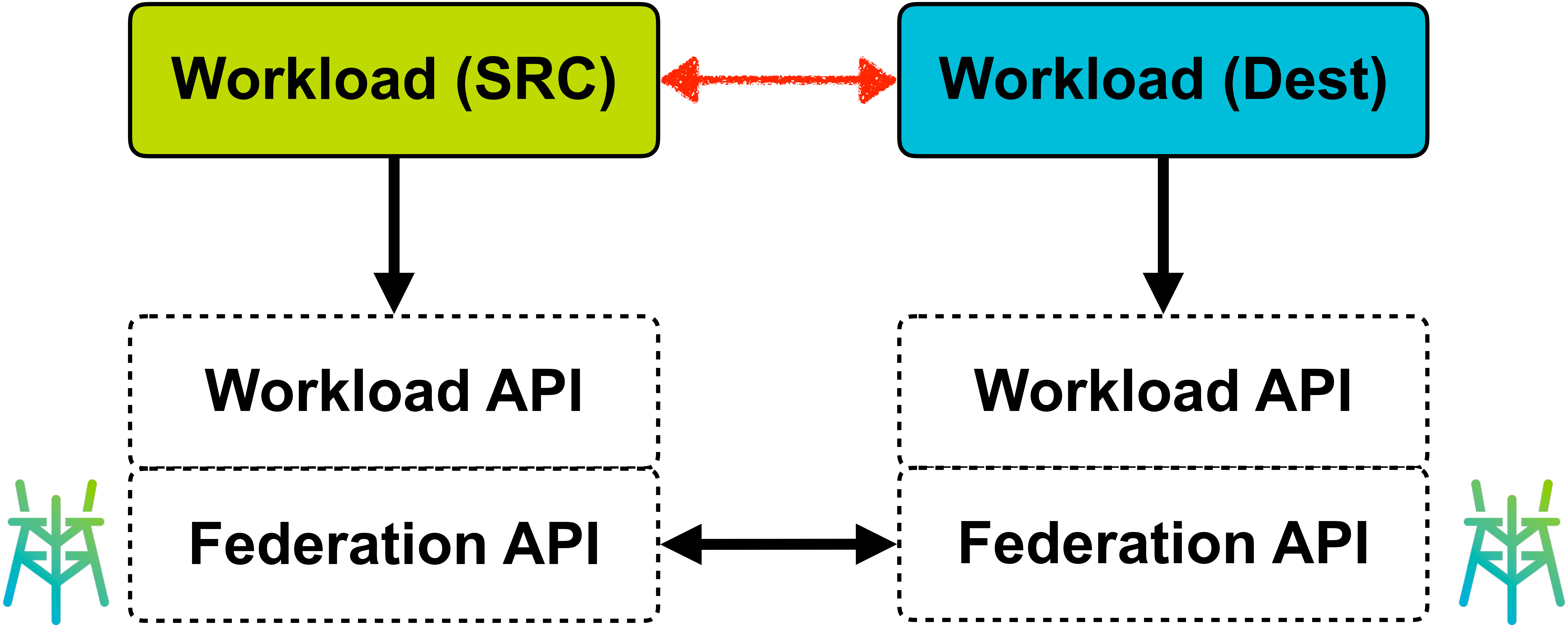
SPIFFE Workload API



SCYTALE

FEDERATION FEDERATION
FEDERATION FEDERATION
imgflip.com

SPIFFE Federation API



Workload (SRC)

Workload (Dest)

Workload API

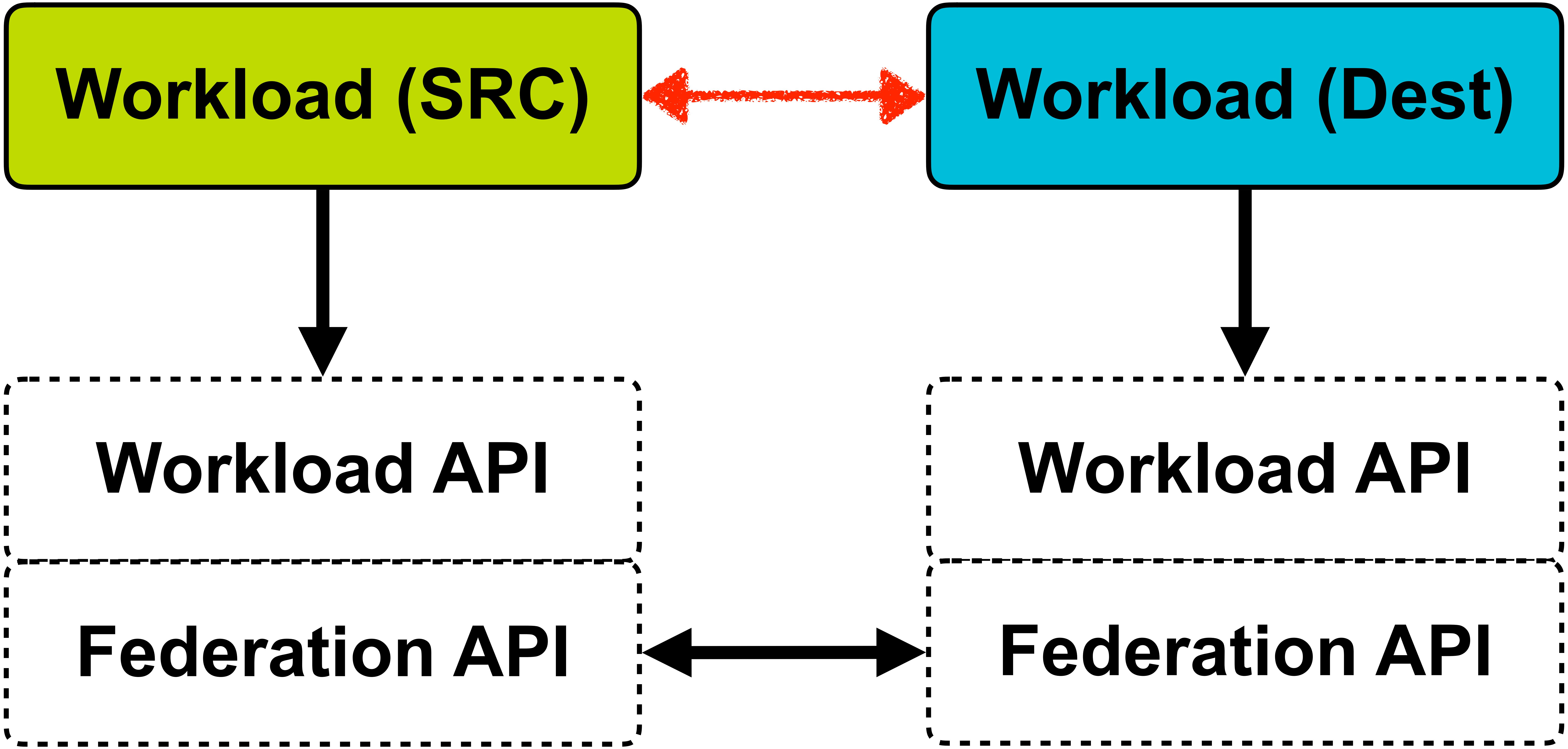
Federation API

Workload API

Federation API

SCYTALE

SPIFFE Federation API



Workload (SRC)

Workload (Dest)

Workload API

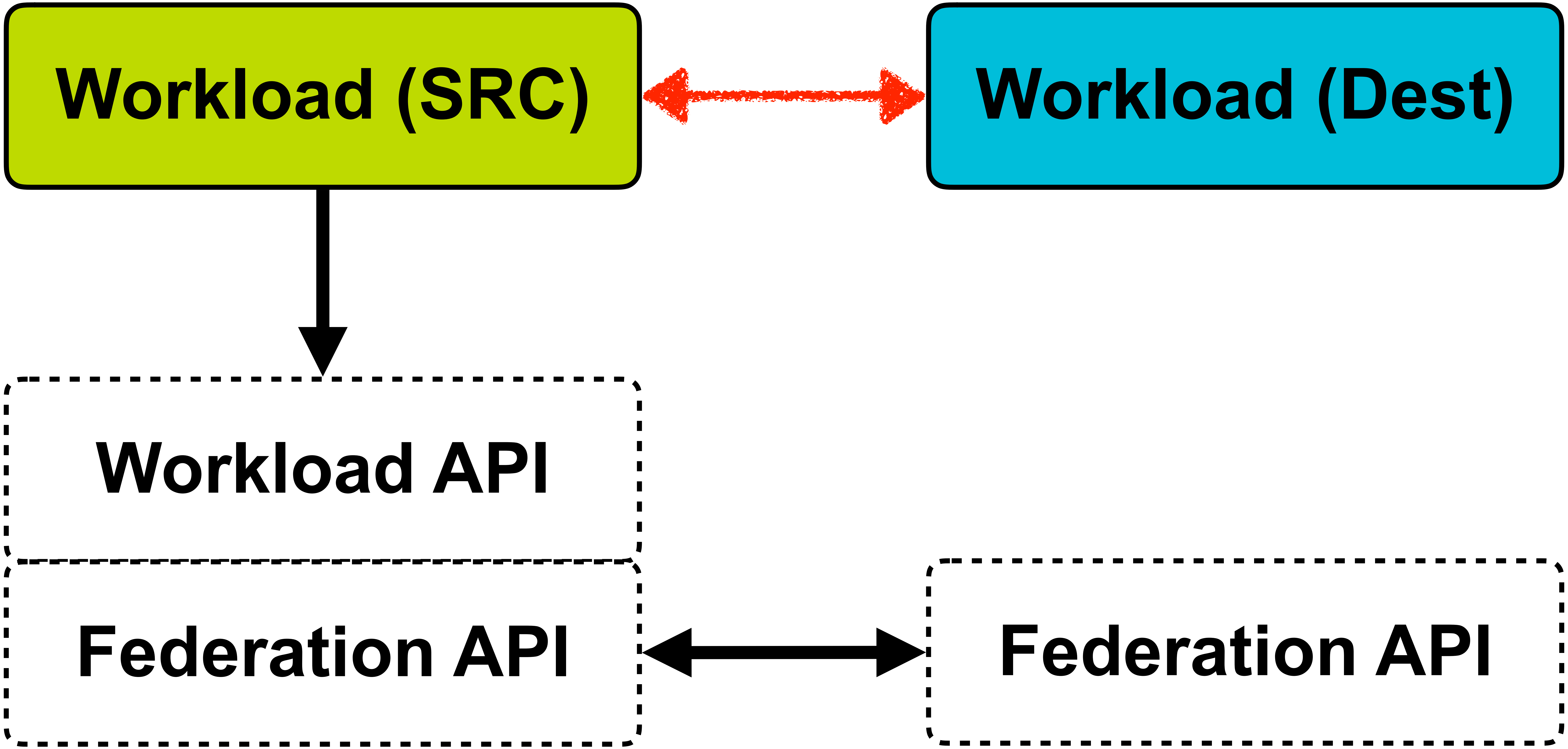
Workload API

Federation API

Federation API

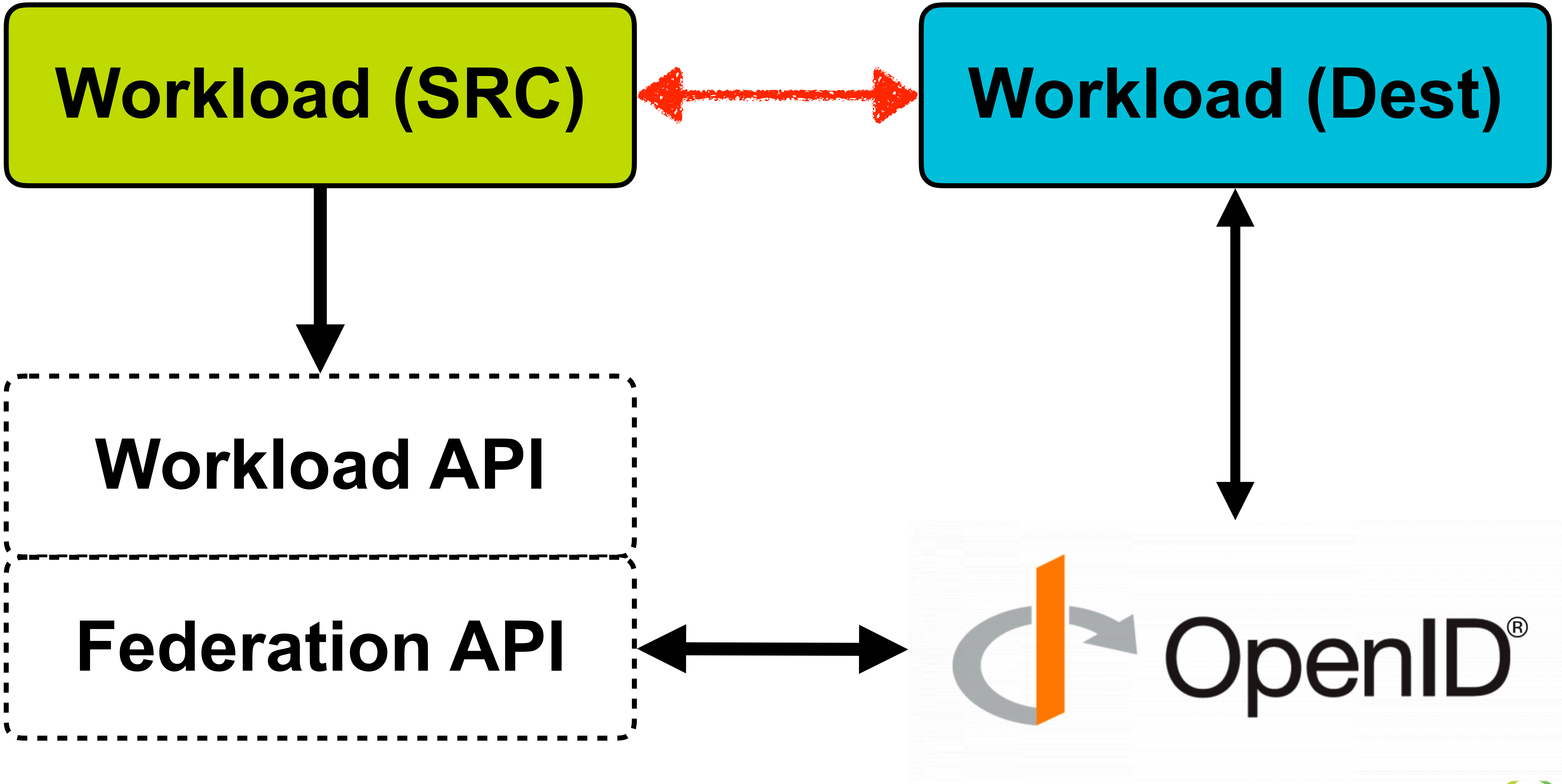
SCYTALE

SPIFFE Federation API



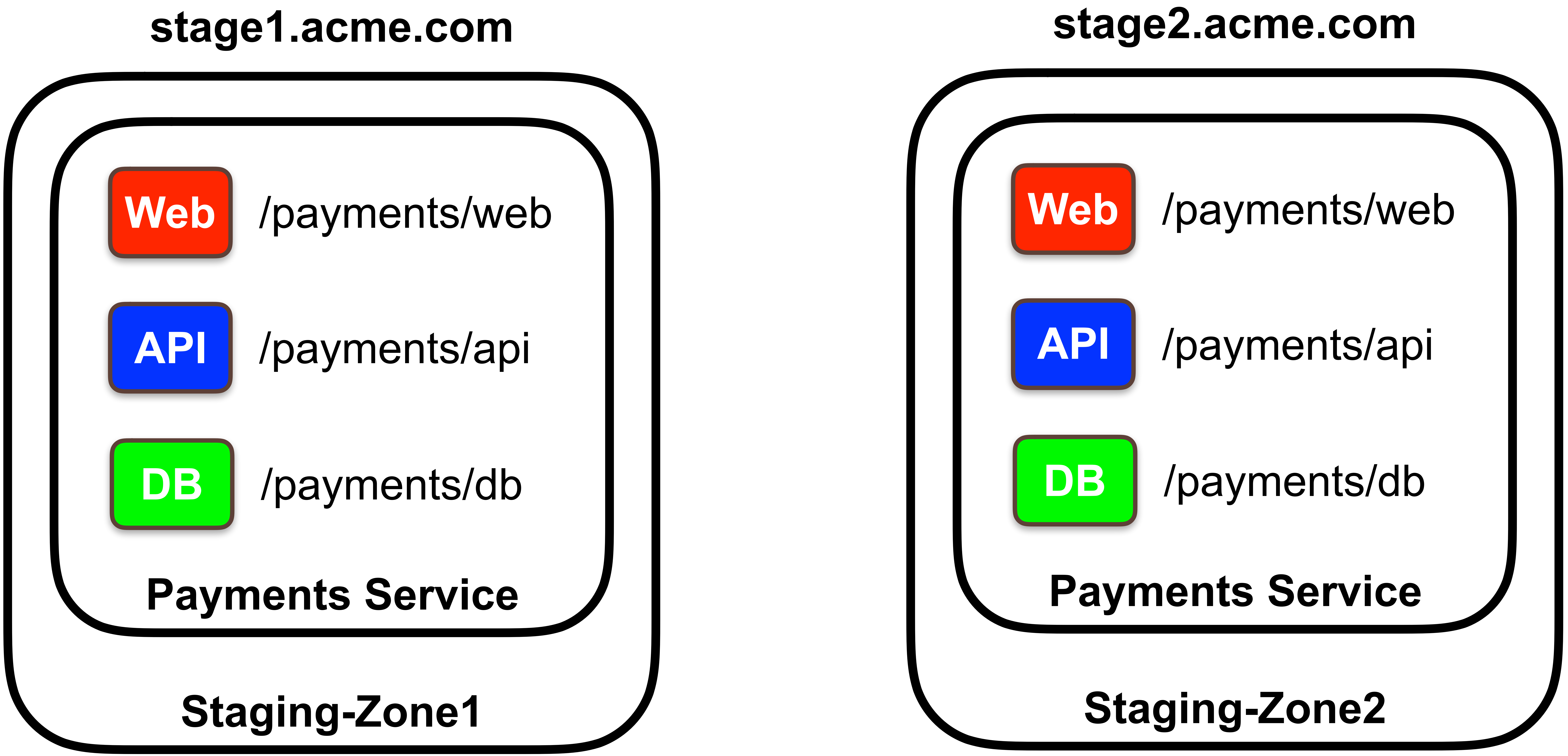
SCYTALE

SPIFFE Federation API



SPIRE

SCYTALE



stage1.acme.com

Web /payments/web

API /payments/api

DB /payments/db

Payments Service

Staging-Zone1

stage2.acme.com

Web /payments/web

API /payments/api

DB /payments/db

Payments Service

Staging-Zone2

SCYTALE

stage1.acme.com

spiffe://stage1.acme.com/payments/api

API /payments/api

DB /payments/db

Payments Service

Staging-Zone1

stage2.acme.com

Web /payments/web

API /payments/api

spiffe://stage2.acme.com/payments/db

Payments Service

Staging-Zone2

SCYTALE

stage1.acme.com

spiffe://stage1.acme.com/payments/api

API /payments/api

DB /payments/db

Payments Service

Staging-Zone1

stage2.acme.com

Web /payments/web

API /payments/api

spiffe://stage2.acme.com/payments/db

Payments Service

Staging-Zone2

SCYTALE

SPIRE Server

Identity Mapping

Node Attestation

SVID Issuance

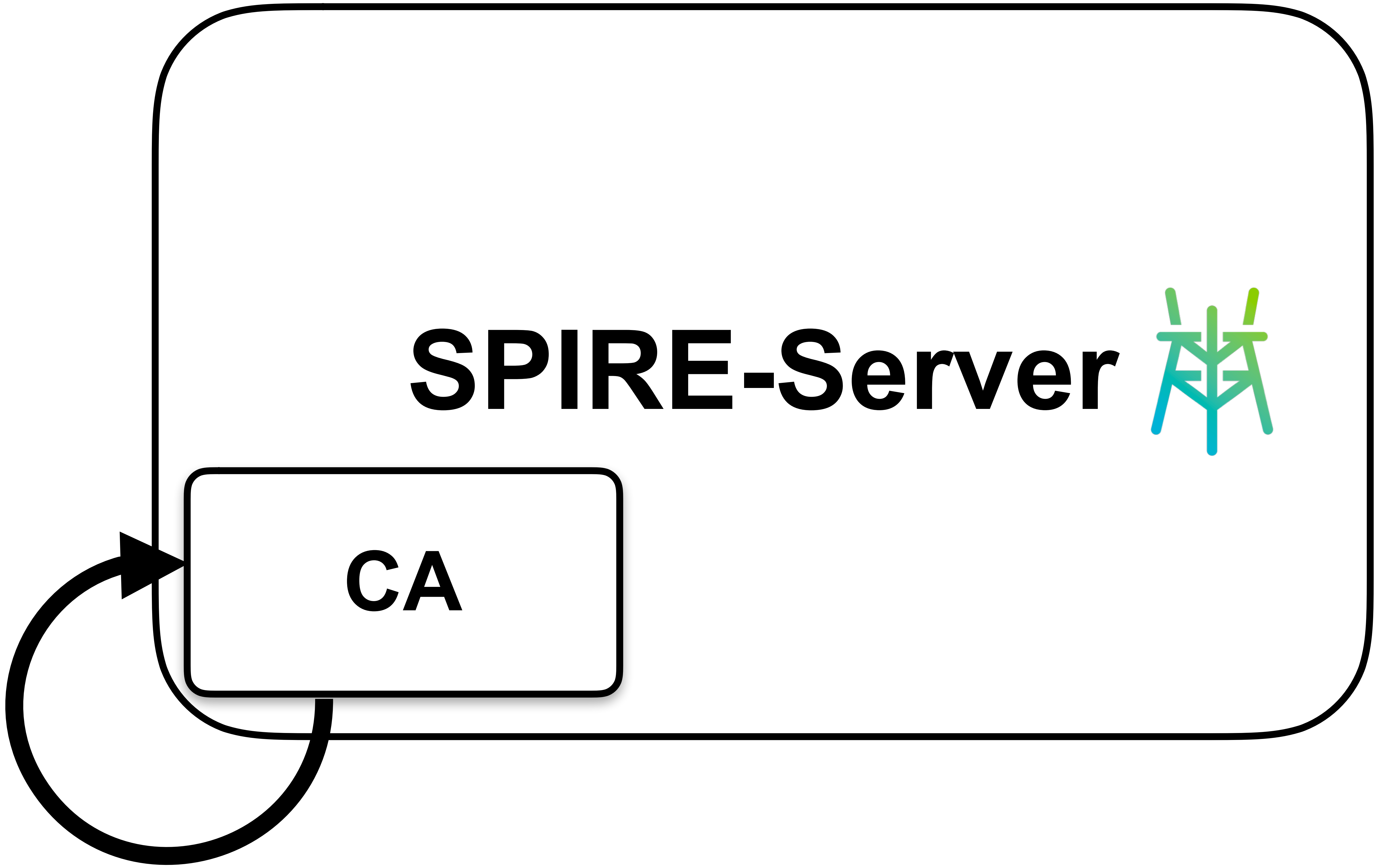
Federation API

SPIRE Agent

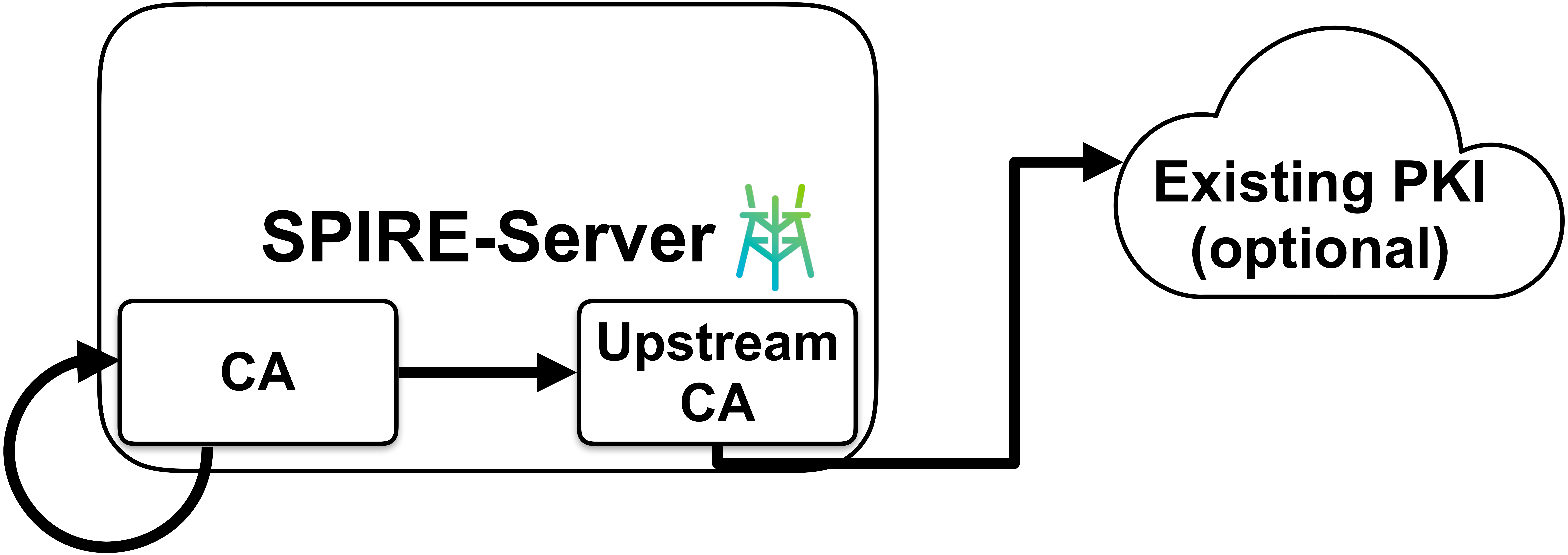
Workload Attestation

Workload API

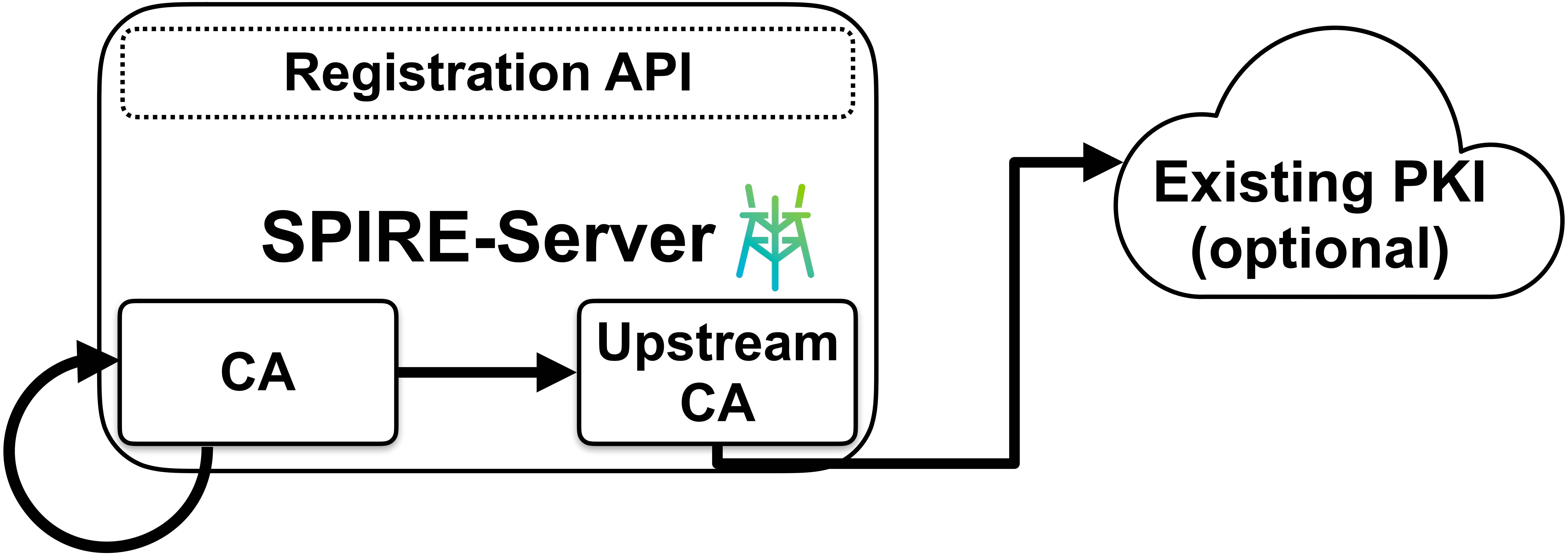
SPIRE Walkthrough



SPIRE Walkthrough



SPIRE Walkthrough

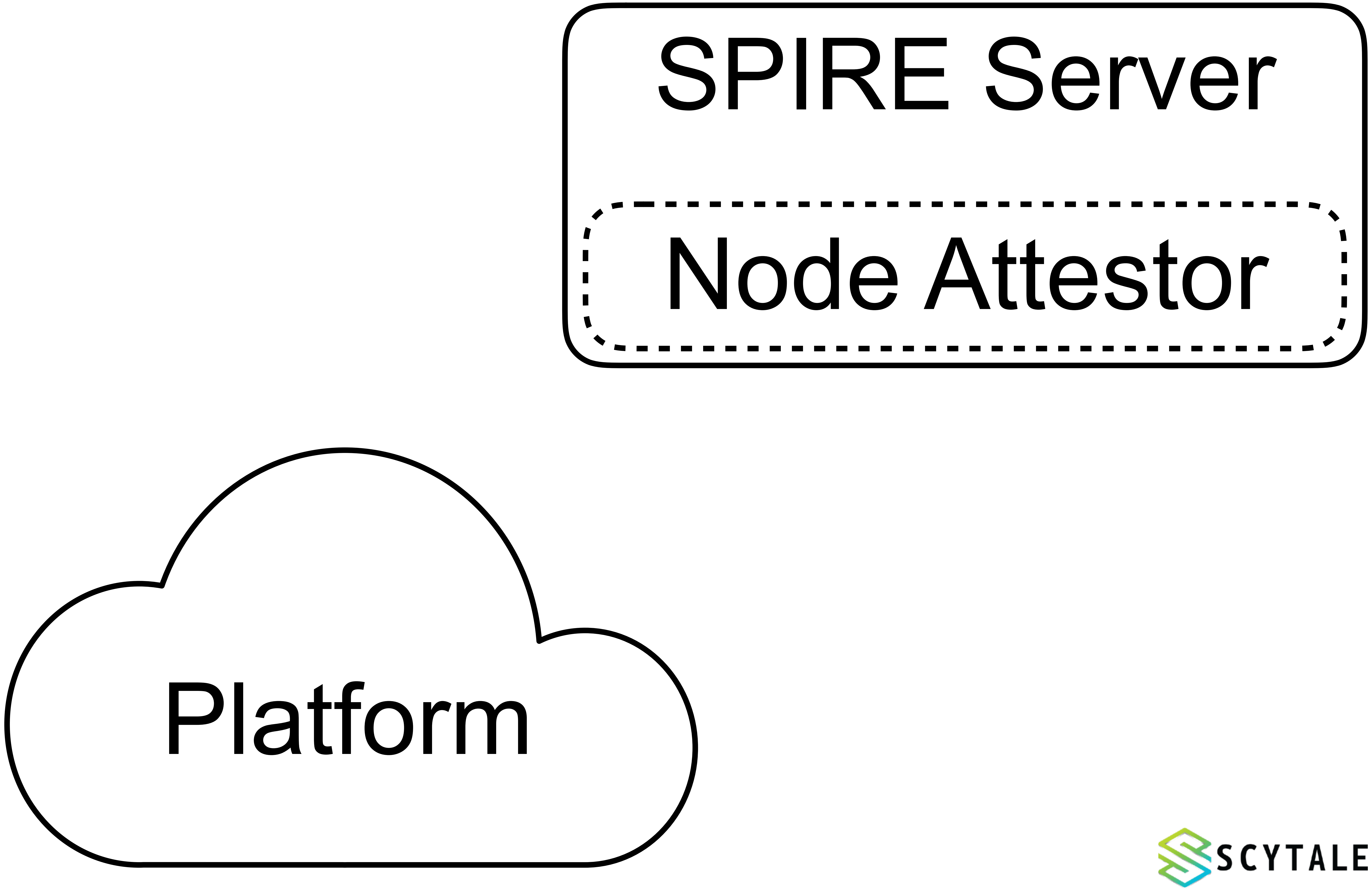


SCYTALE

SPIRE Walkthrough

Parent ID:	spiffe://staging.acme.com/k8s/cluster/staging
Selector:	K8s:ns:payments
Selector:	K8s:sa:staging
Selector:	docker:image-id: 746b819f315e
SPIFFE ID:	spiffe://staging.acme.com/payments/web

SPIRE Walkthrough

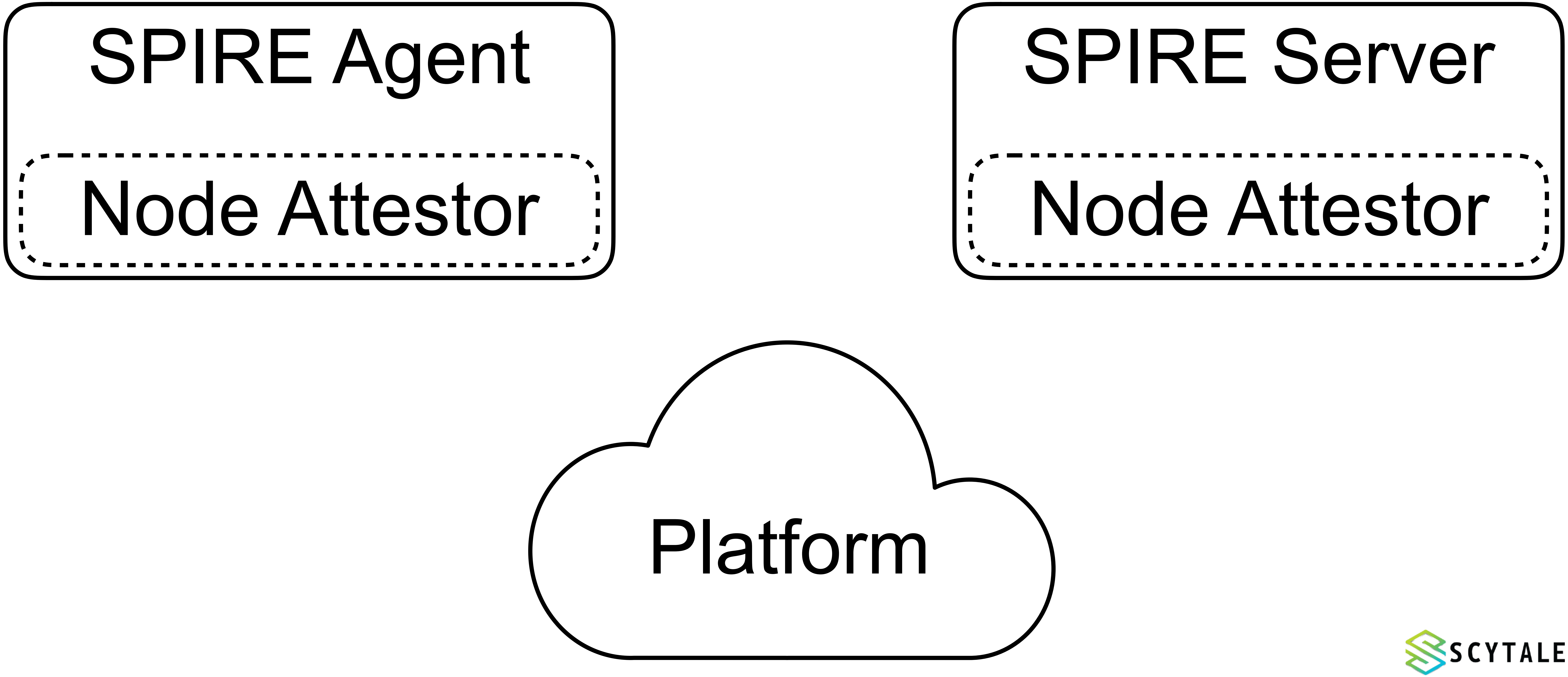


SPIRE Server

Node Attestor

Platform

SPIRE Walkthrough



SPIRE Agent

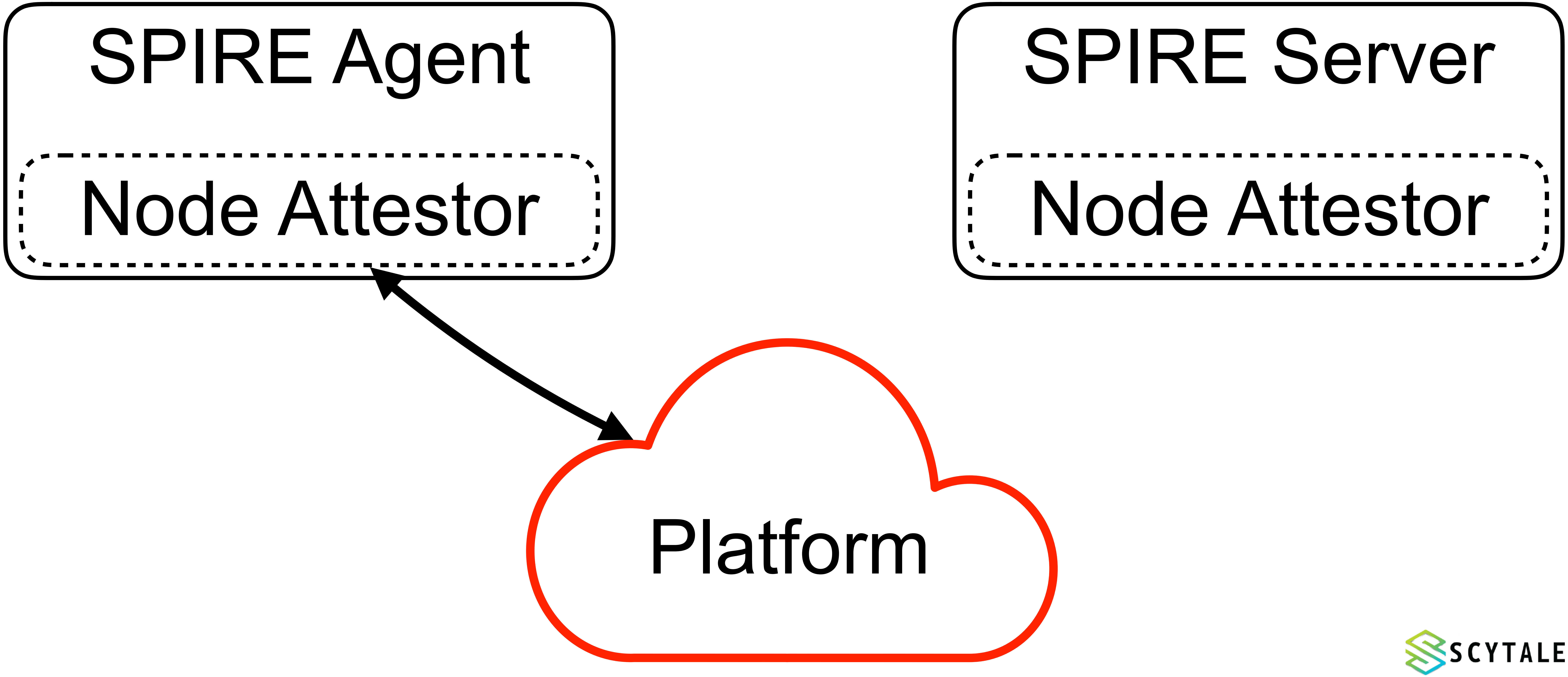
Node Attestor

SPIRE Server

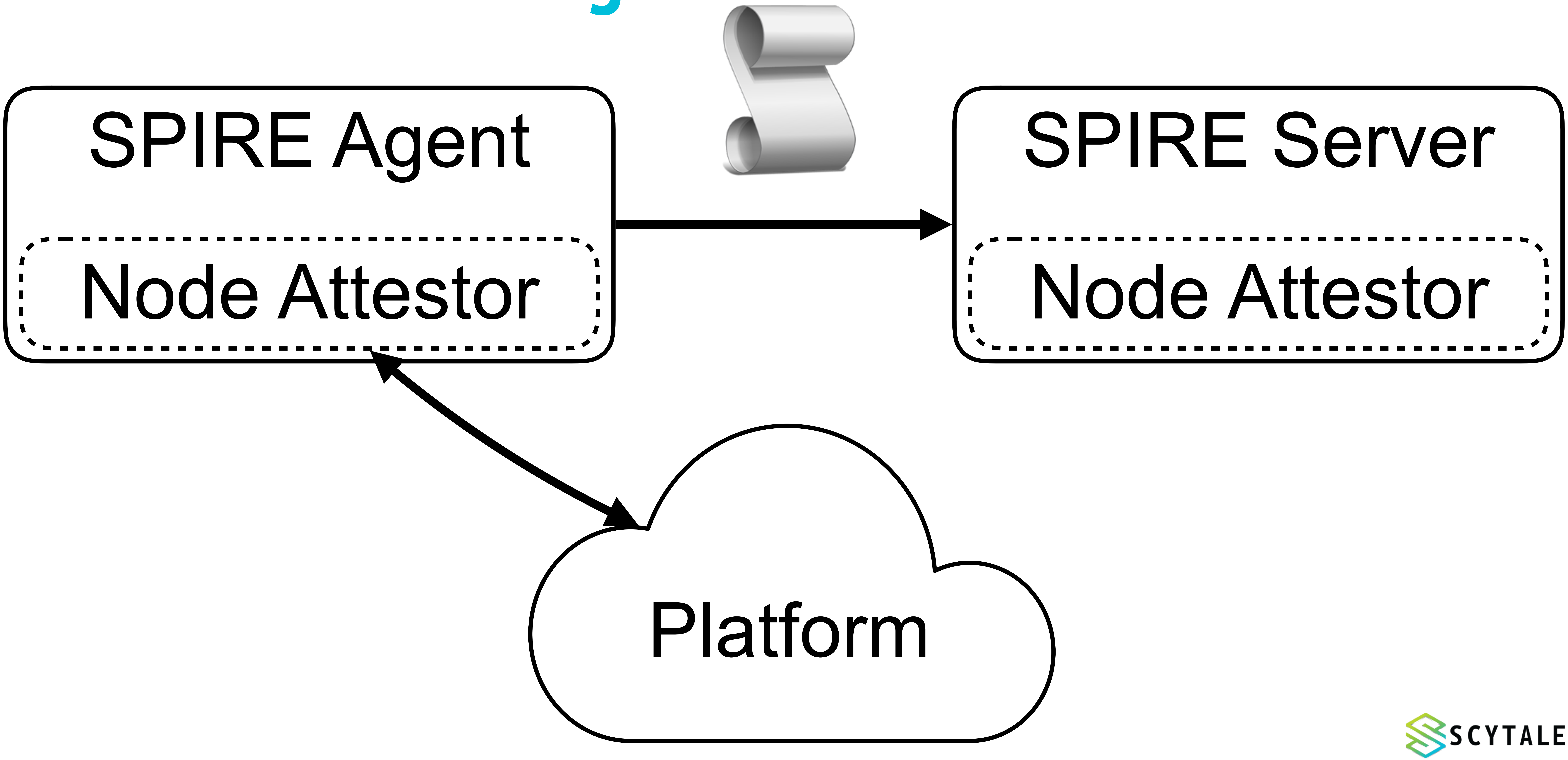
Node Attestor

Platform

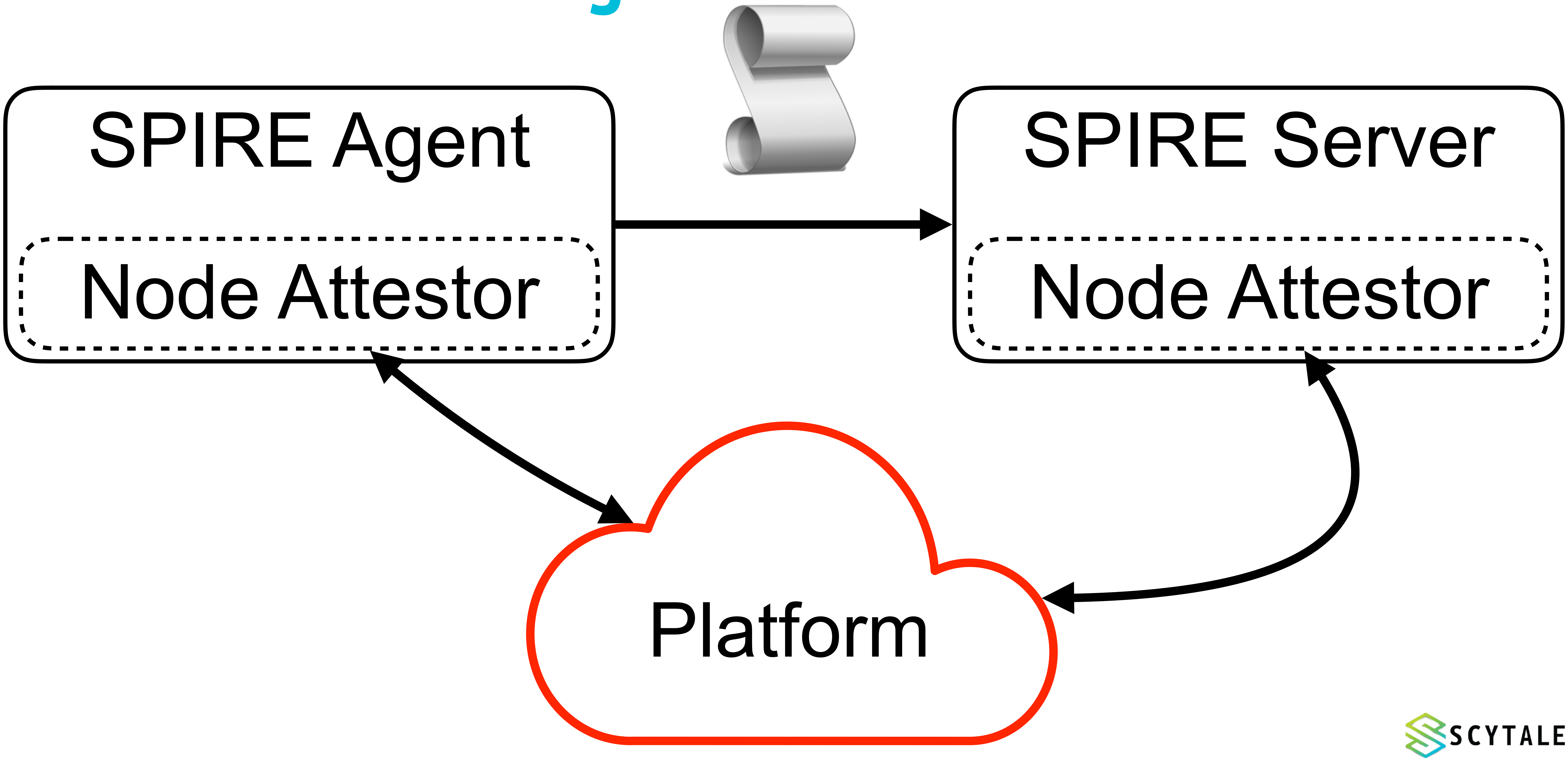
SPIRE Walkthrough



SPIRE Walkthrough

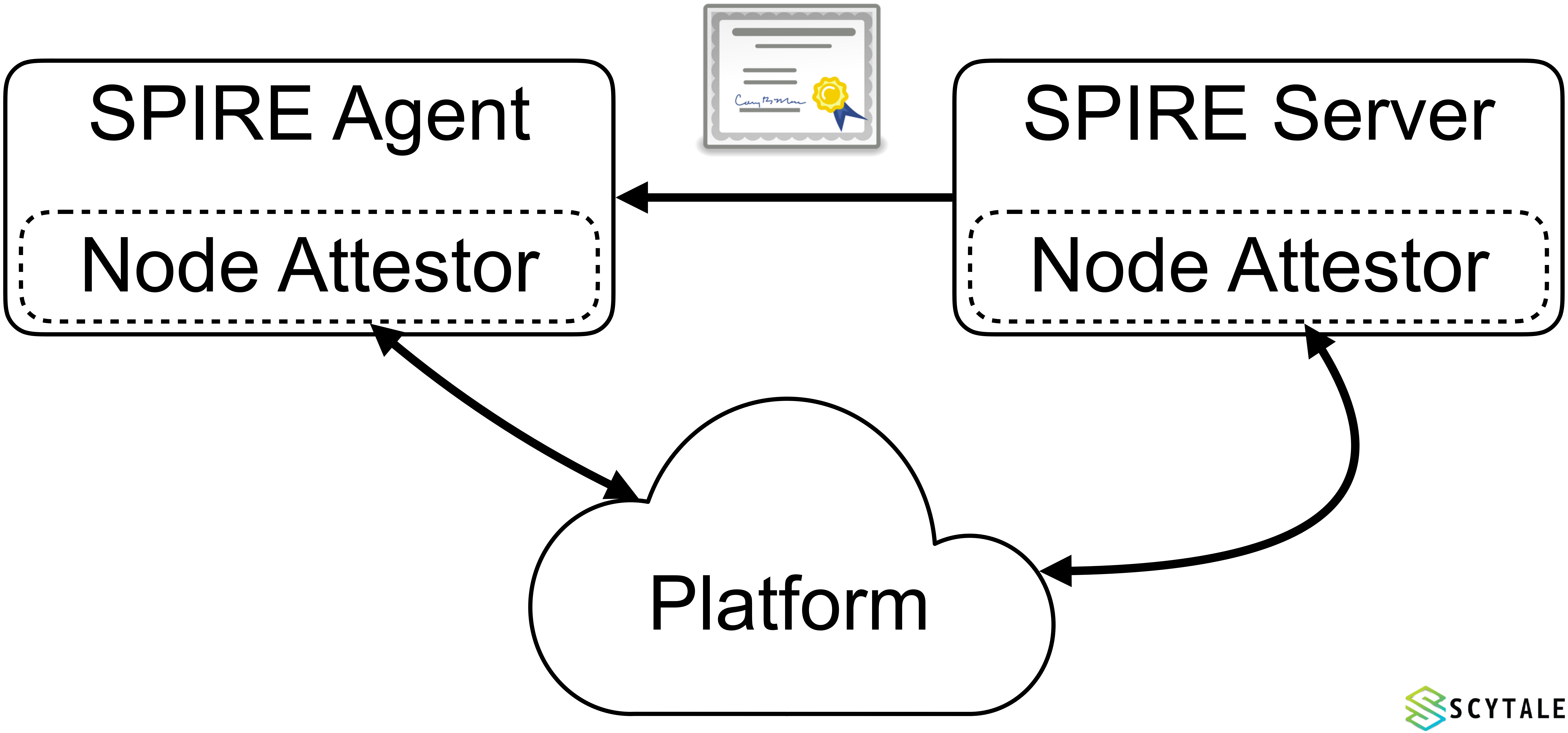


SPIRE Walkthrough



SCYTALE

SPIRE Walkthrough



SPIRE Agent

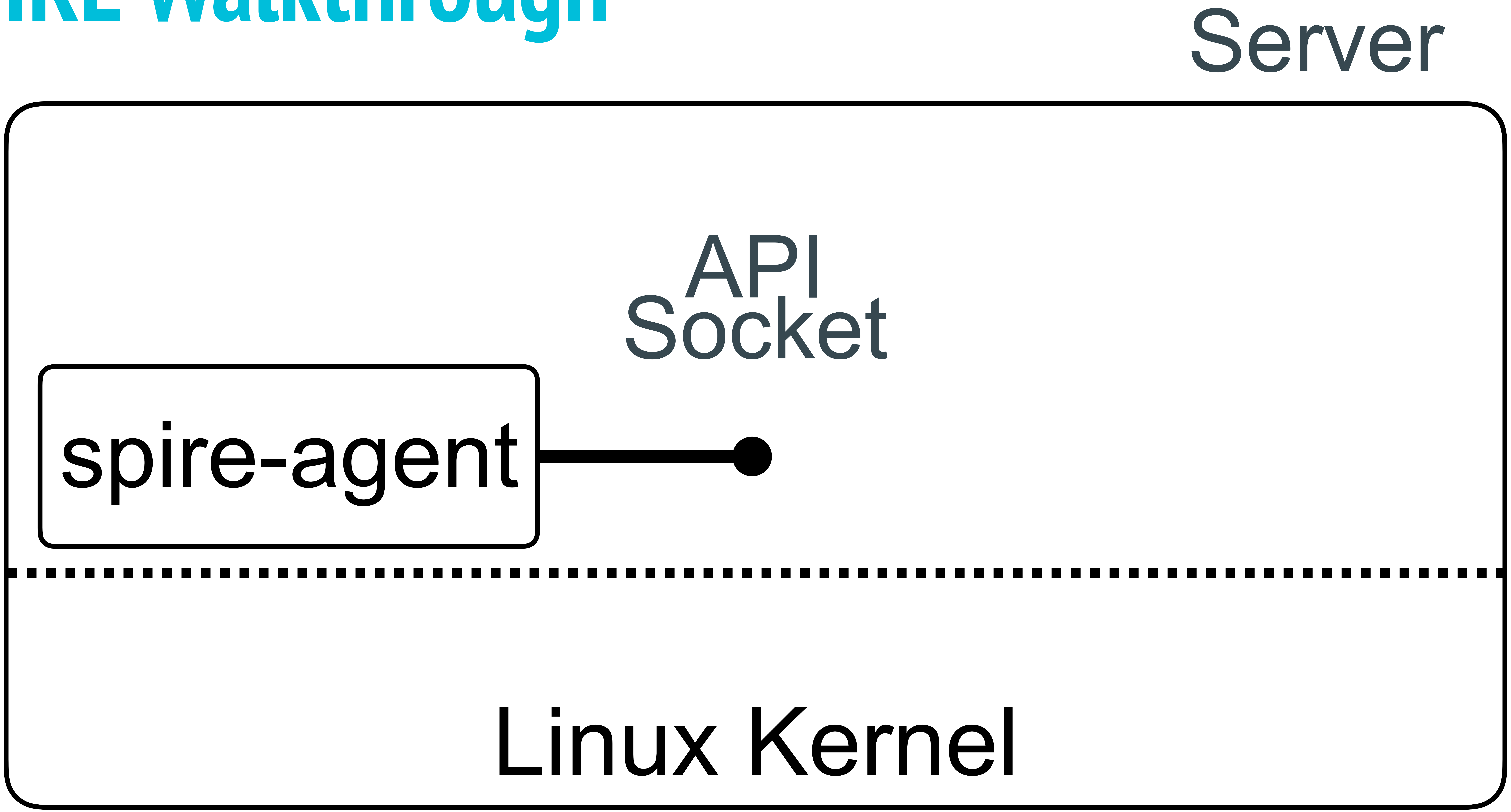
Node Attestor

SPIRE Server

Node Attestor

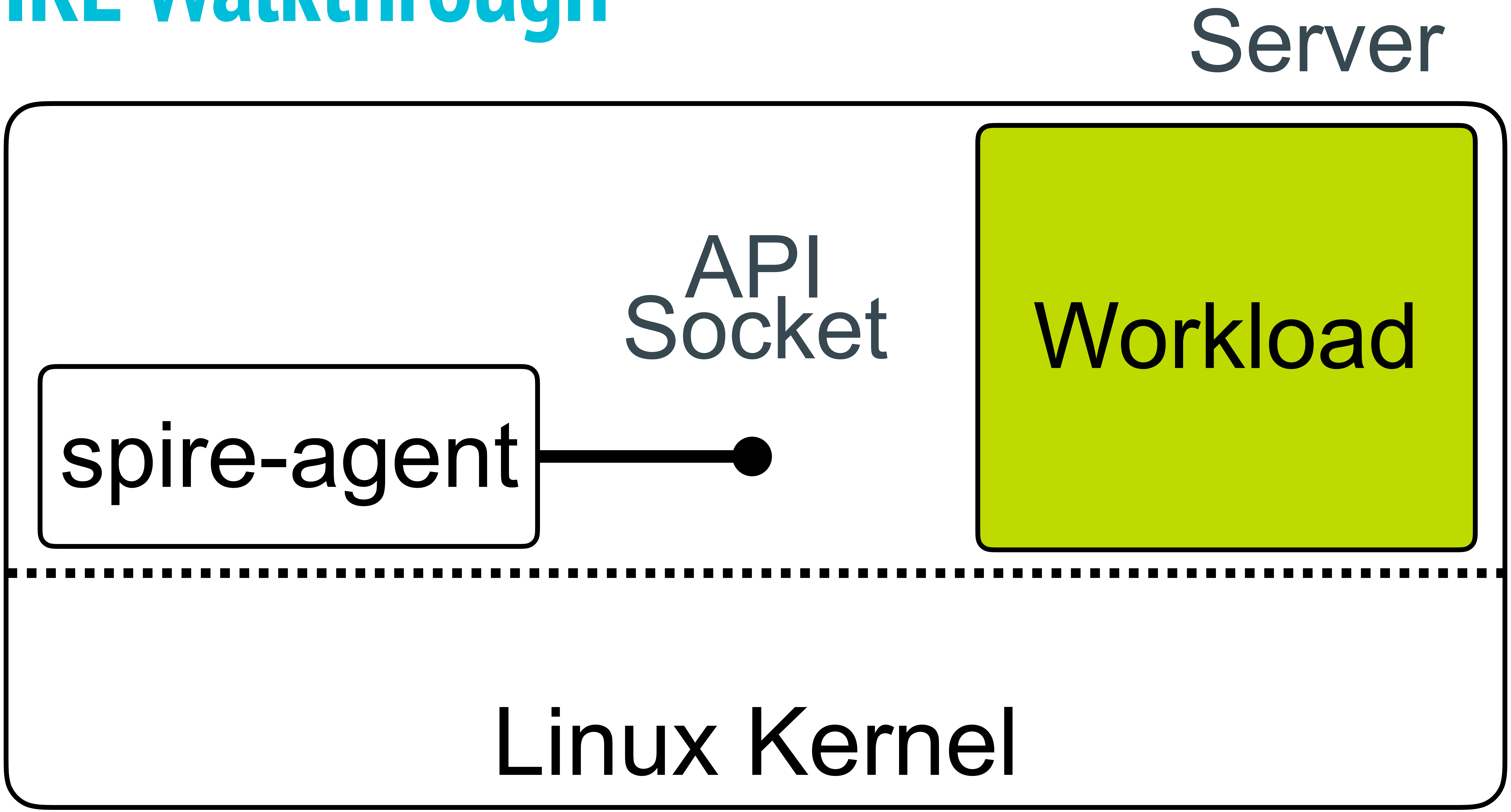
Platform

SPIRE Walkthrough

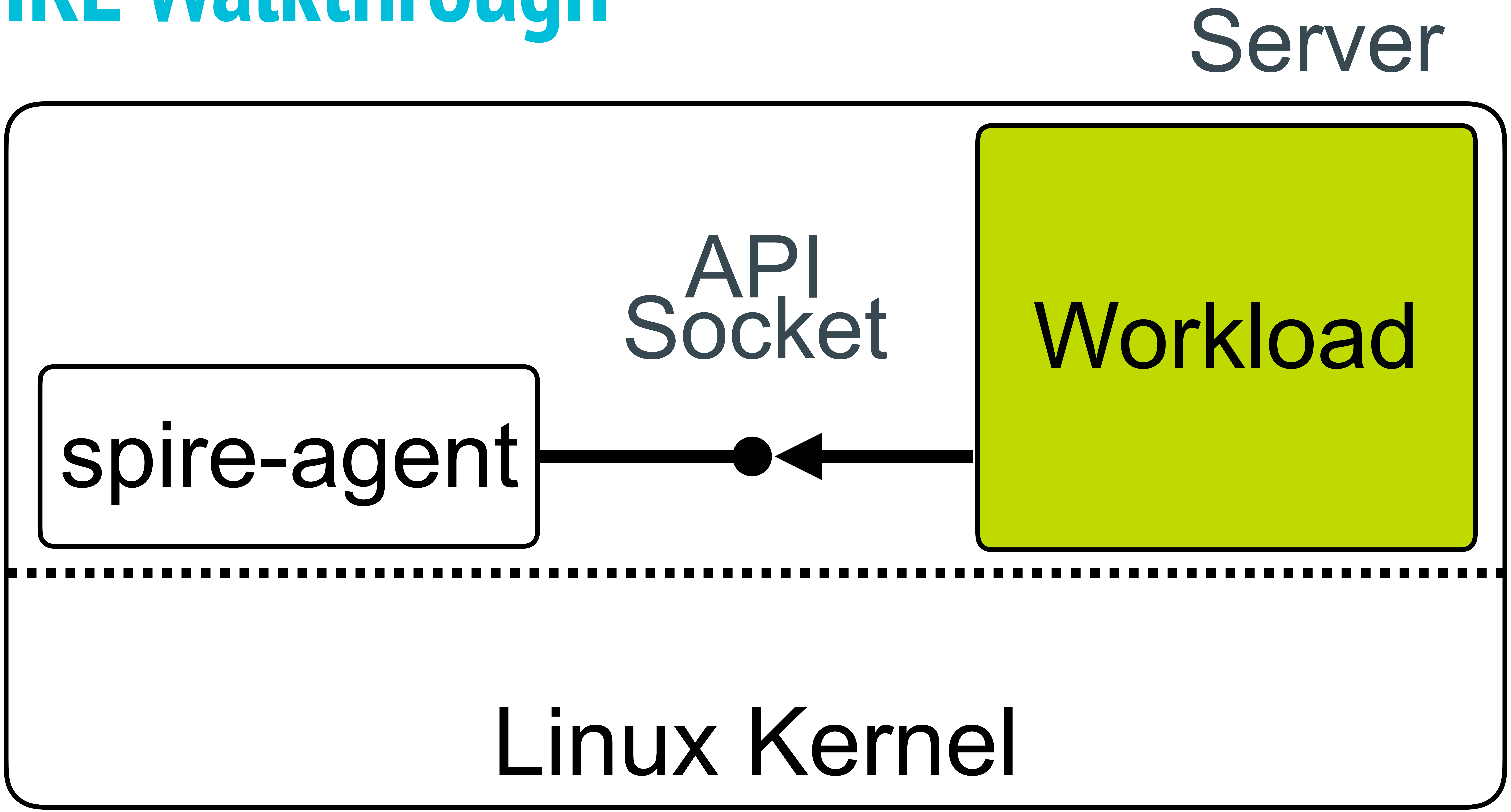


SCYTALE

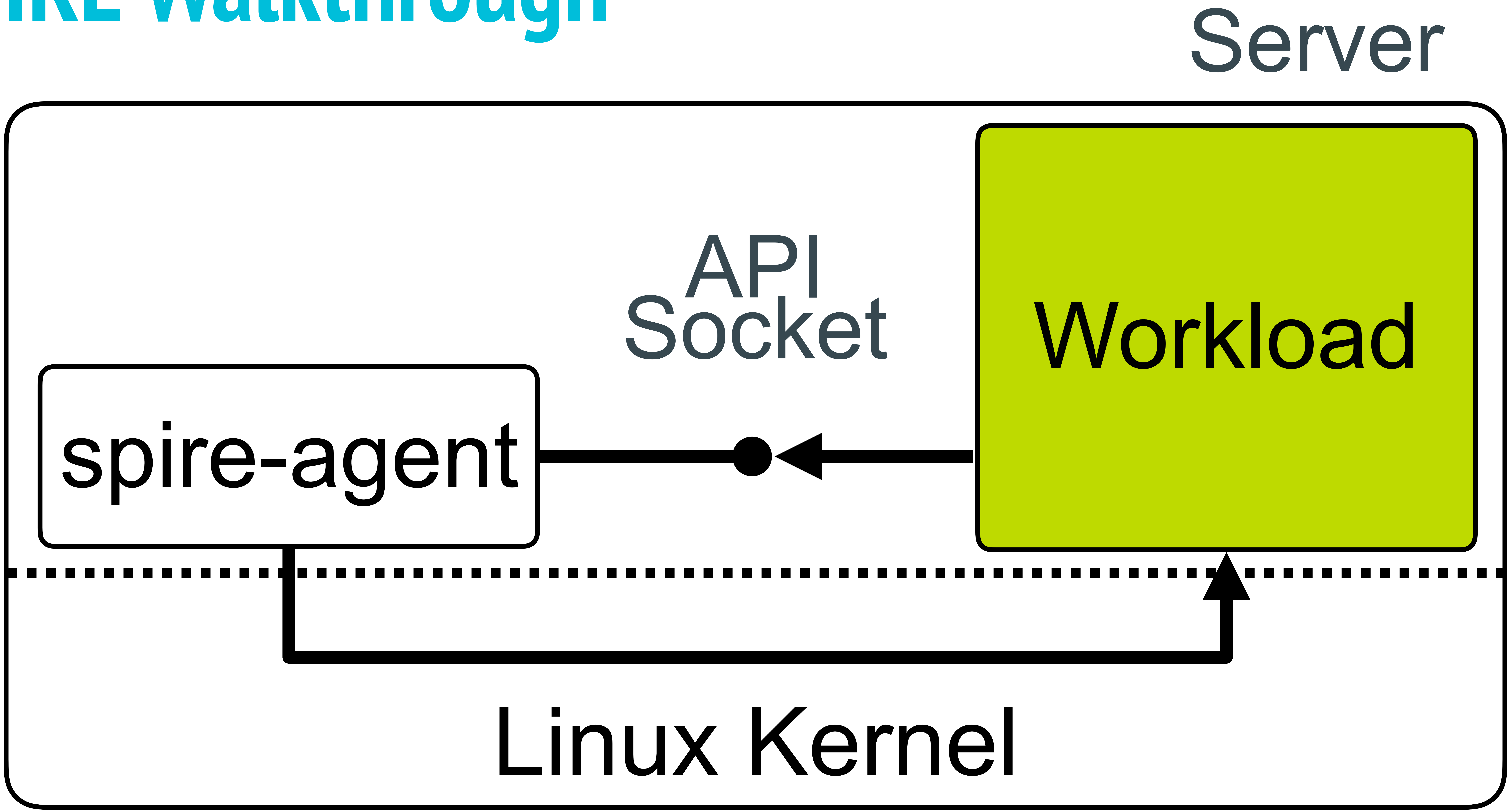
SPIRE Walkthrough



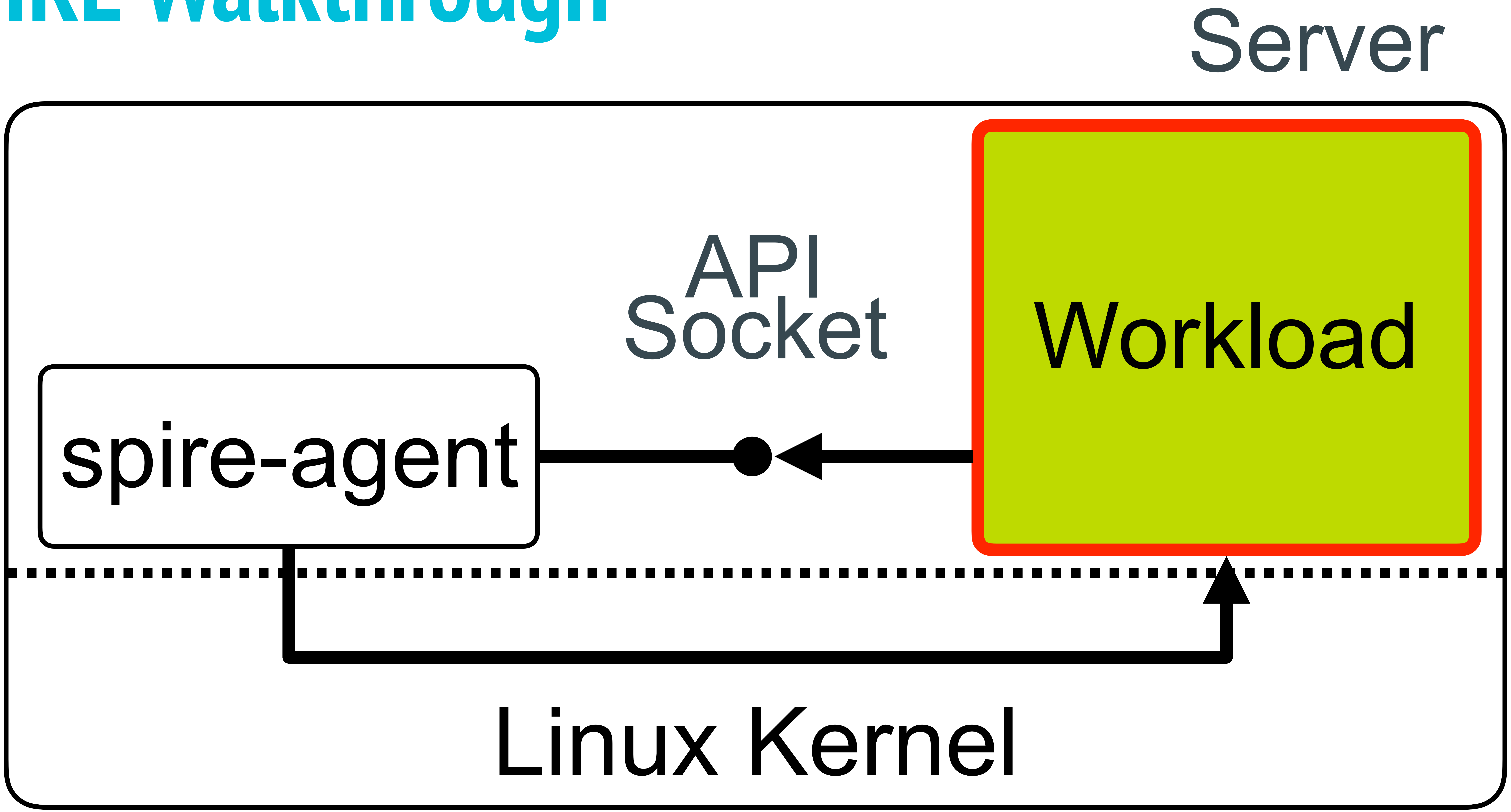
SPIRE Walkthrough



SPIRE Walkthrough

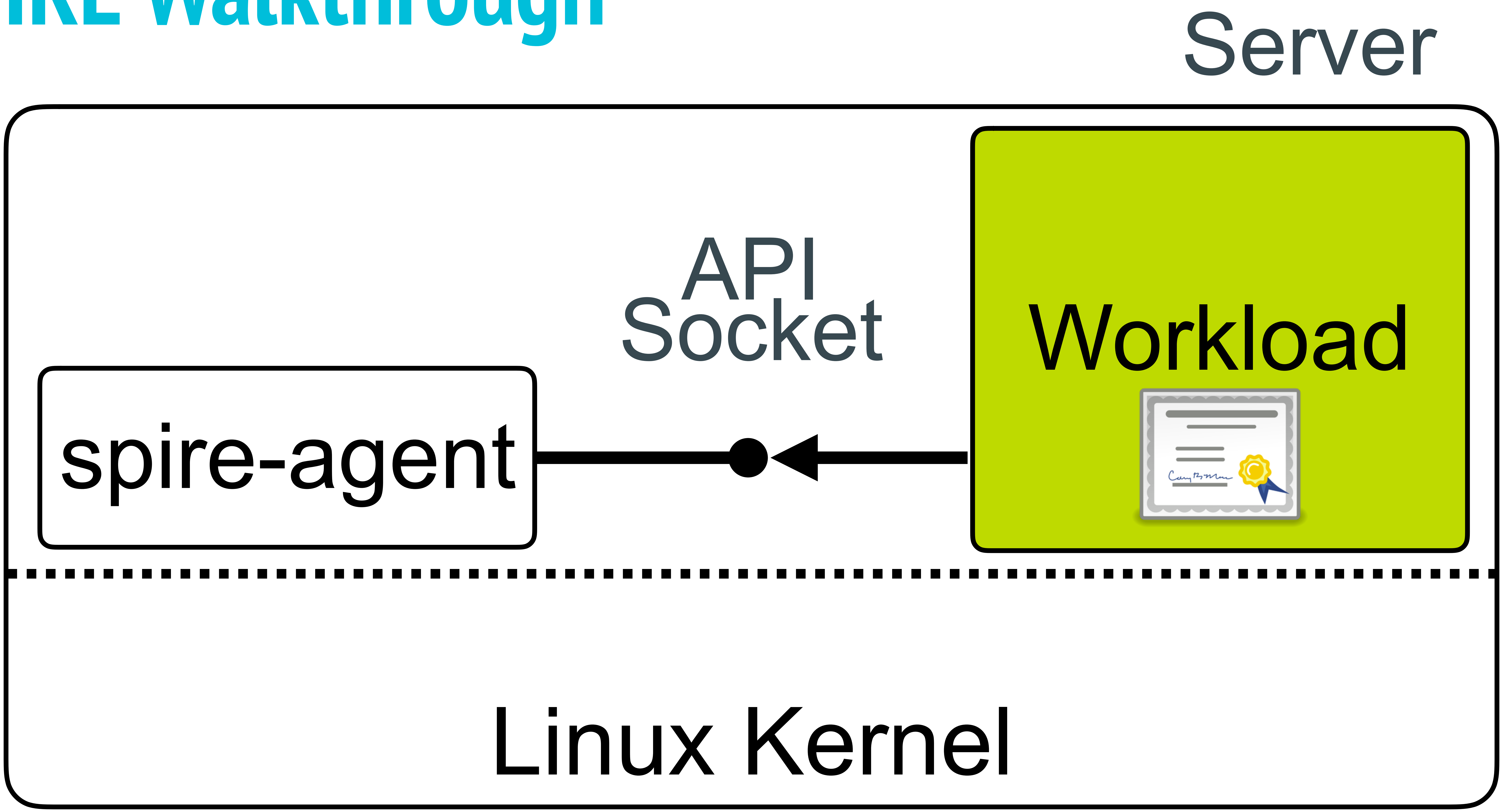


SPIRE Walkthrough



SCYTALE

SPIRE Walkthrough



Updates

SCYTALE

SPIRE Updates

- 120 + Merged PRs
- 3 Releases
- 18 Contributors
- 13 Major Features
- Getting Started Guides and Sample Configurations

Thank you to the contributors

- **MySQL datastore plugin for SPIRE server** (thanks to Matt McPherrin and Mat Byczkowski of Square Inc)
- **Node attestation using SSH certificates** (Tyler Julian of Uber Inc)
- **Support for using the AWS Secrets Manager as an upstream signing authority for SPIRE issued identities** (thanks to Michael Weissbacher of Square Inc.)
- **The ability to specify a common name (CN) and DNSName in a X.509 SVID** (thanks to Andrew Moore of Uber Inc.)
- **Not forgetting:** Michael Merril (Vonage), Jonathan Oddy (Transferwise), Trilok Geer (Huawei), Costin Manolache (Google), Denis Kolegov (B.i.Zone), Evan Gilman, Andrew Harding, Maximiliano Churichi, Marcos Yedro, Agustin Fayo, Jenny Beth Schafer and Scott Emmons (Scytale)

SIG-SPEC Update

- JWT-SVID Completed
  - SPIRE Implementation available
- Federation Draft stabilized
  - SPIFFE Trust Domain and Bundle

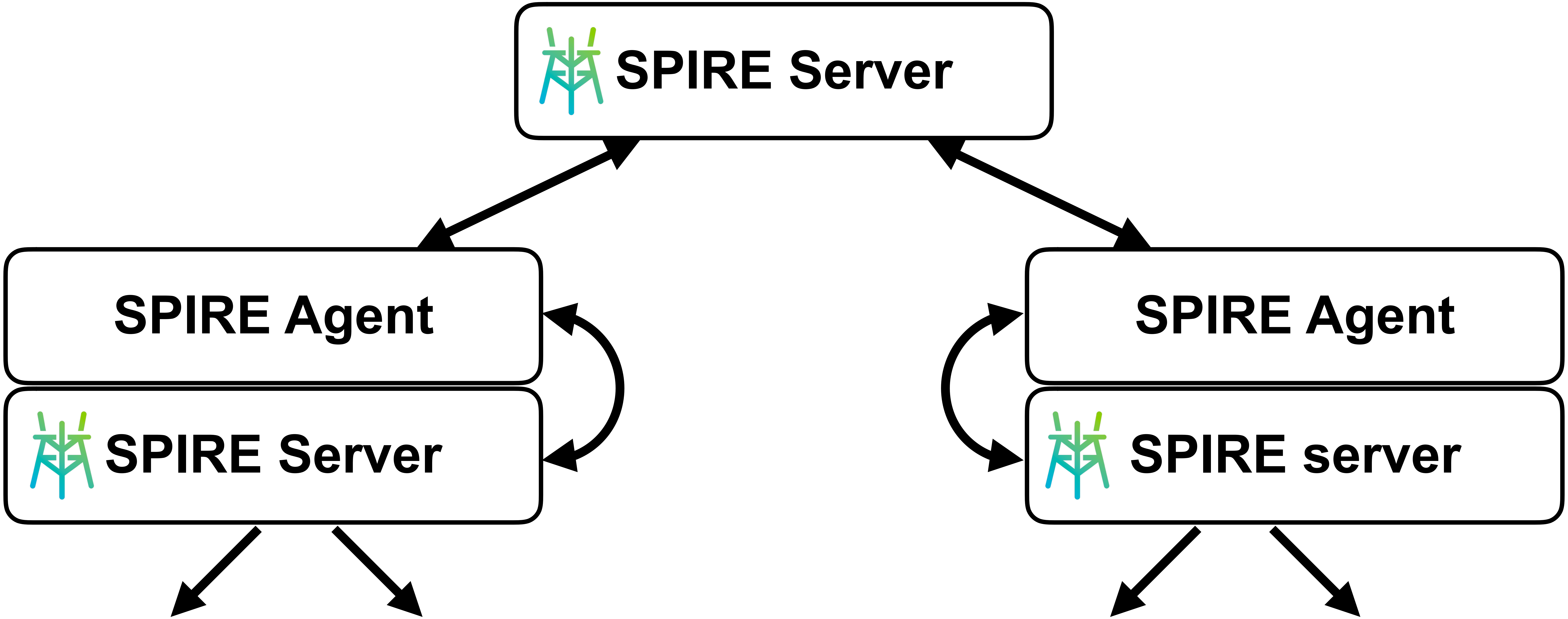
SPIRE 0.8

SCYTALE

SPIRE 0.8

- AWS Secret Manager Upstream CA
- Telemetry
- Plugin and Host Services
- k8s Bundle Notifier Plugin
- Nested SPIRE

Nested SPIRE



●- Fix a bug in which the agent periodically logged connection errors (#906)

●- Kubernetes SAT node attestor now supports the TokenReview API (#904)

●- Agent cache refactored to improve memory management and fix a leak (#863)

●- UpstreamCA "disk" will now reload cert and keys when needed (#903)

●- Introduced Nested SPIRE: server clusters can now be chained together (#890)

●- Fix a bug in AWS IID NodeResolver with instance profile lookup (888)

●- Improved workload attestation and fixed a security bug related to PID reuse (#886)

●- New Kubernetes bundle notifier for keeping a bundle configmap up-to-date (#877)

●- New plugin type Notifier for programatically taking action on important events (#877)

●- New NodeAttestor based on SSH certificates (#868, #870)

●- v2 client library for Workload API interaction interaction (#841)

●- Back-compat bundle management code removed - bundle is now handled correctly (#858, #859)

●- Plugins can now expose auxiliary services and consume host-based services (#840)

●- Fix bug preventing agent recovery prior to its first SVID rotation (#839)

●- Agent and Server can now export telemetry to Prometheus, Statsd, DogStatsd (#817)

●- Fix bug in SDS API that prevented updates following Envoy restart (#820)

●- Kubernetes workload attestor now supports using the secure port (#814)

●- Support for TLS-protected connections to MySQL (#821)

●- X509-SVID can now include an optional CN/DNS SAN (#798)

●- SQL DataStore plugin now supports MySQL (#784)

●- Fix bug preventing agent from reconnecting to a new server after an error (#795)

●- Fix bug preventing agent from shutting down when streams are open (#790)

●- Registration entries can now have an expiry and be pruned automatically (#776, #793)

●- New Kubernetes NodeAttestor based on PSAT for node specificity (#771, #860)

●- New UpstreamCA plugin for AWS secret manager (#751)

●- Healthcheck commands exposed in Server and Agent (#758, #763)

●- Kubernetes workload attestor extended with additional selectors (#720)

●- UpstreamCA "disk" now supports loading multiple key types (#717)

SCYTALE

- **Fix a bug in which the agent periodically logged connection errors (#906)**
- Kubernetes SAT node attestor now supports the TokenReview API (#904)
- Agent cache refactored to improve memory management and fix a leak (#863)
- **UpstreamCA "disk" will now reload cert and keys when needed (#903)**
- **Introduced Nested SPIRE: server clusters can now be chained together (#890)**
- **Fix a bug in AWS IID NodeResolver with instance profile lookup (888)**
- Improved workload attestation and fixed a security bug related to PID reuse (#886)
- New Kubernetes bundle notifier for keeping a bundle configmap up-to-date (#877)
- New plugin type Notifier for programatically taking action on important events (#877)
- **New NodeAttestor based on SSH certificates (#868, #870)**
- **v2 client library for Workload API interaction interaction (#841)**
- Back-compat bundle management code removed - bundle is now handled correctly (#858, #859)
- Plugins can now expose auxiliary services and consume host-based services (#840)
- Fix bug preventing agent recovery prior to its first SVID rotation (#839)
- Agent and Server can now export telemetry to Prometheus, Statsd, DogStatsd (#817)
- **Fix bug in SDS API that prevented updates following Envoy restart (#820)**
- Kubernetes workload attestor now supports using the secure port (#814)
- **Support for TLS-protected connections to MySQL (#821)**
- **X509-SVID can now include an optional CN/DNS SAN (#798)**
- **SQL DataStore plugin now supports MySQL (#784)**
- Fix bug preventing agent from reconnecting to a new server after an error (#795)
- Fix bug preventing agent from shutting down when streams are open (#790)
- **Registration entries can now have an expiry and be pruned automatically (#776, #793)**
- New Kubernetes NodeAttestor based on PSAT for node specificity (#771, #860)
- **New UpstreamCA plugin for AWS secret manager (#751)**
- Healthcheck commands exposed in Server and Agent (#758, #763)
- Kubernetes workload attestor extended with additional selectors (#720)
- UpstreamCA "disk" now supports loading multiple key types (#717)

Try it out

spiffe/spiffe

spiffe/spire

slack.spiffe.io

Questions?

SCYTALE