SPIFFE/SPIRE Deep Dive

Emiliano Berenbaum

Agenda

- SPIFFE Overview
- SPIRE Plugin Walkthrough
- Node and Workload Attestation
- Neel Shah's presentation
- Questions?

SPIFFE

- SPIFFE ID
- SPIFFE IDENTITY Document
- Workload API

SPIFFE ID

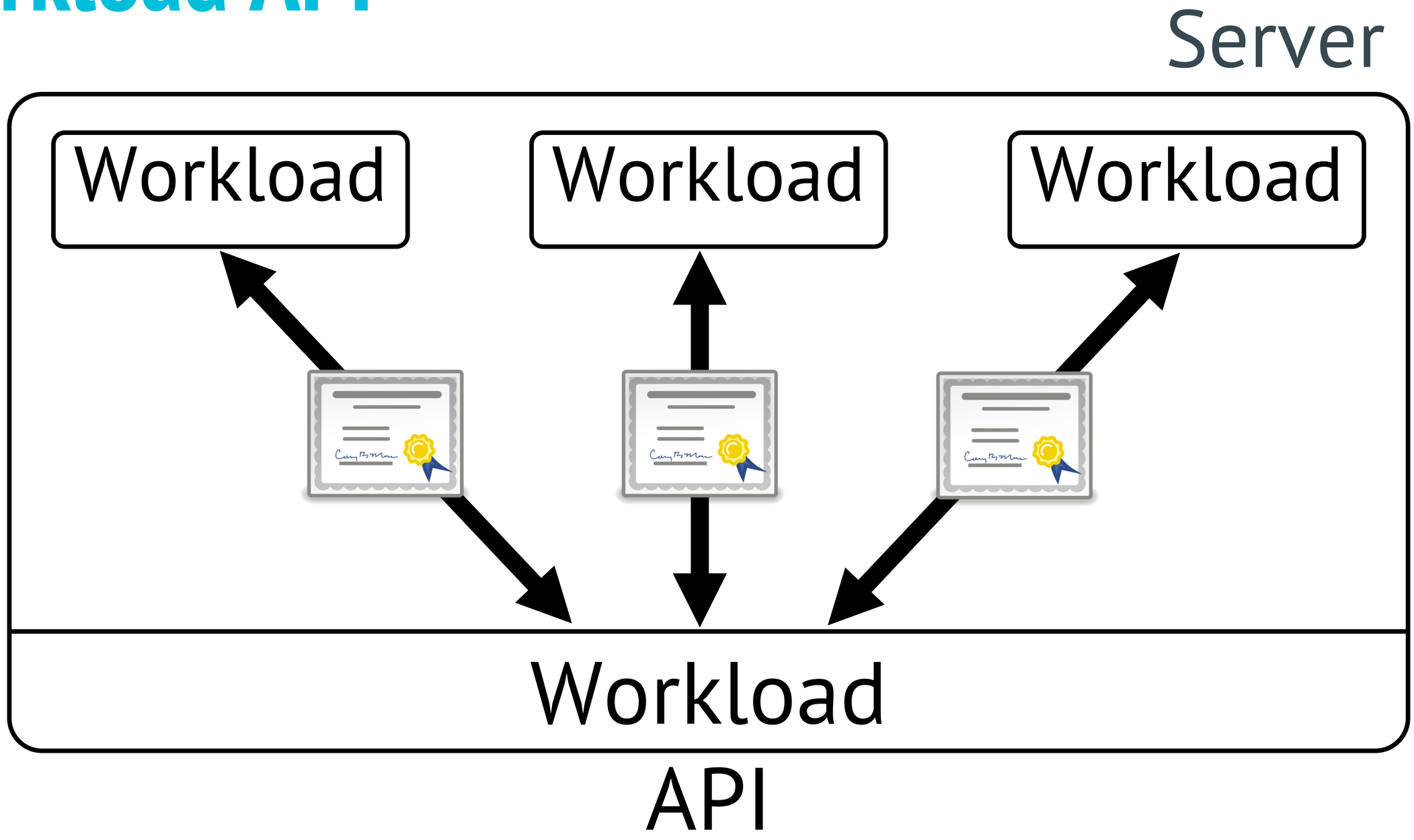
spiffe://example.org/foo

SVID: SPIFFE Verifiable Identity Document

spiffe://example.org/foo

SCYTALE

Workload API



SCYTALE

SPIRE

SPIRE

- SPIFFE Runtime Environment

SPIRE

spire-server

- Identity Mapping
- Node Attestation
- SVID Issuance

spire-agent

- Workload Attestation
- Workload API

SPIRE Server Plugins

Node Attestor

SPIRE Server Plugins

Node Attestor

Node Resolver

SPIRE Server Plugins

Node Attestor

Node Resolver

CA

SPIRE Server Plugins

Node Attestor

Node Resolver

CA

Upstream CA

SPIRE Server Plugins

Node Attestor
Node Resolver
CA
Upstream CA
Data Store

SPIRE Agent Plugins

Key Manager

SPIRE Agent Plugins

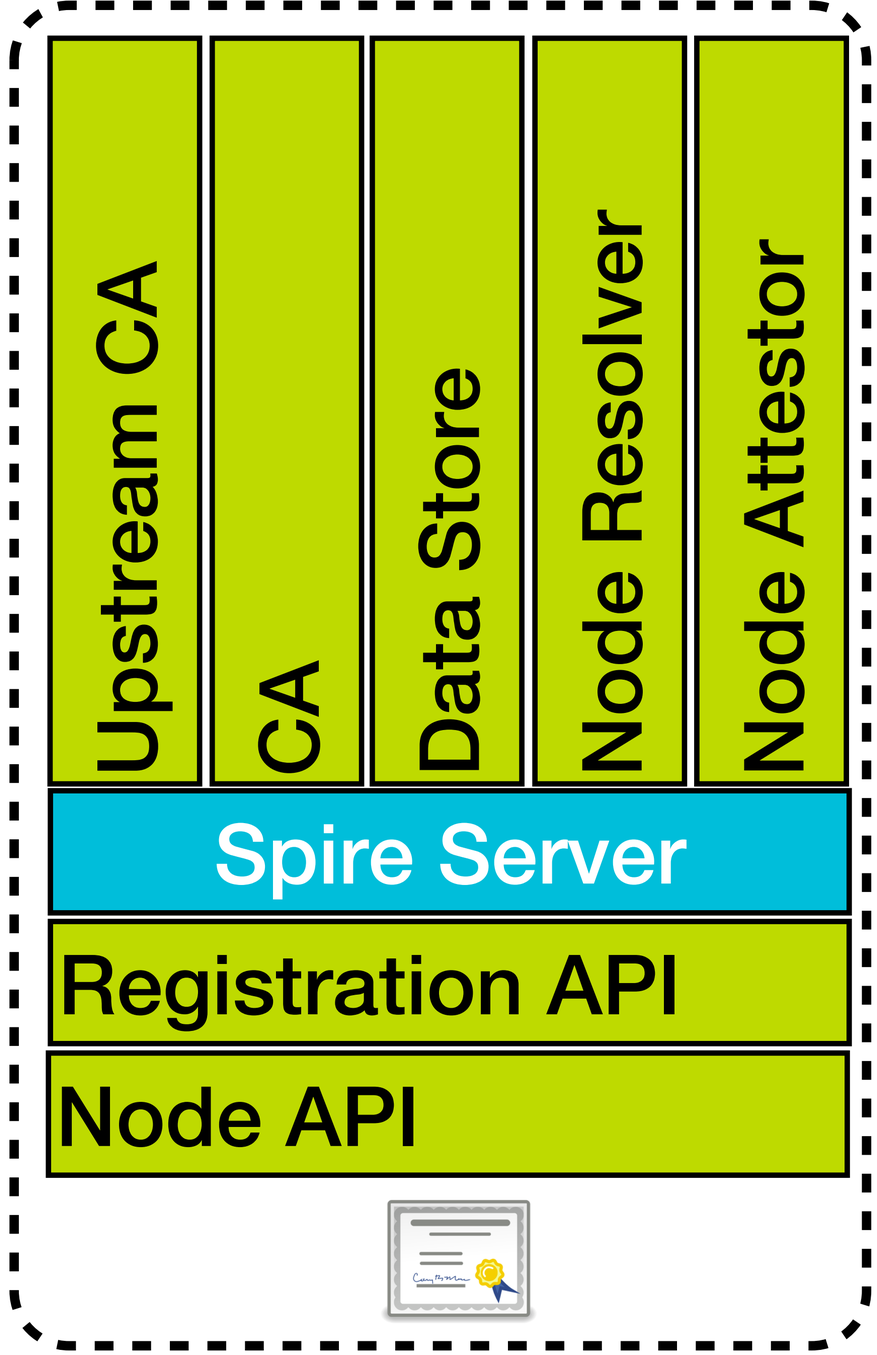
Key Manager
Node Attestor

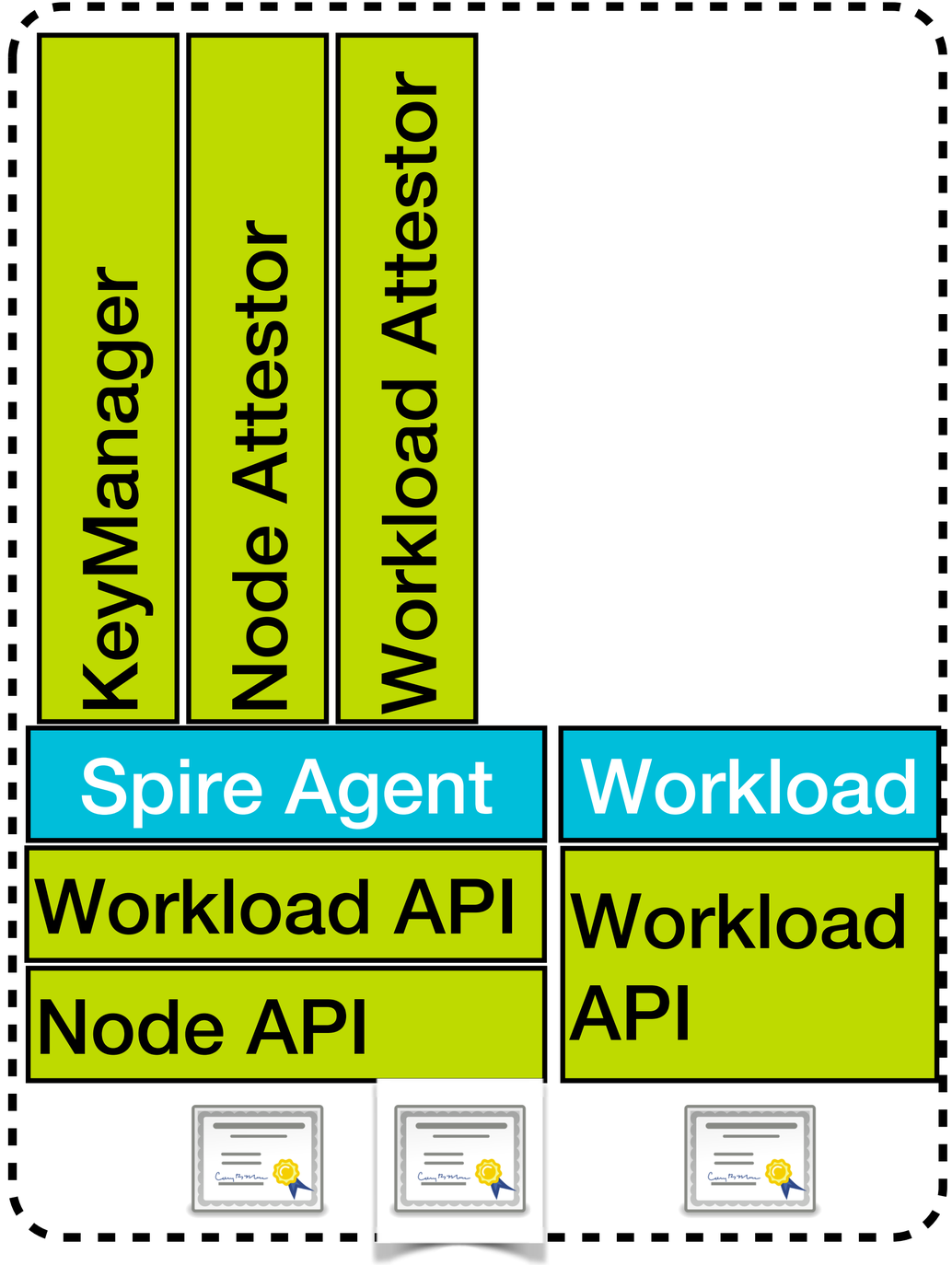
SPIRE Agent Plugins

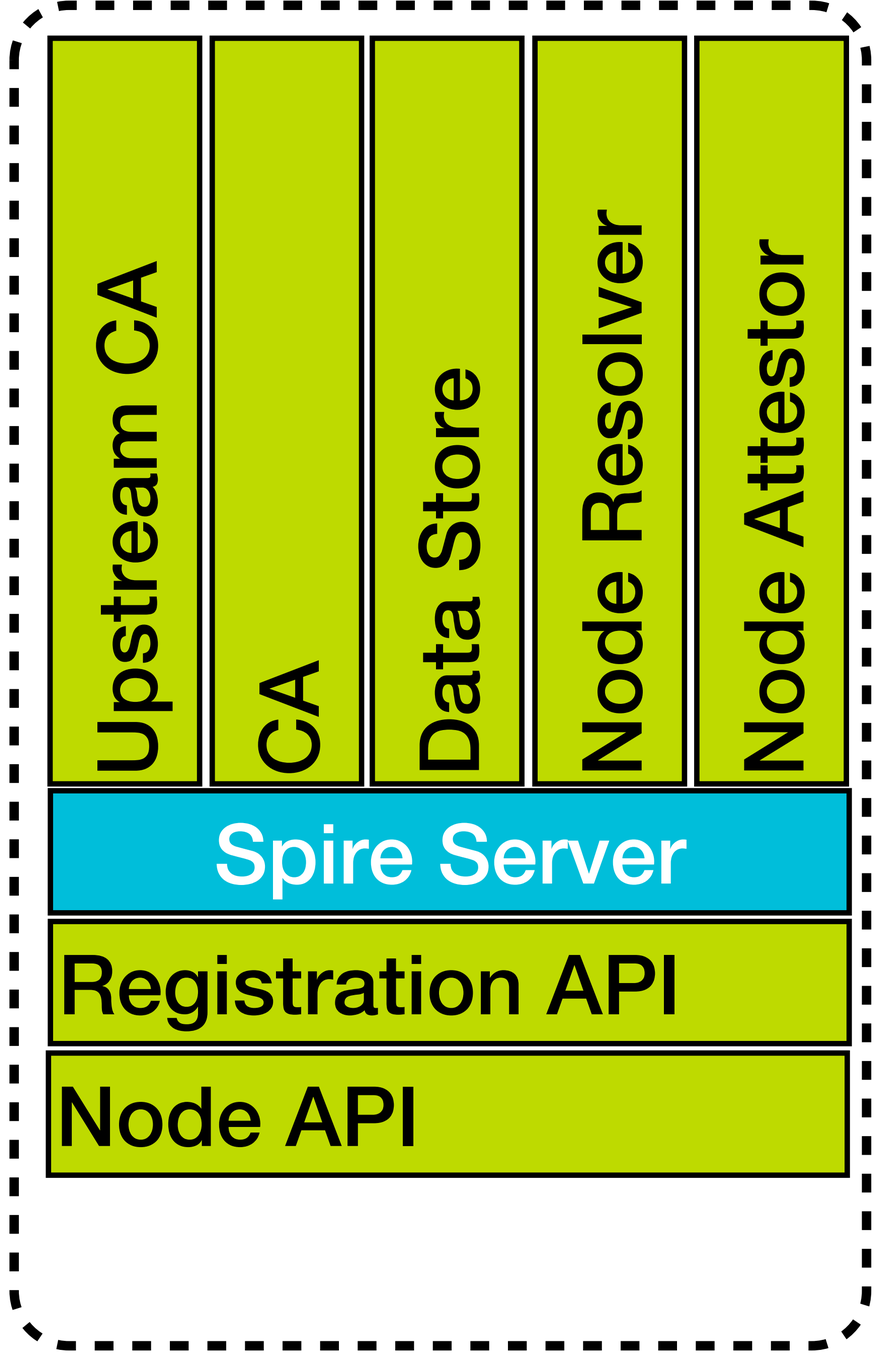
Key Manager
Node Attestor
Workload Attestor

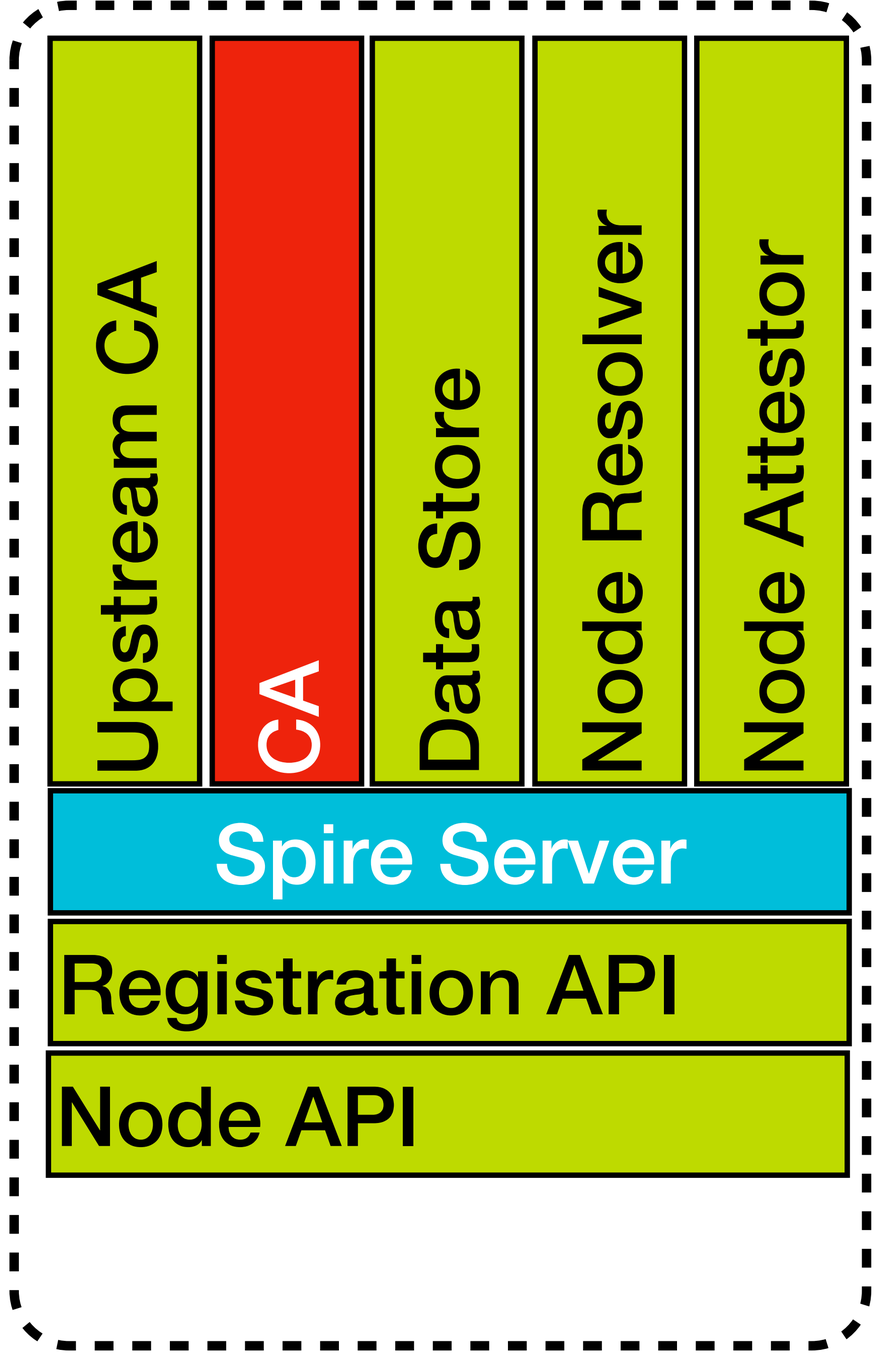
Node
Attestation

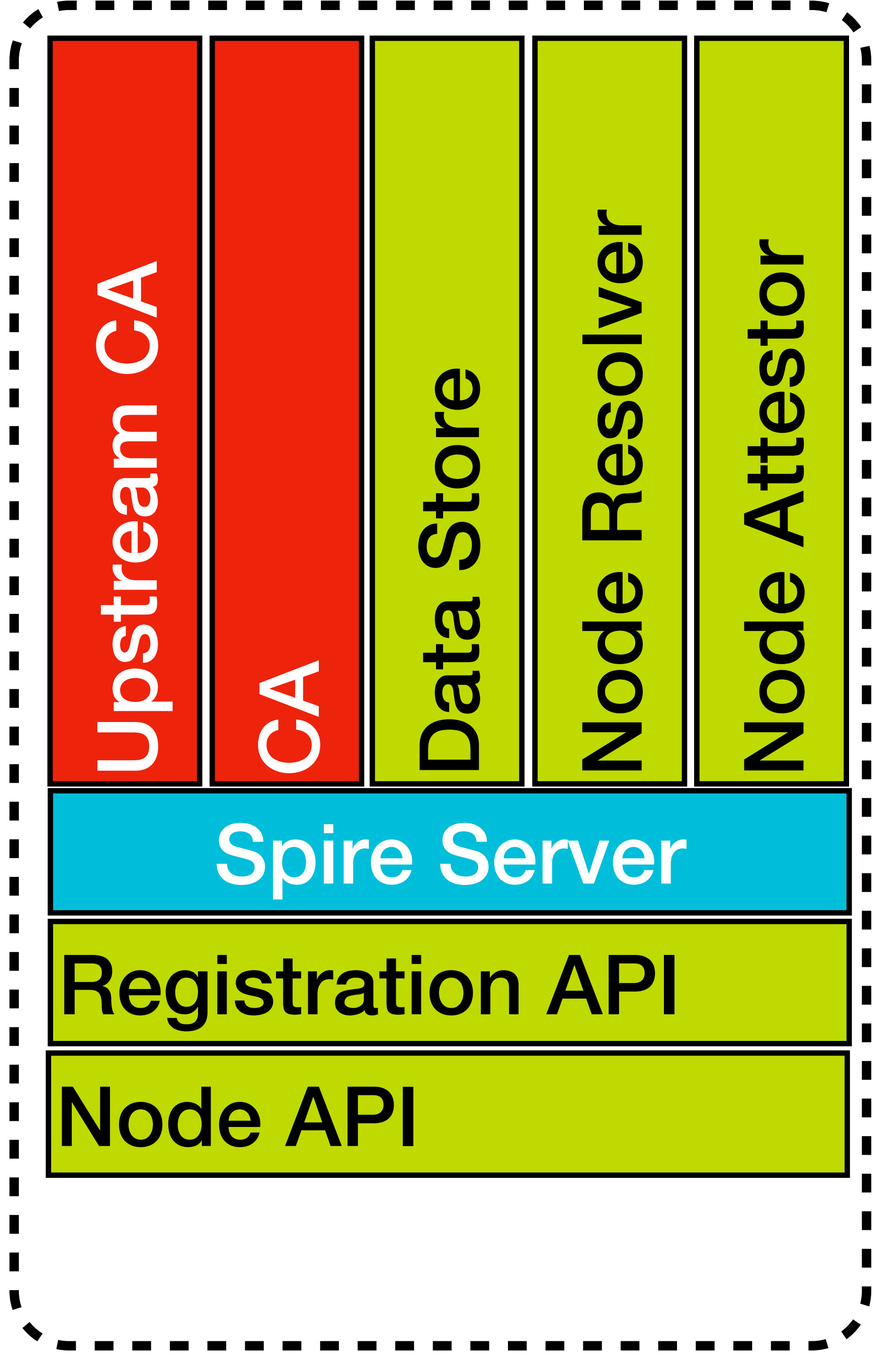
SCYTALE

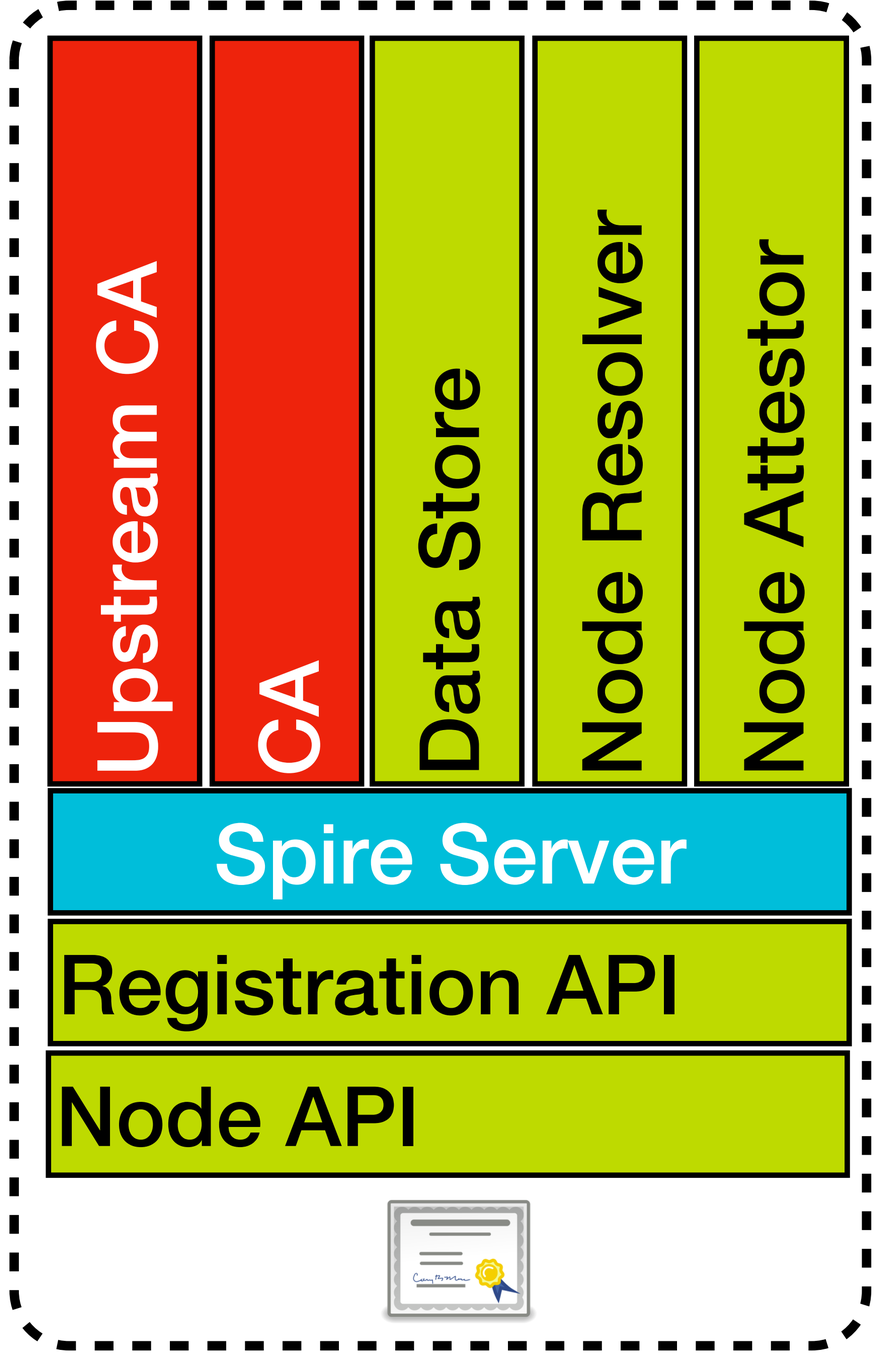

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

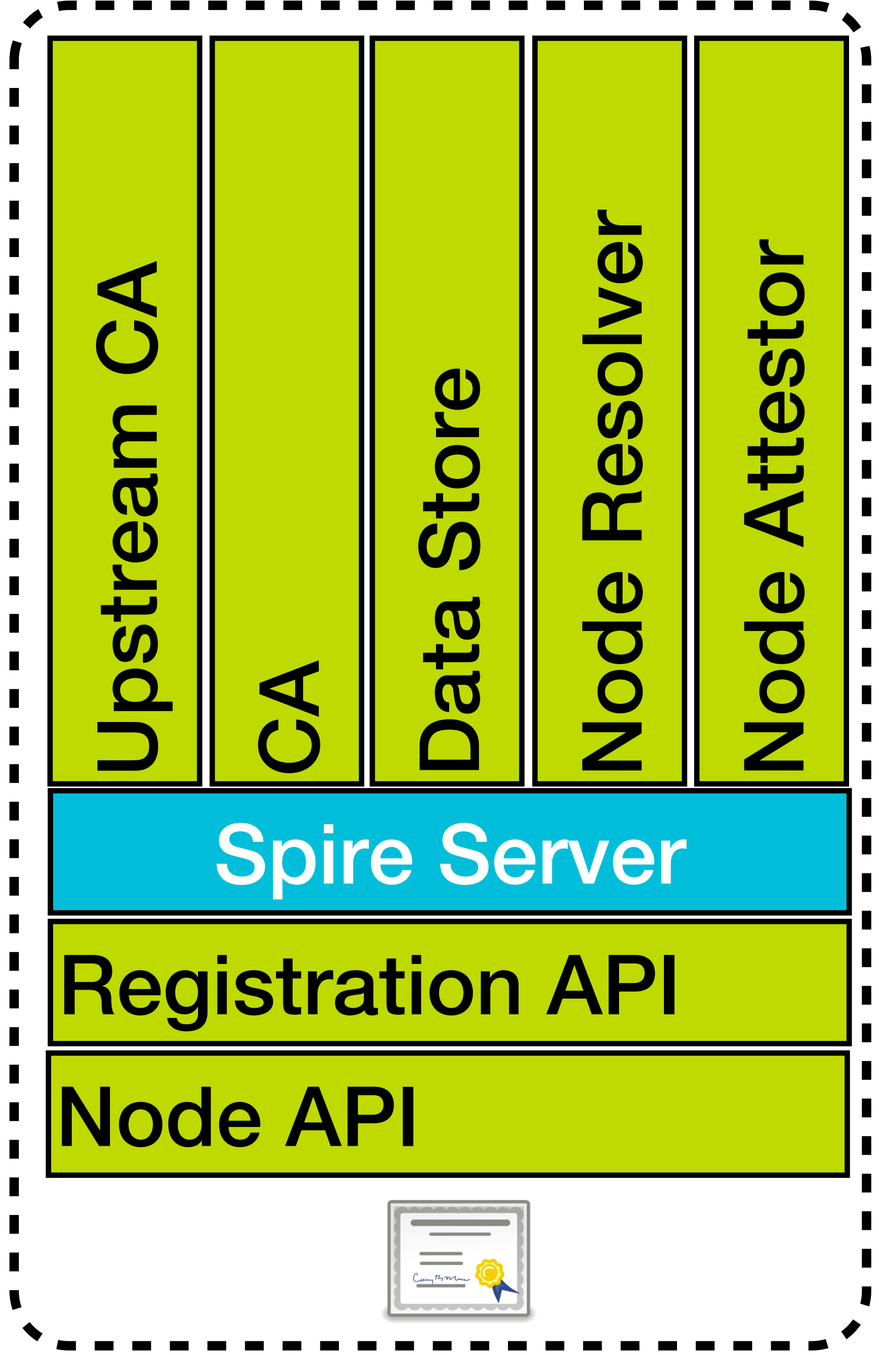

KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload
Workload API
Node API
Workload API

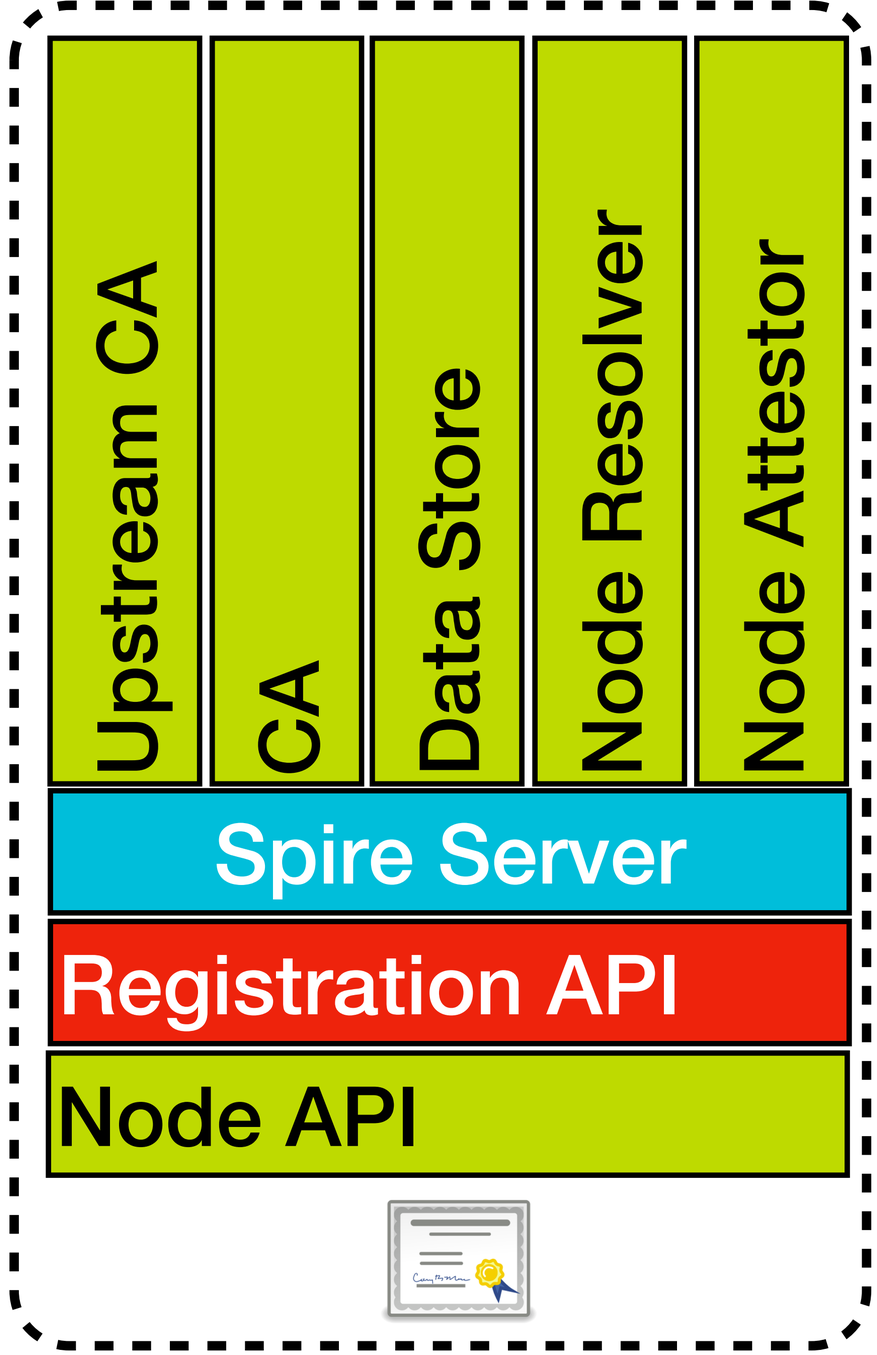

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

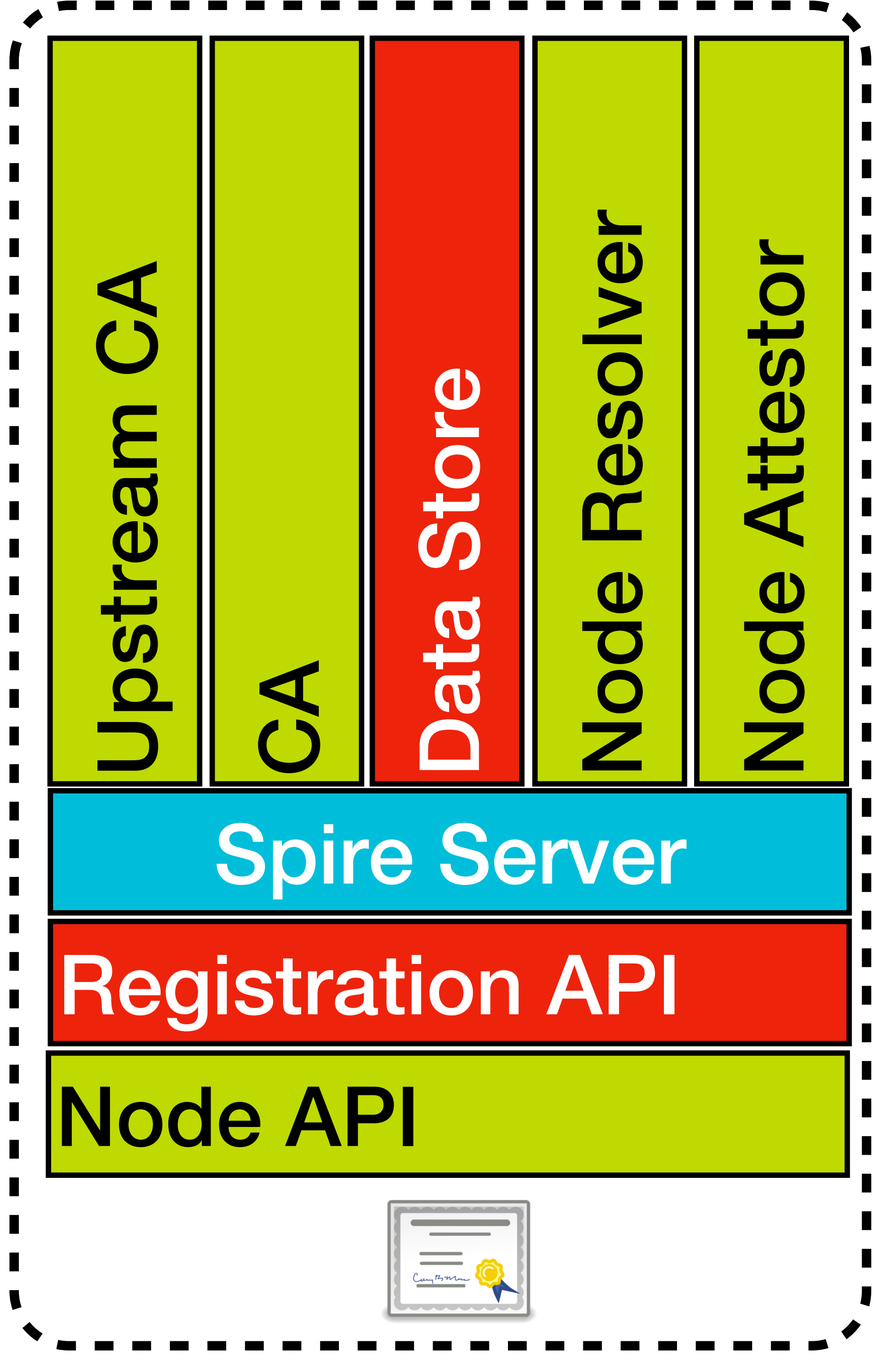

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

Node
Attestation

SCYTALE

Upstream CA

CA

Data Store

Node Resolver

Node Attestor

Spire Server

Registration API

Node API

KeyManager

Node Attestor

Workload Attestor

Spire Agent

Workload API

Node API

SCYTALE

Upstream CA

CA

Data Store

Node Resolver

Node Attestor

Spire Server

Registration API

Node API

KeyManager

Node Attestor

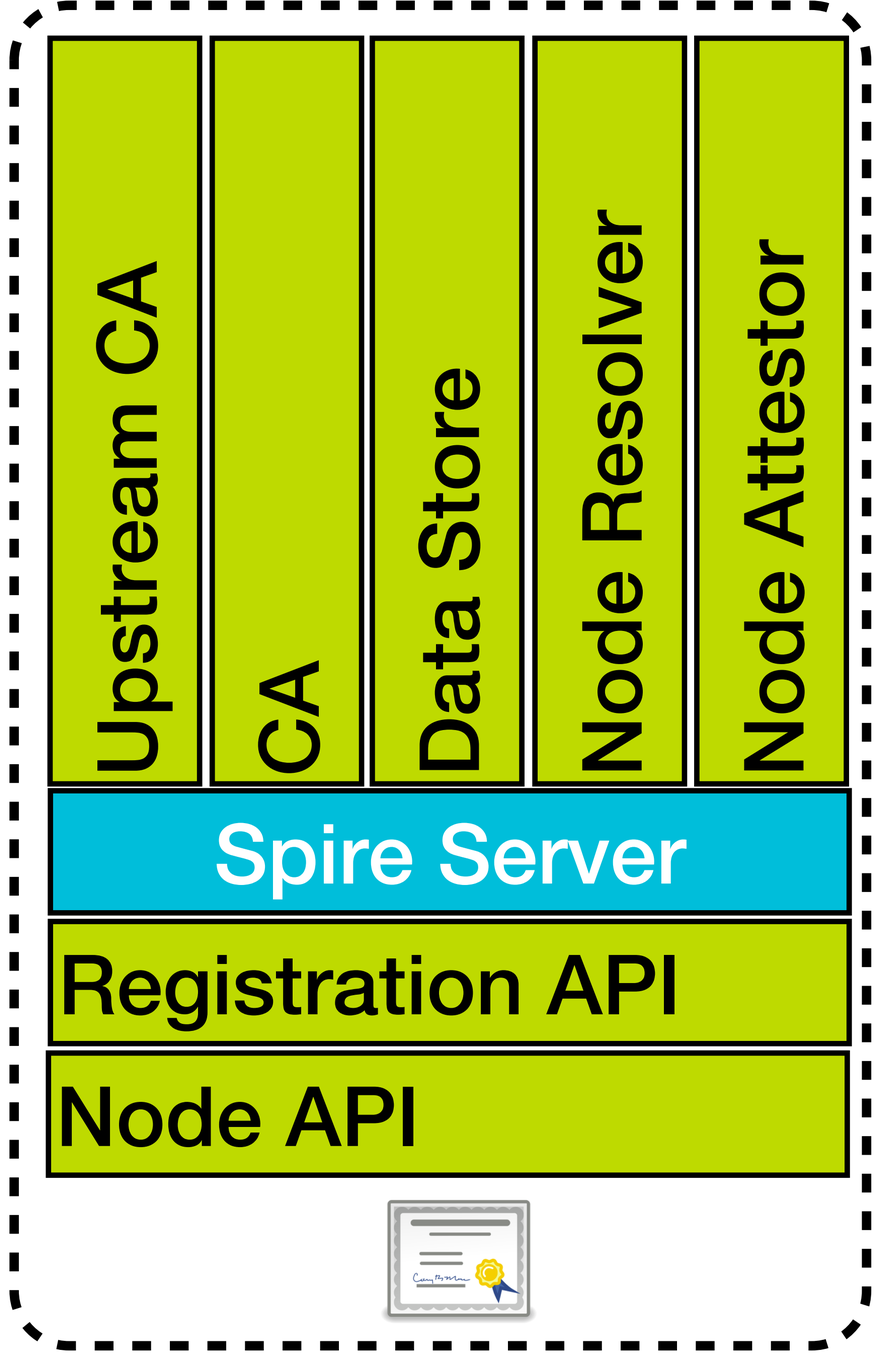
Workload Attestor

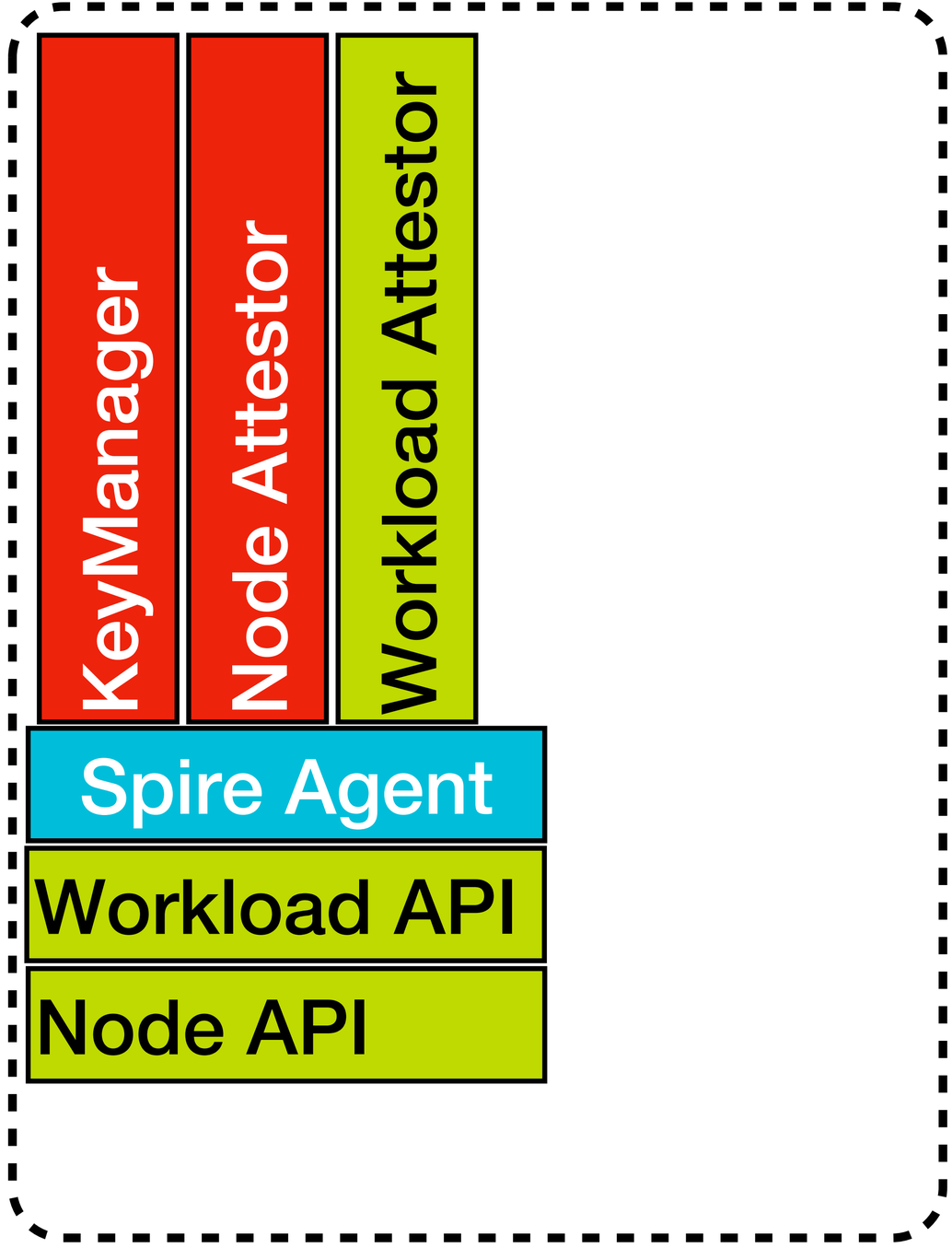
Spire Agent

Workload API

Node API

SCYTALE


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

SCYTALE

Upstream CA

CA

Data Store

Node Resolver

Node Attestor

Spire Server

Registration API

Node API

KeyManager

Node Attestor

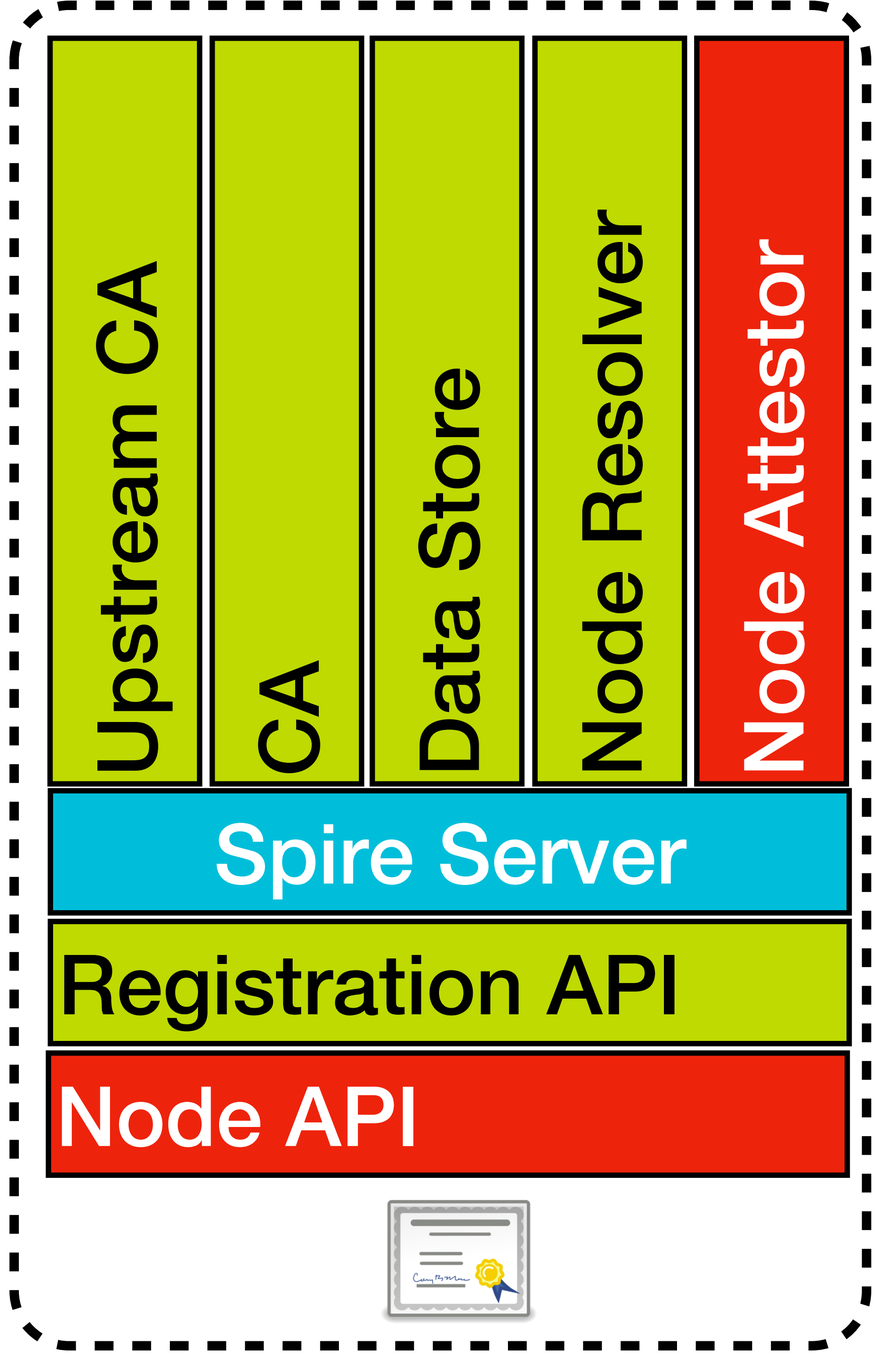
Workload Attestor

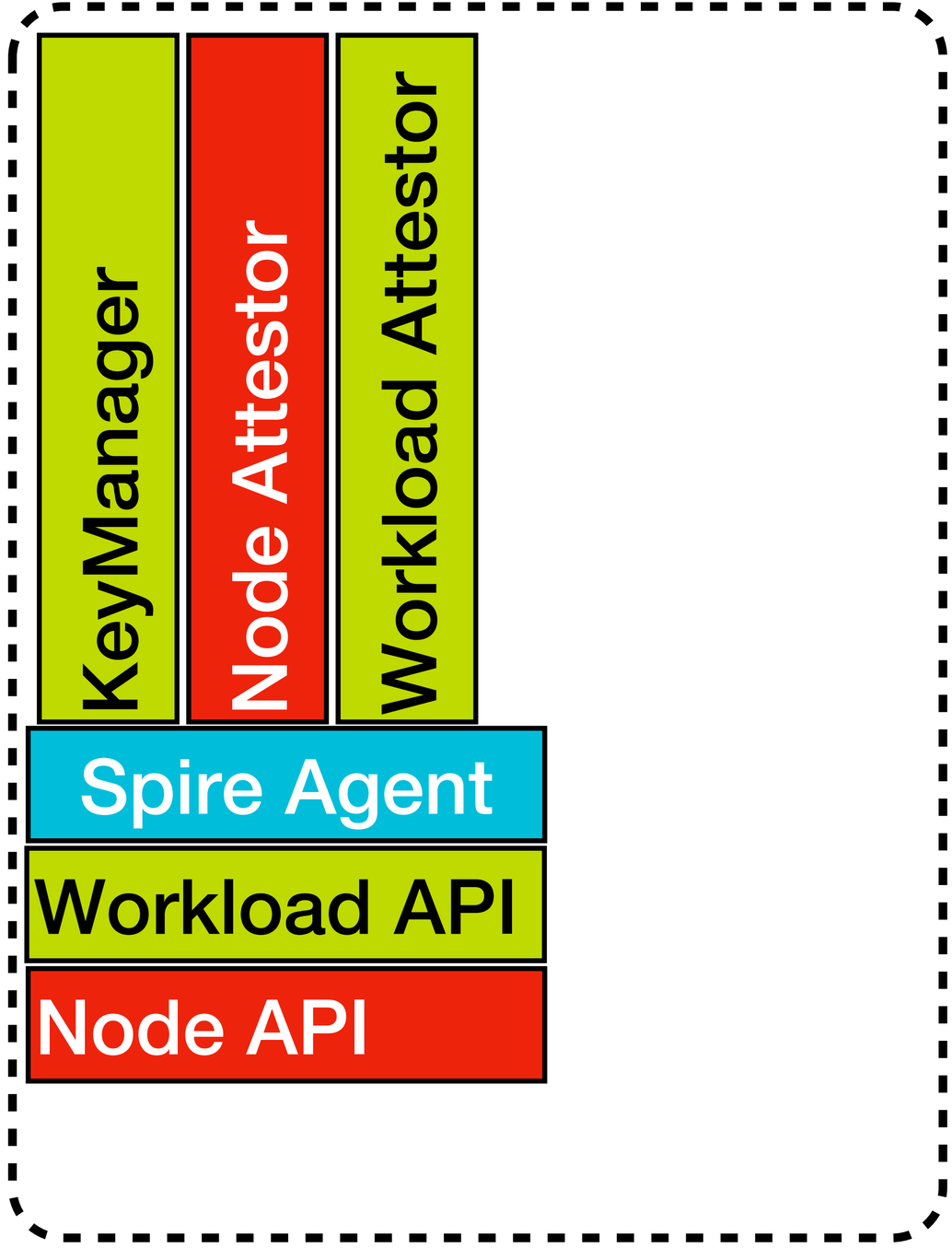
Spire Agent

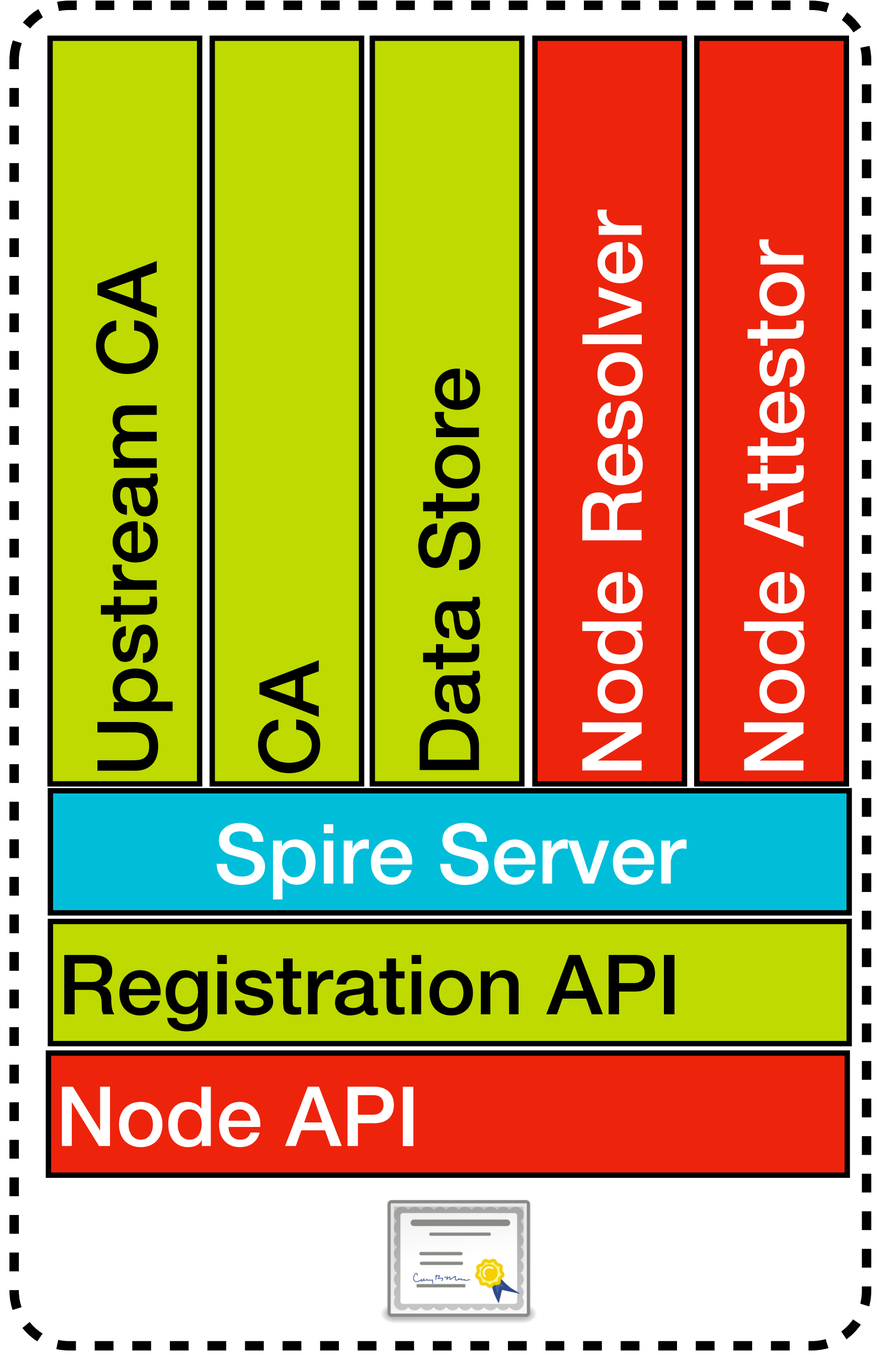
Workload API

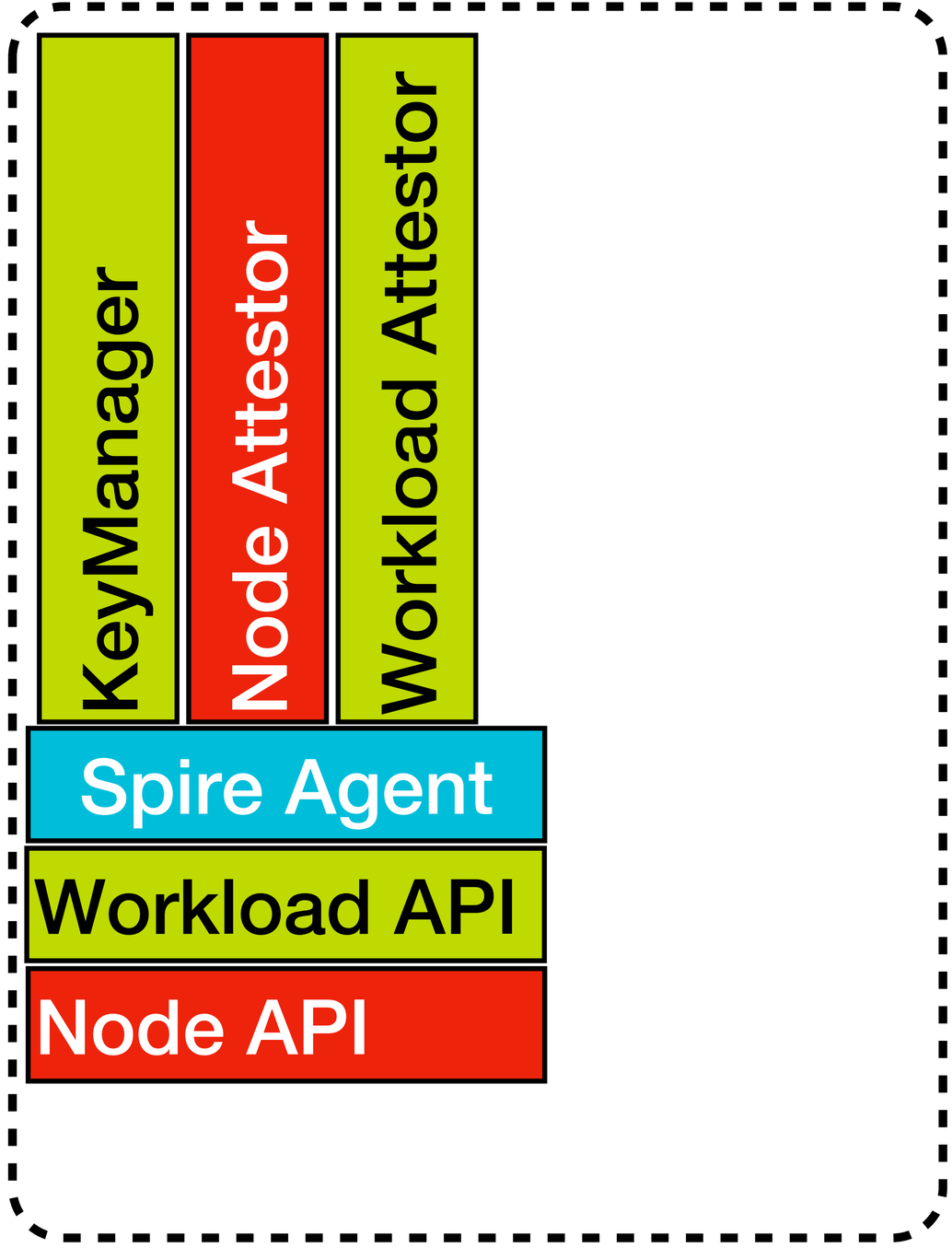
Node API

SCYTALE


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

SCYTALE

Upstream CA

CA

Data Store

Node Resolver

Node Attestor

Spire Server

Registration API

Node API

KeyManager

Node Attestor

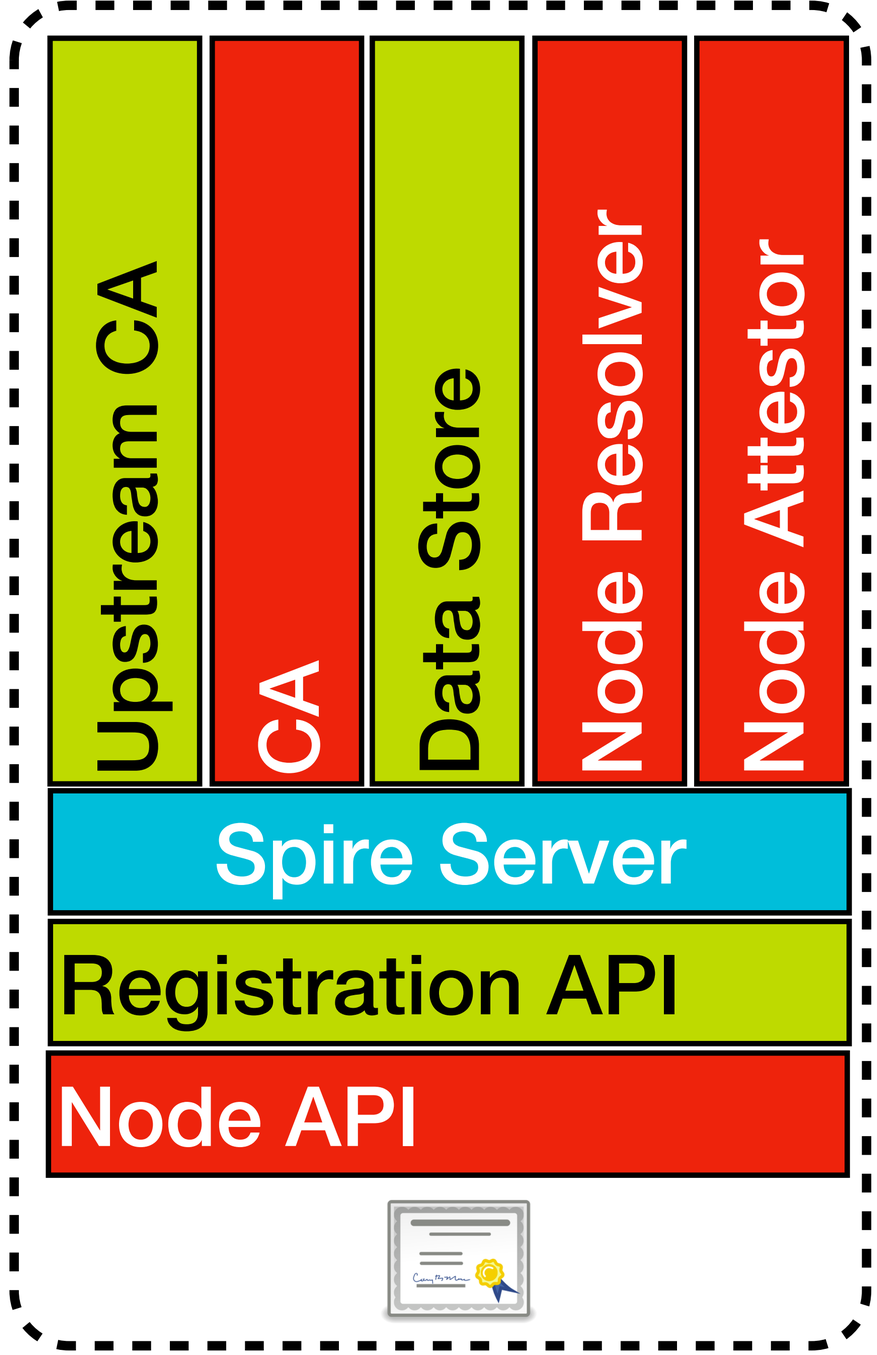
Workload Attestor

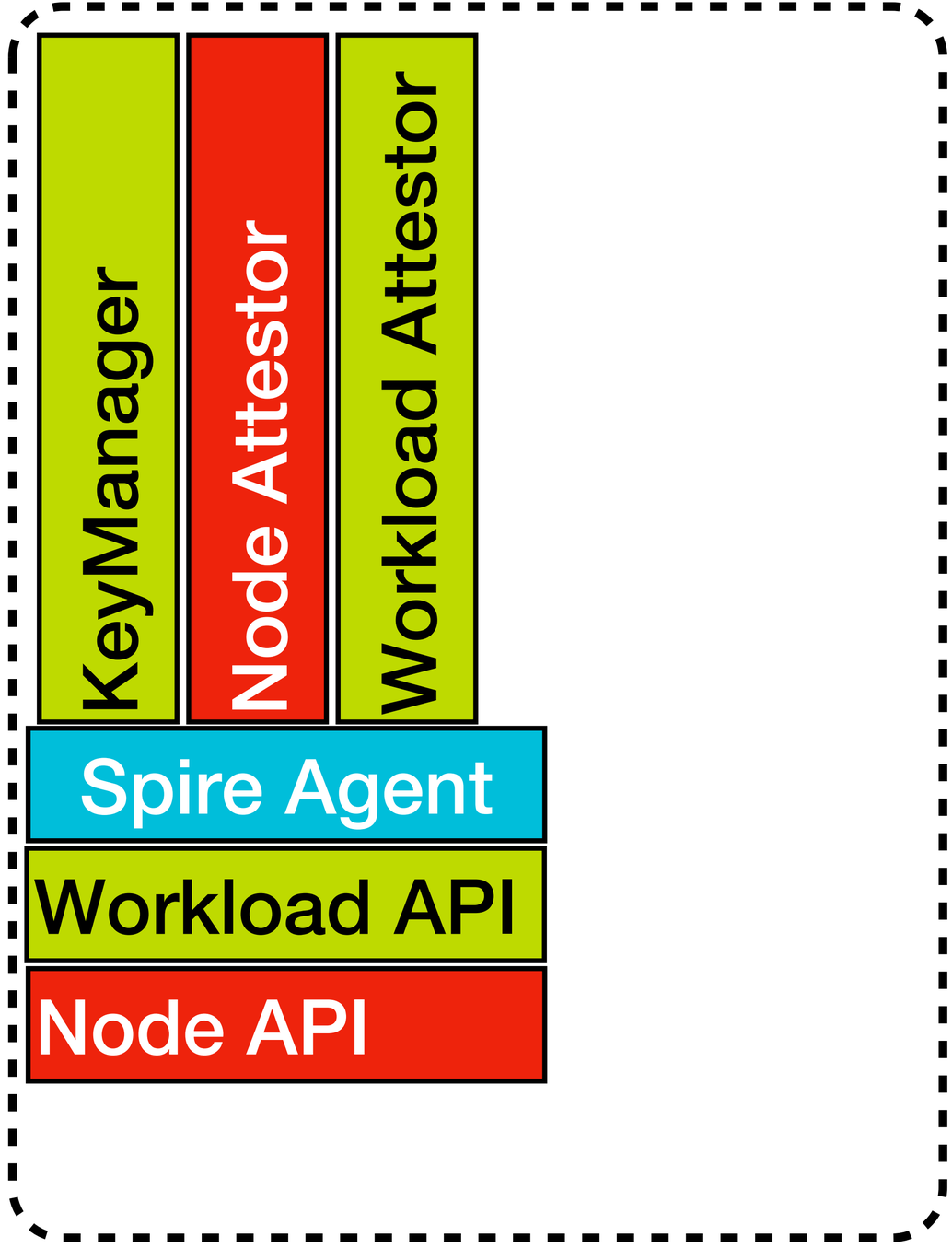
Spire Agent

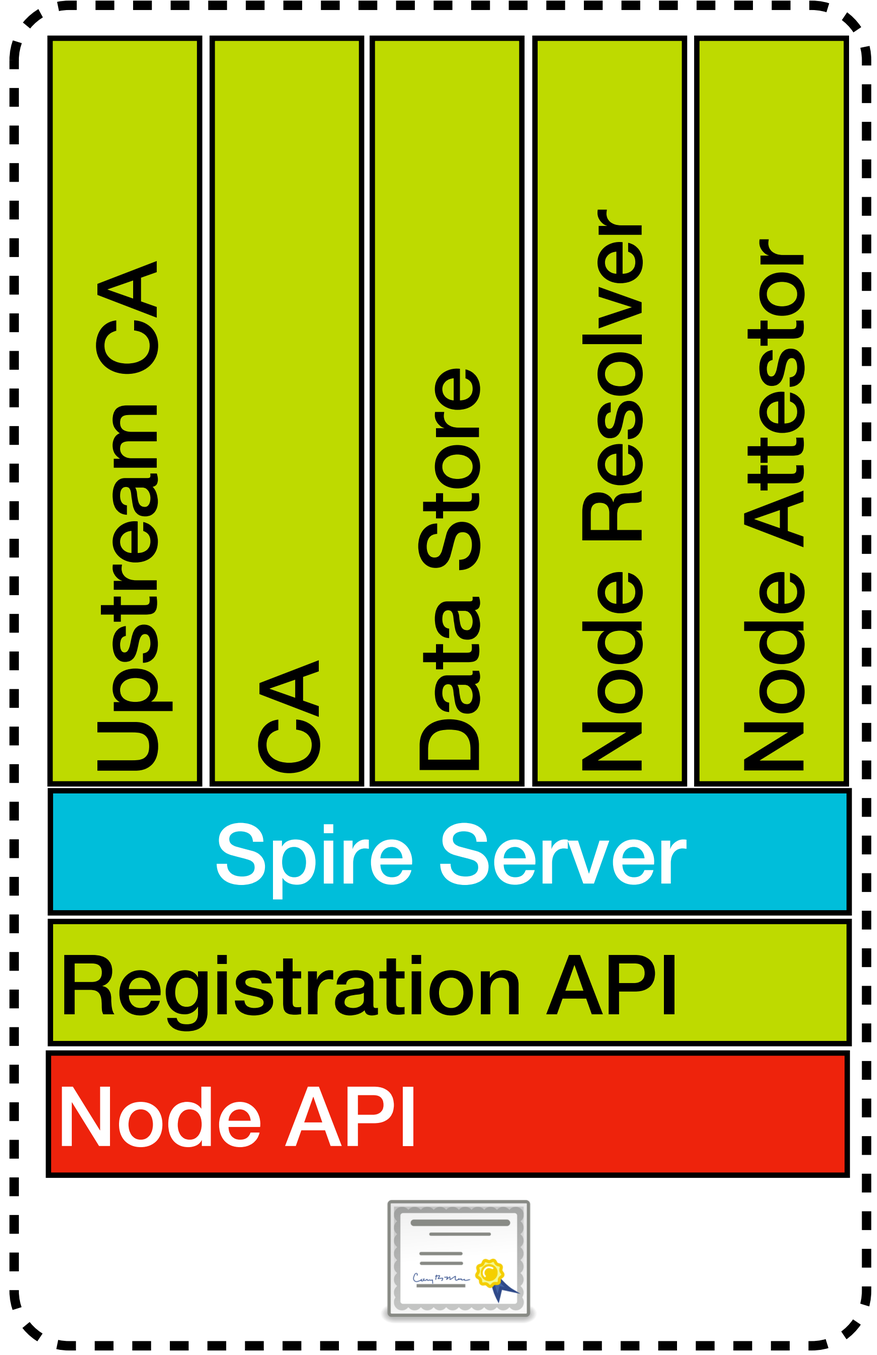
Workload API

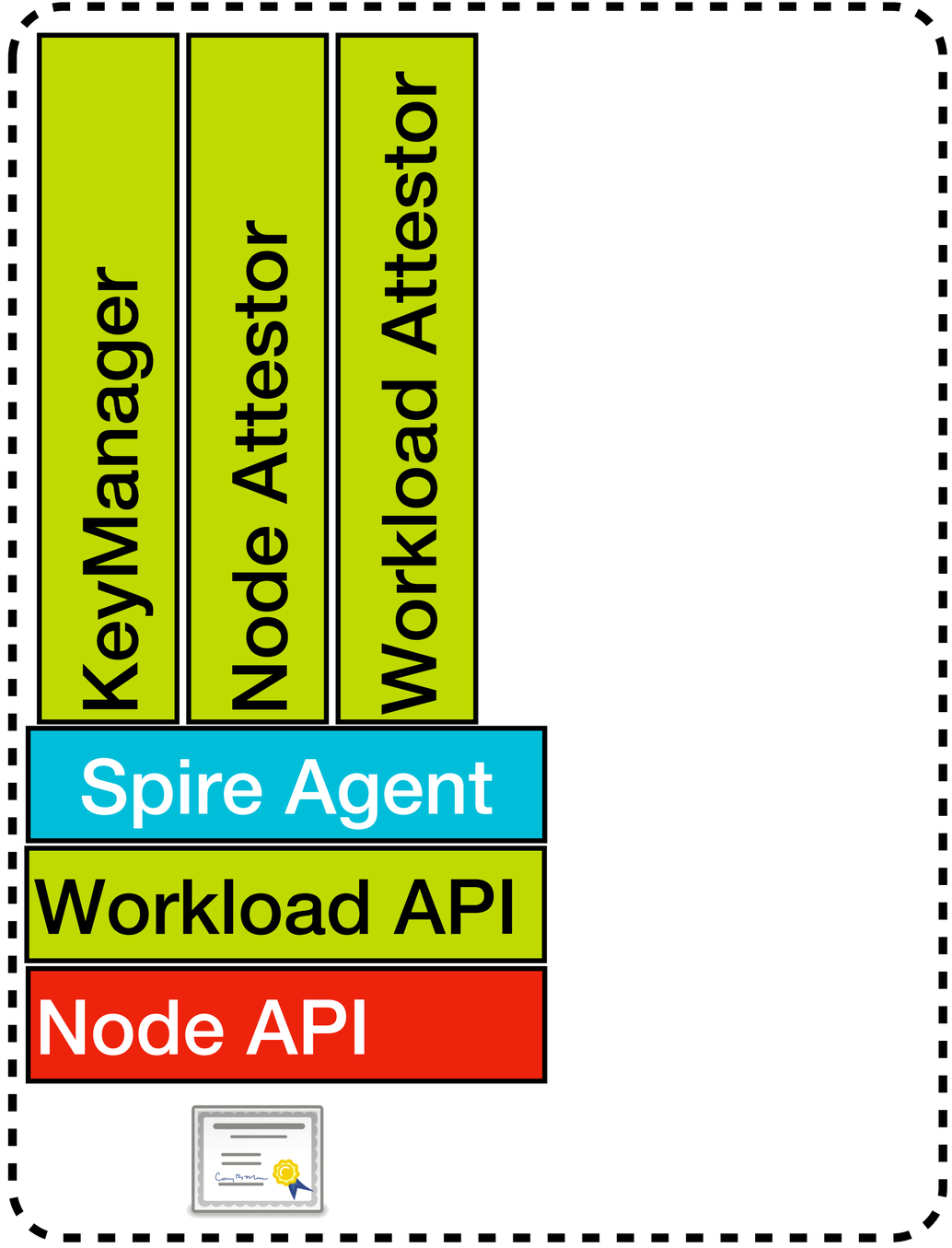
Node API

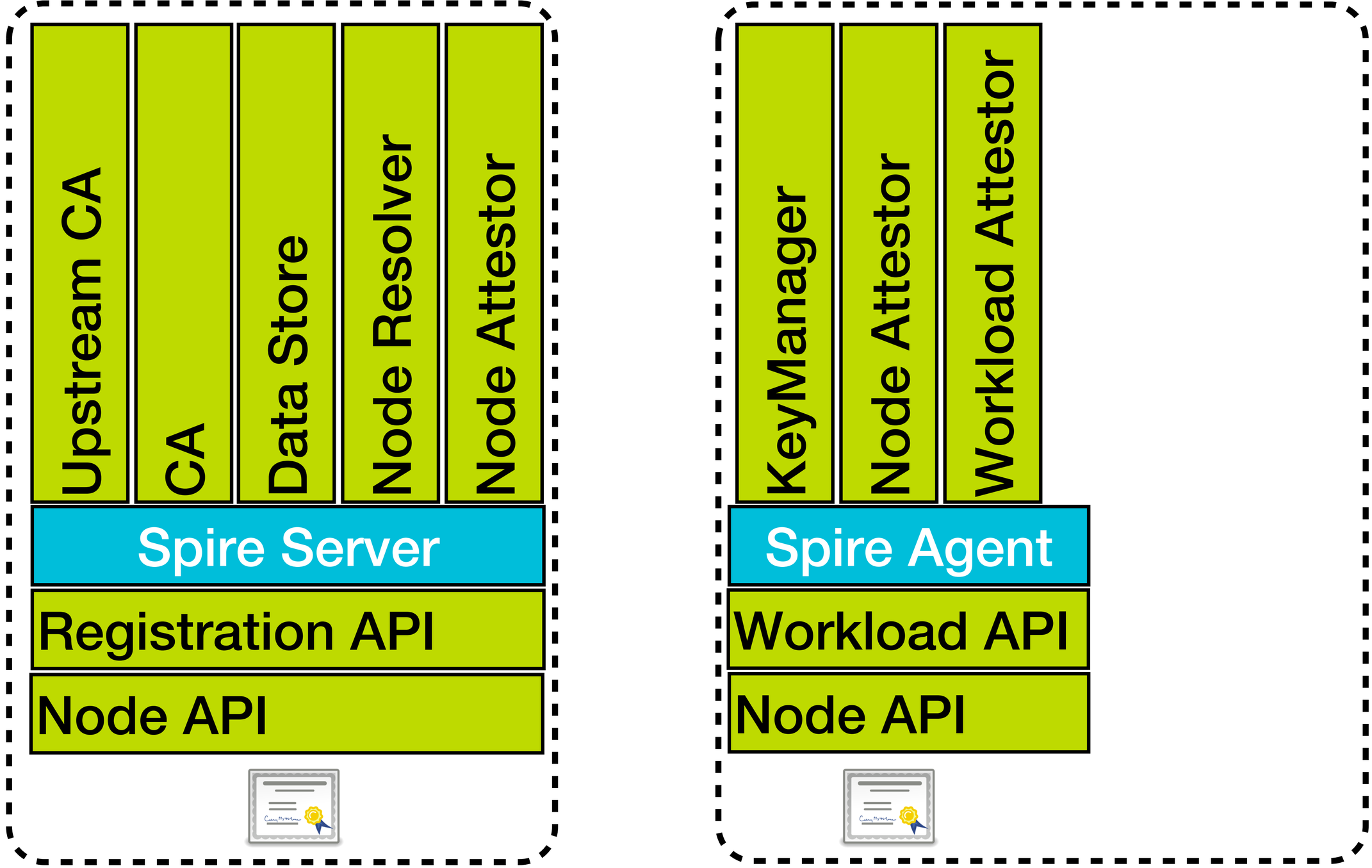
SCYTALE

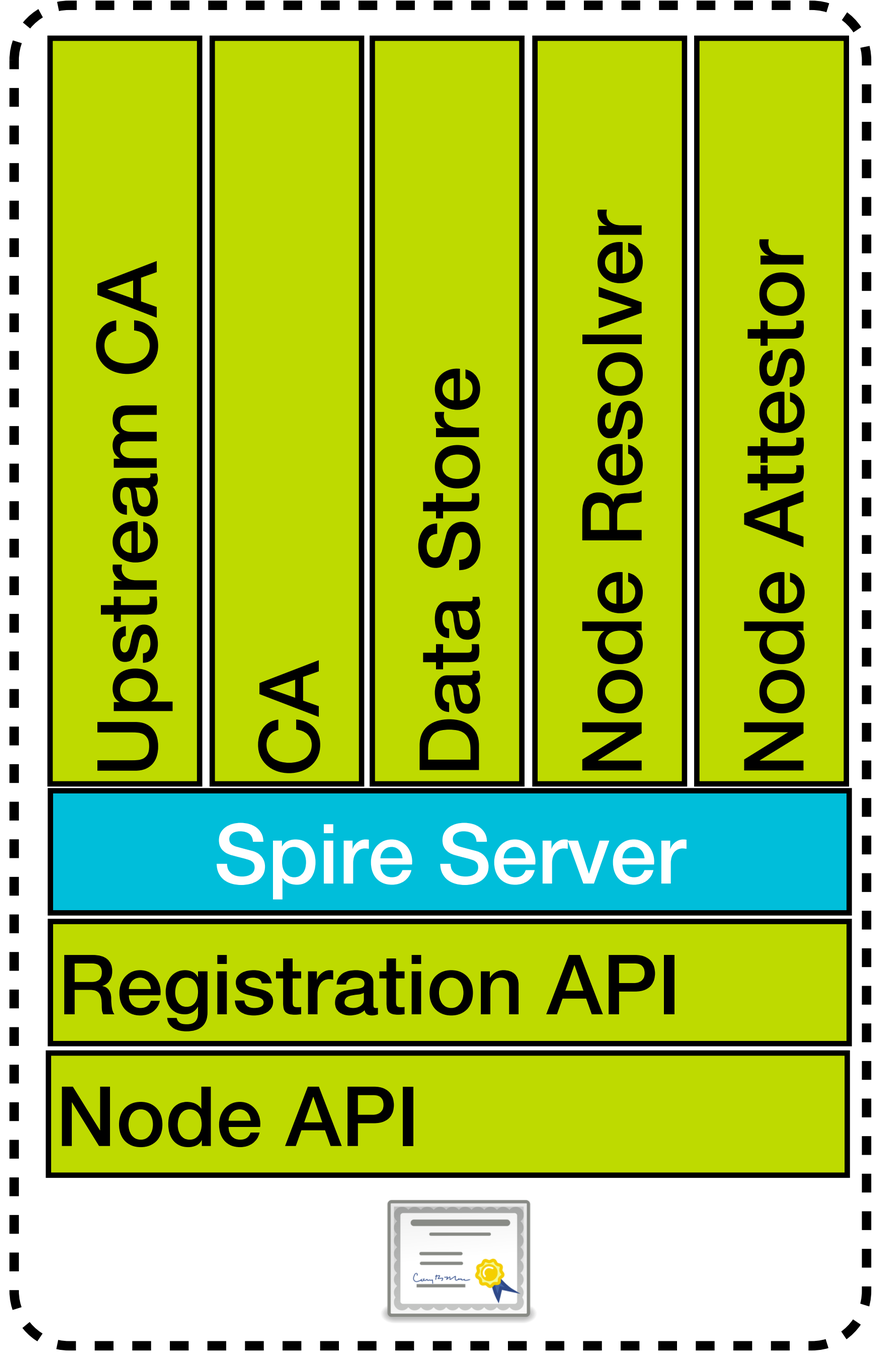

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

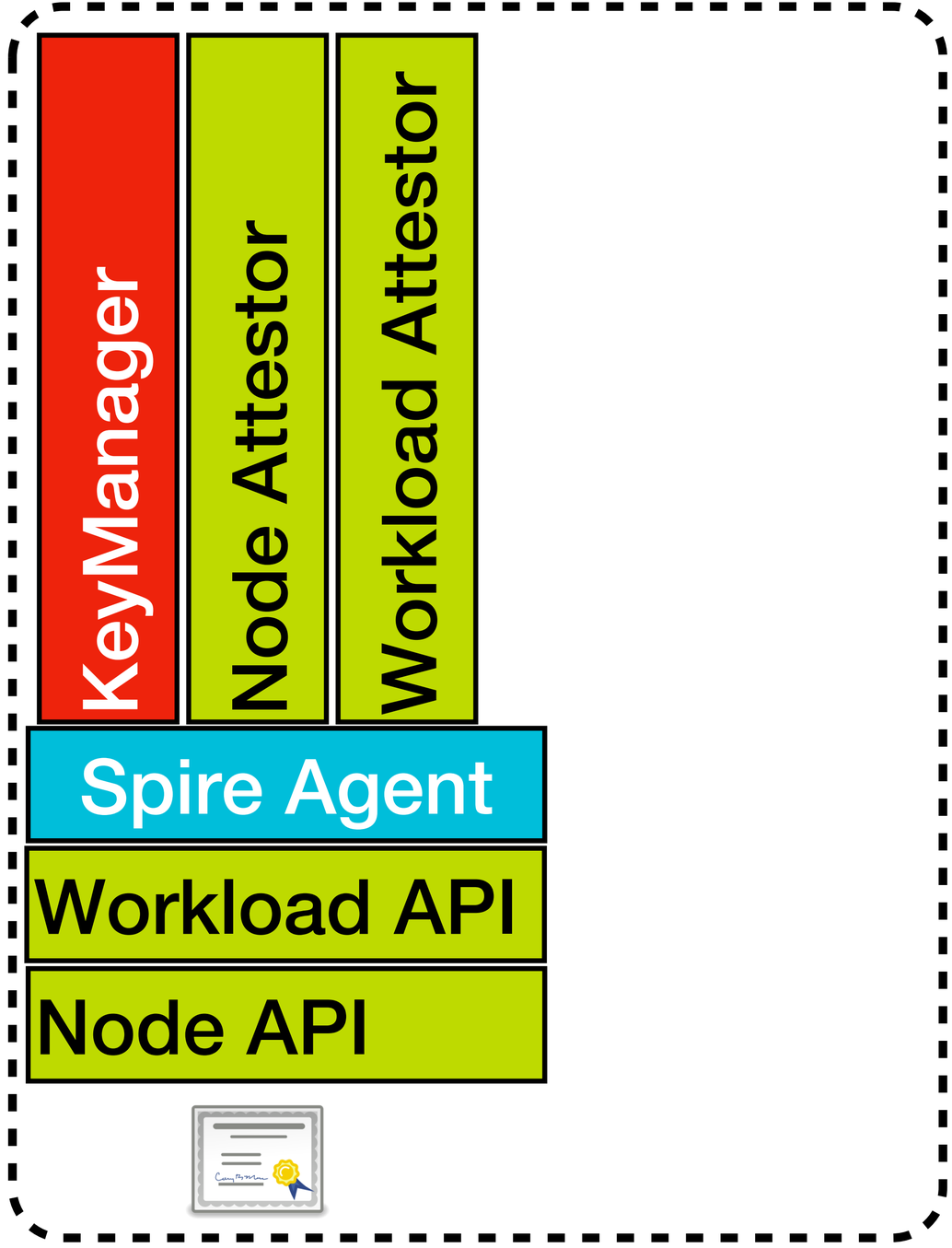

KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

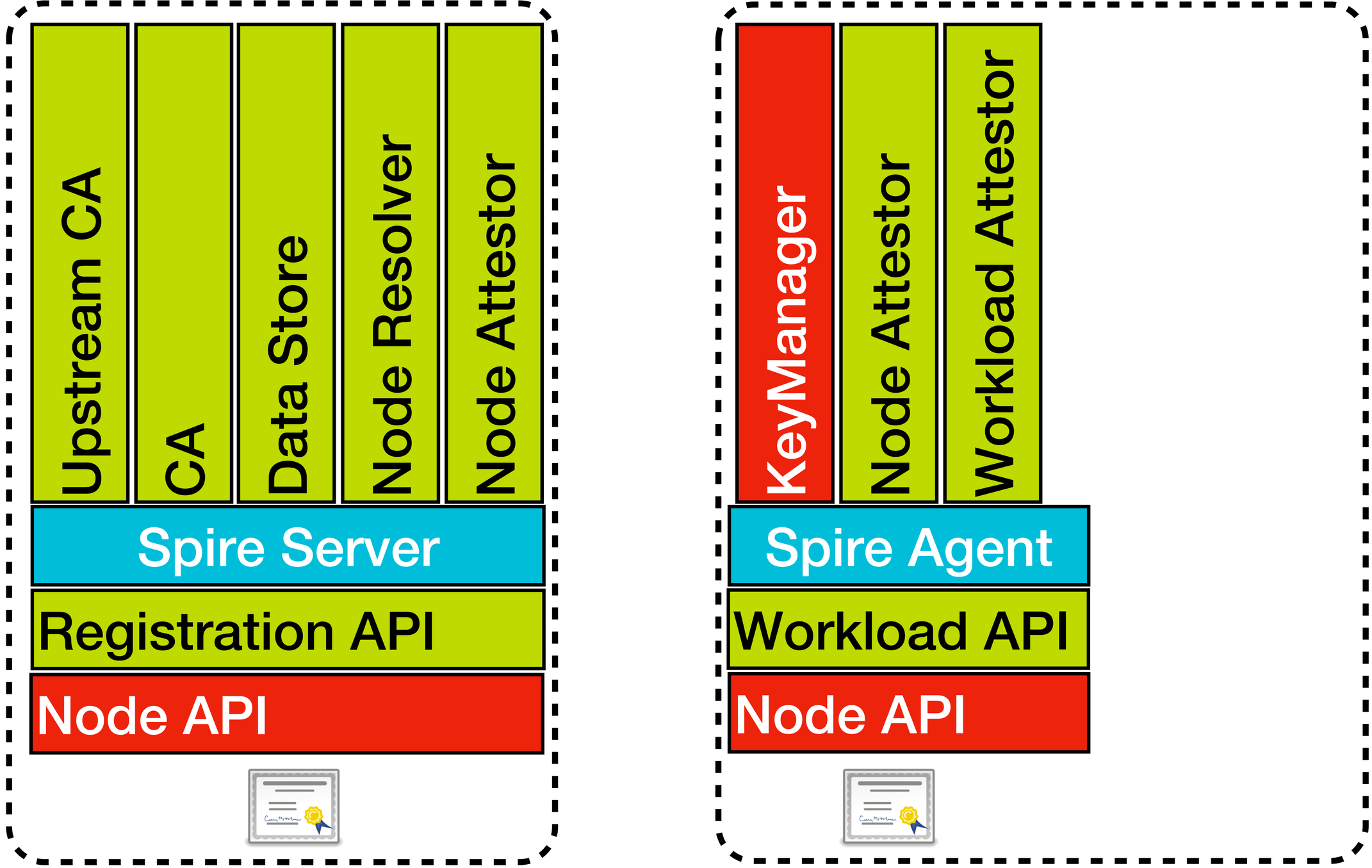

KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

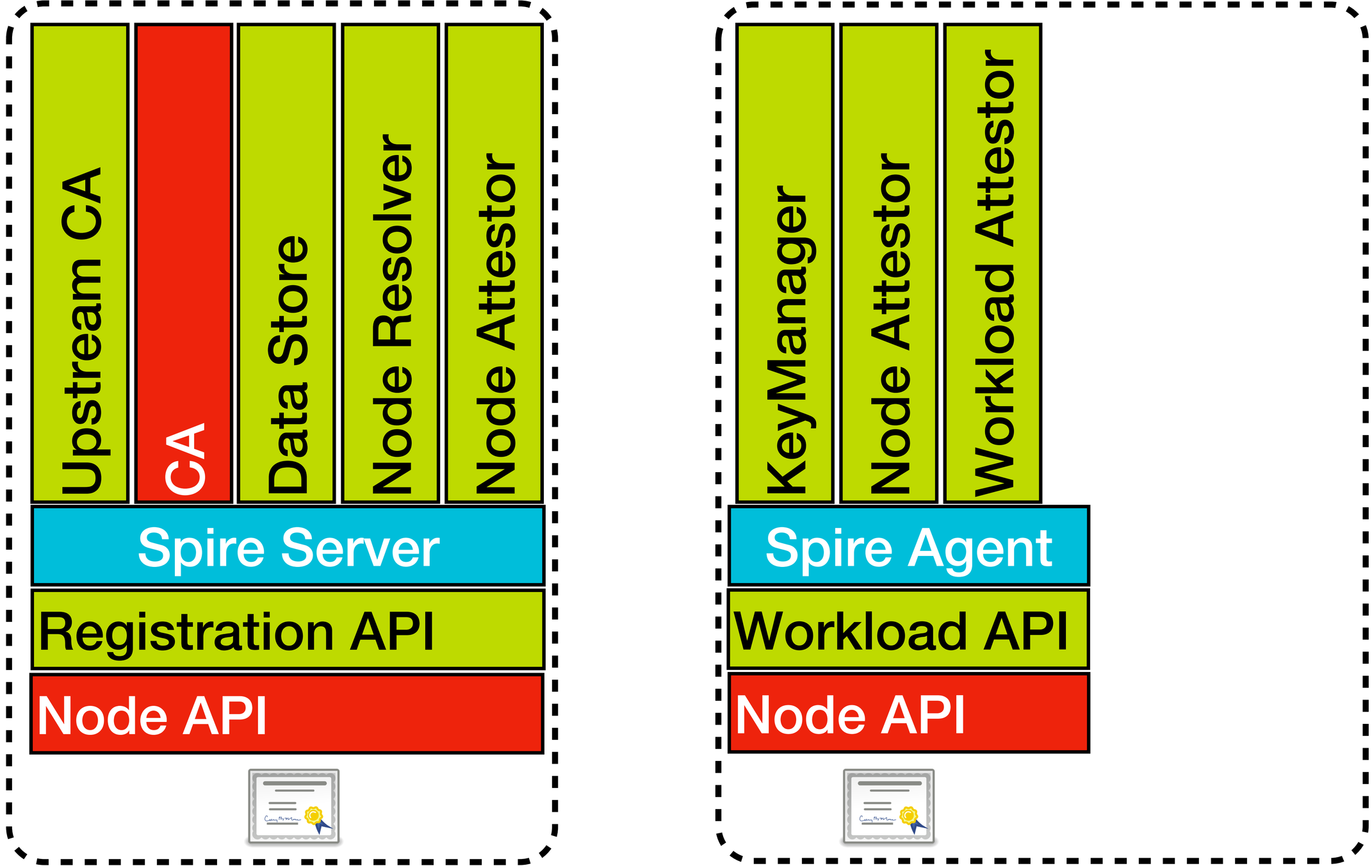

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API
KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

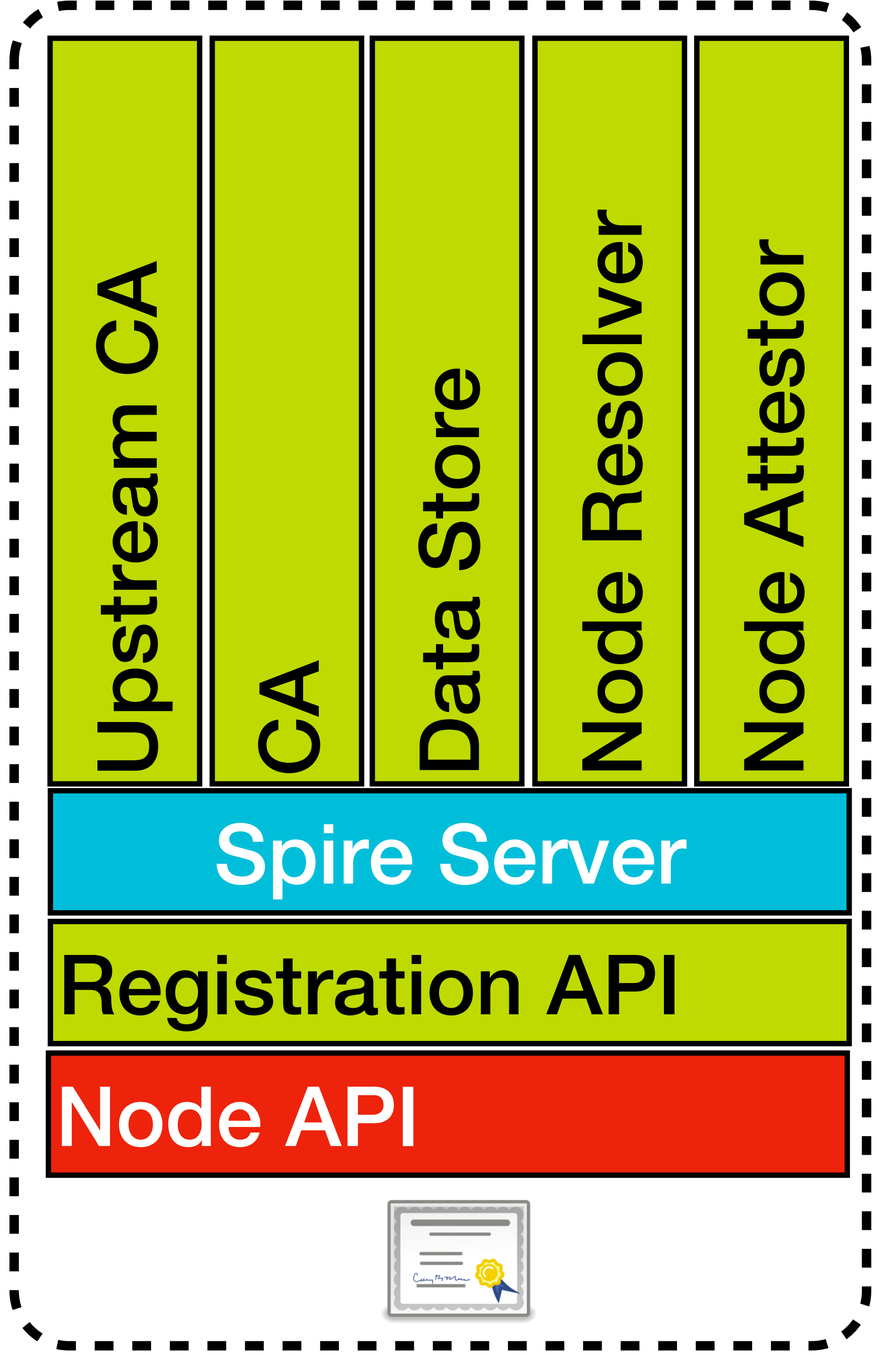

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

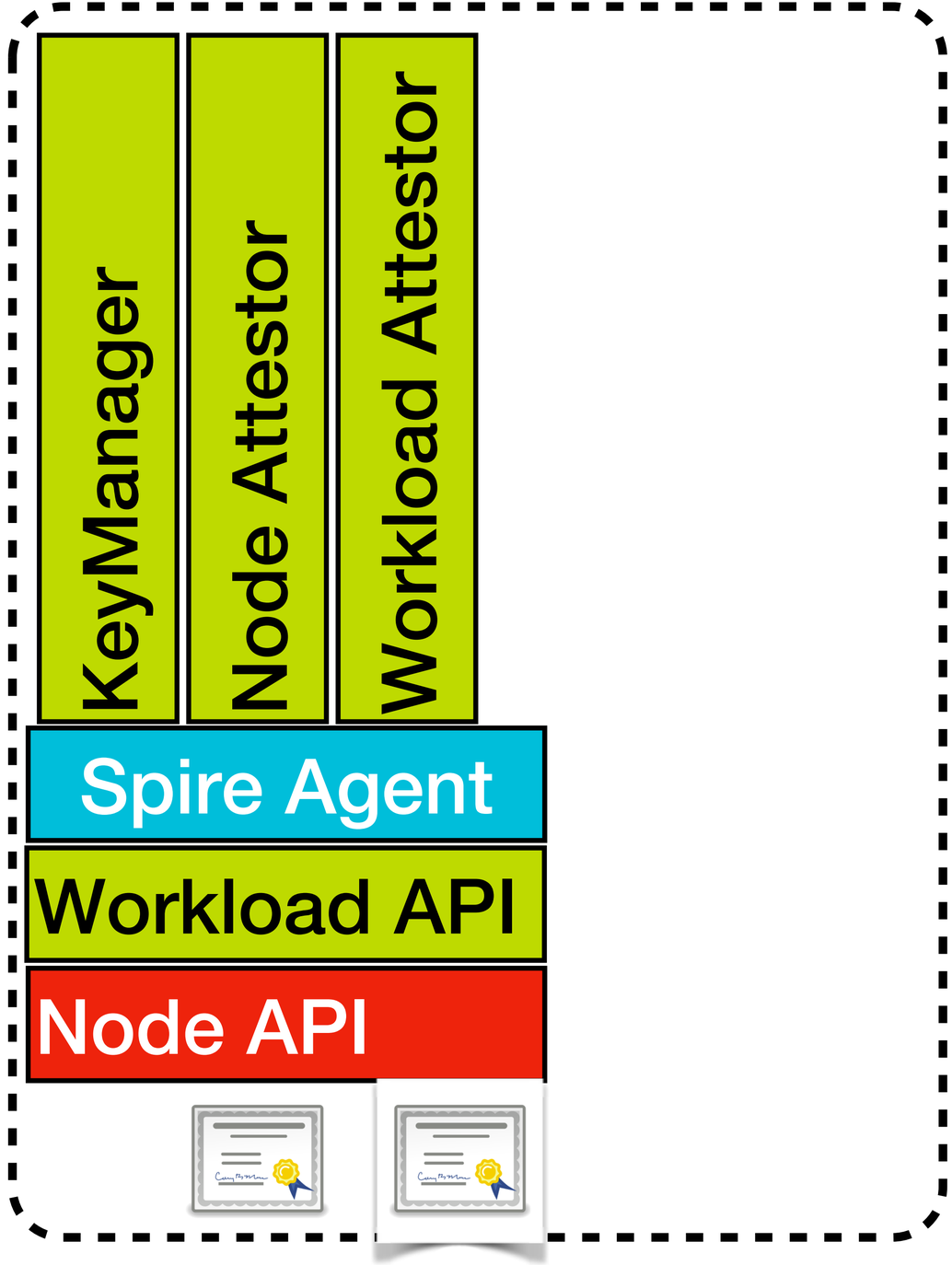

KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

SCYTALE

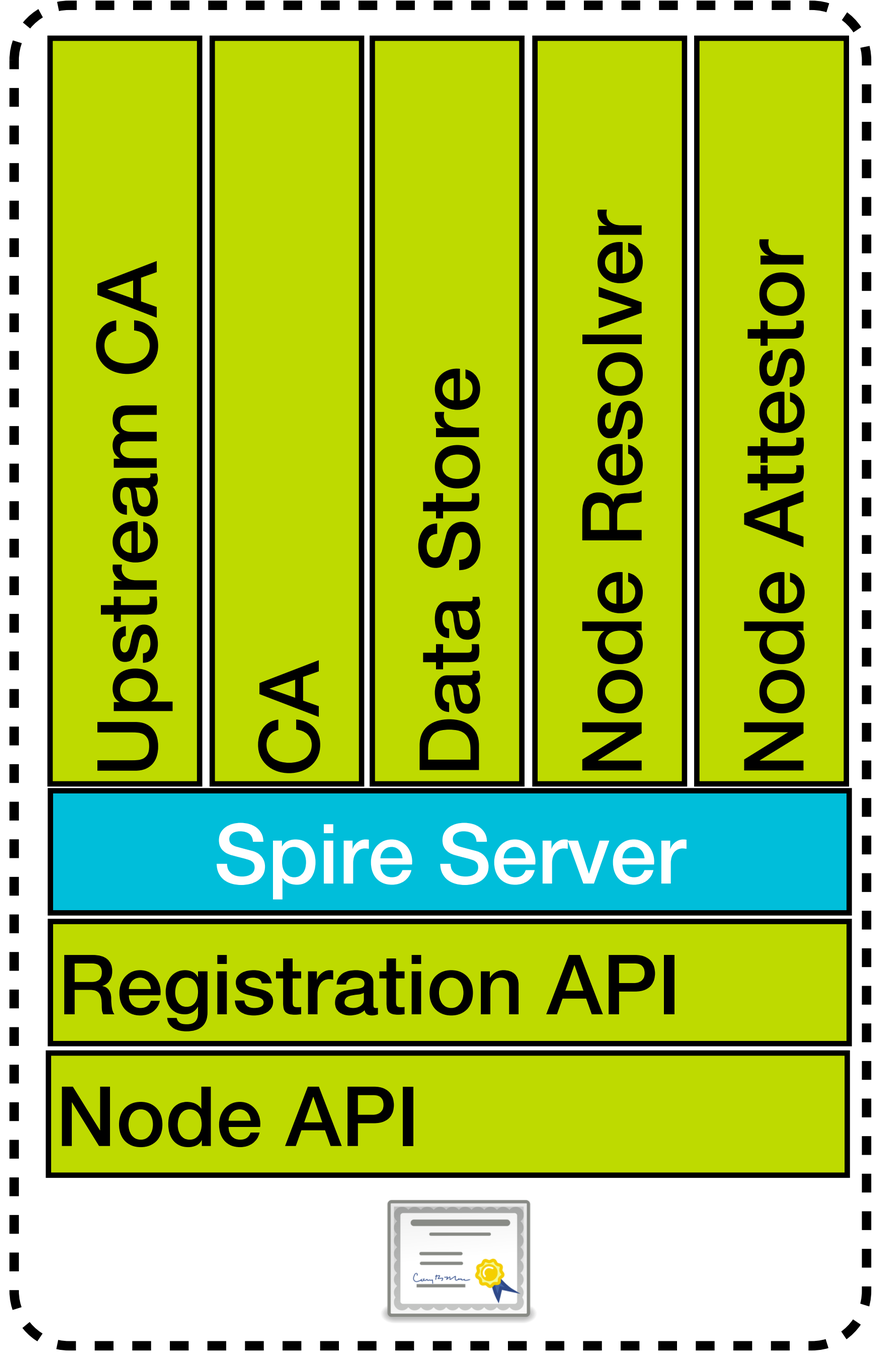

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API
KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

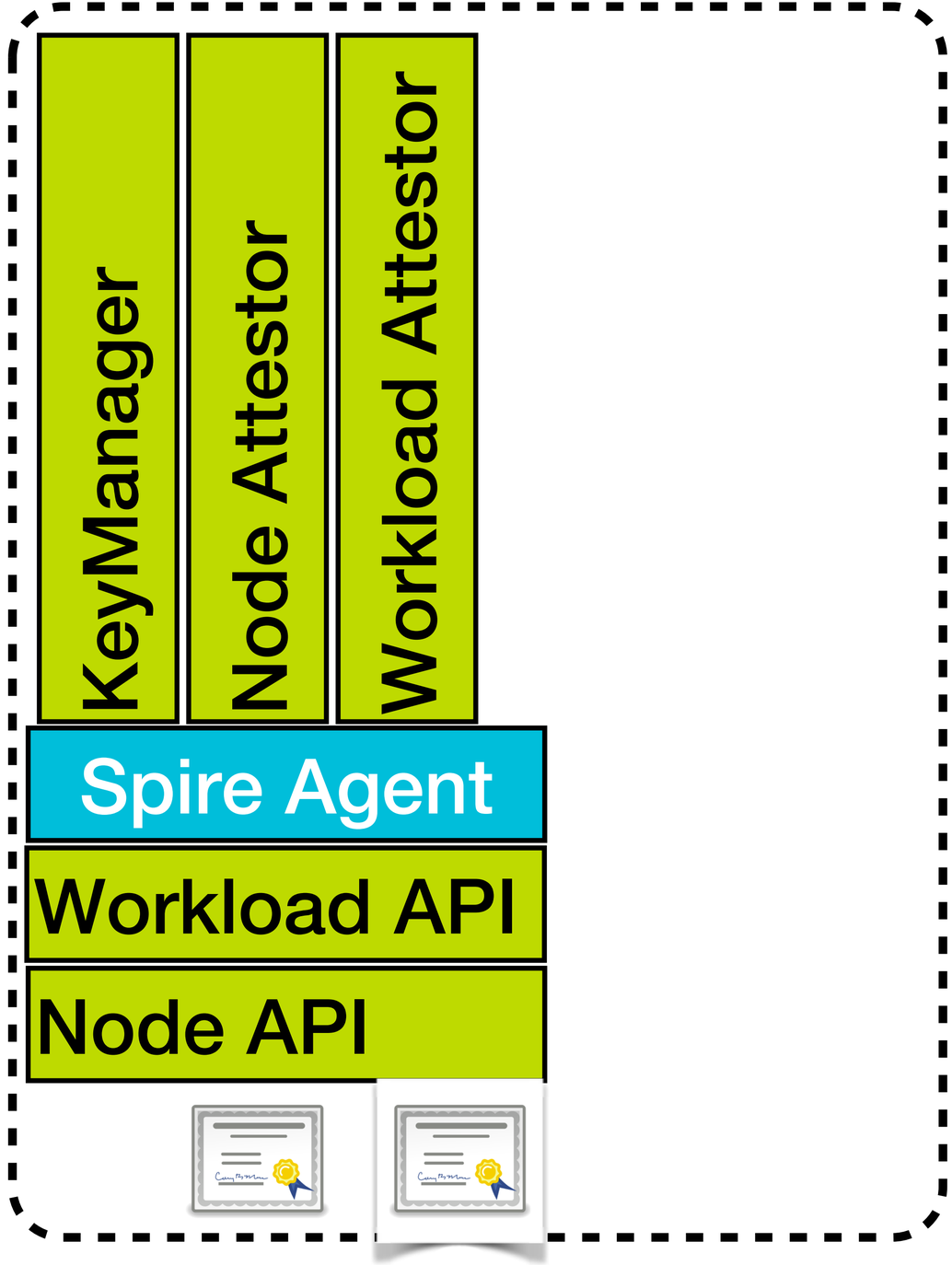

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API
KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

SCYTALE


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload API
Node API

SCYTALE

Workload
Attestation

SCYTALE

Upstream CA

CA

Data Store

Node Resolver

Node Attestor

Spire Server

Registration API

Node API

KeyManager

Node Attestor

Workload Attestor

Spire Agent

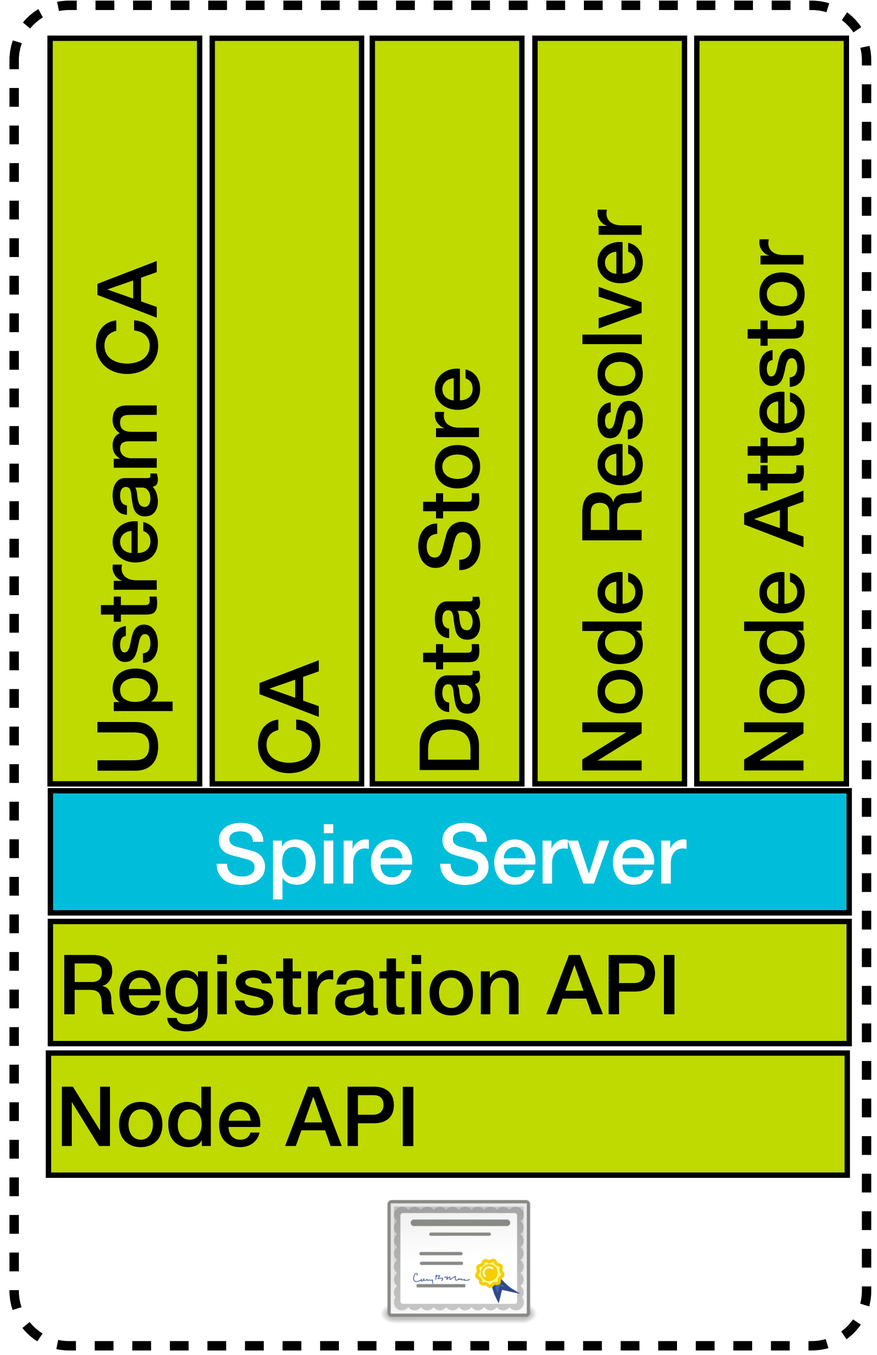
Workload API

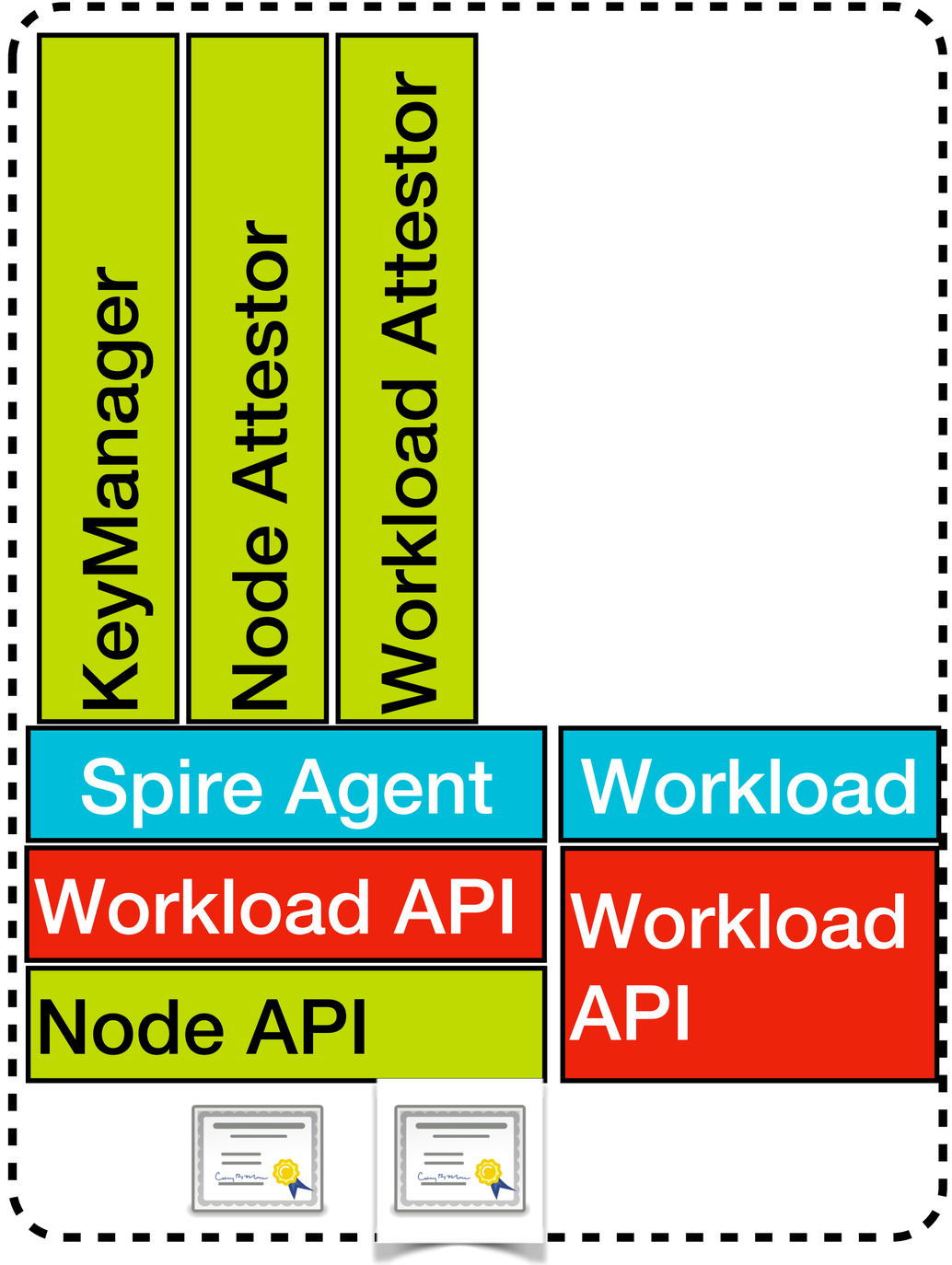
Node API

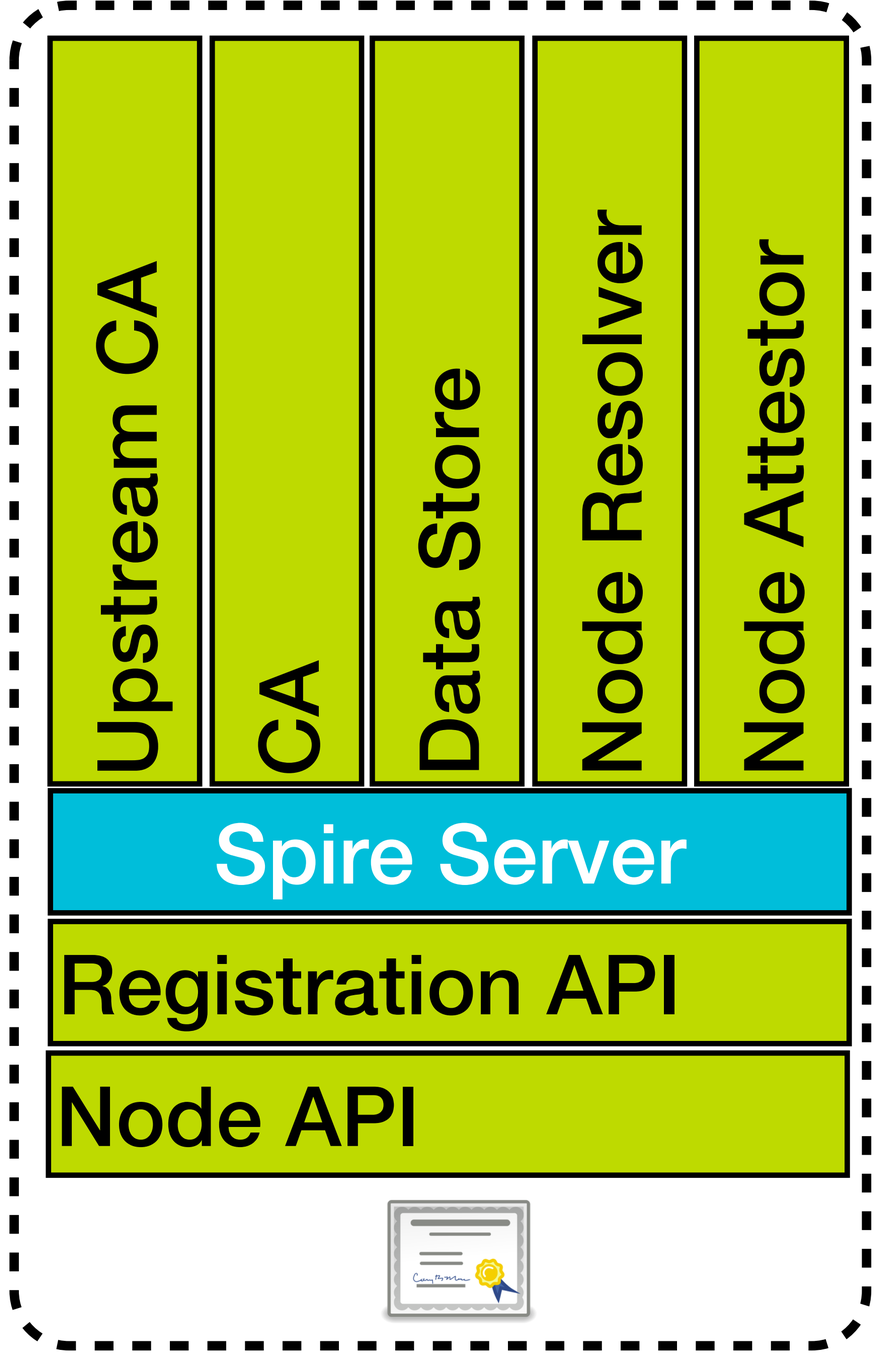
Workload

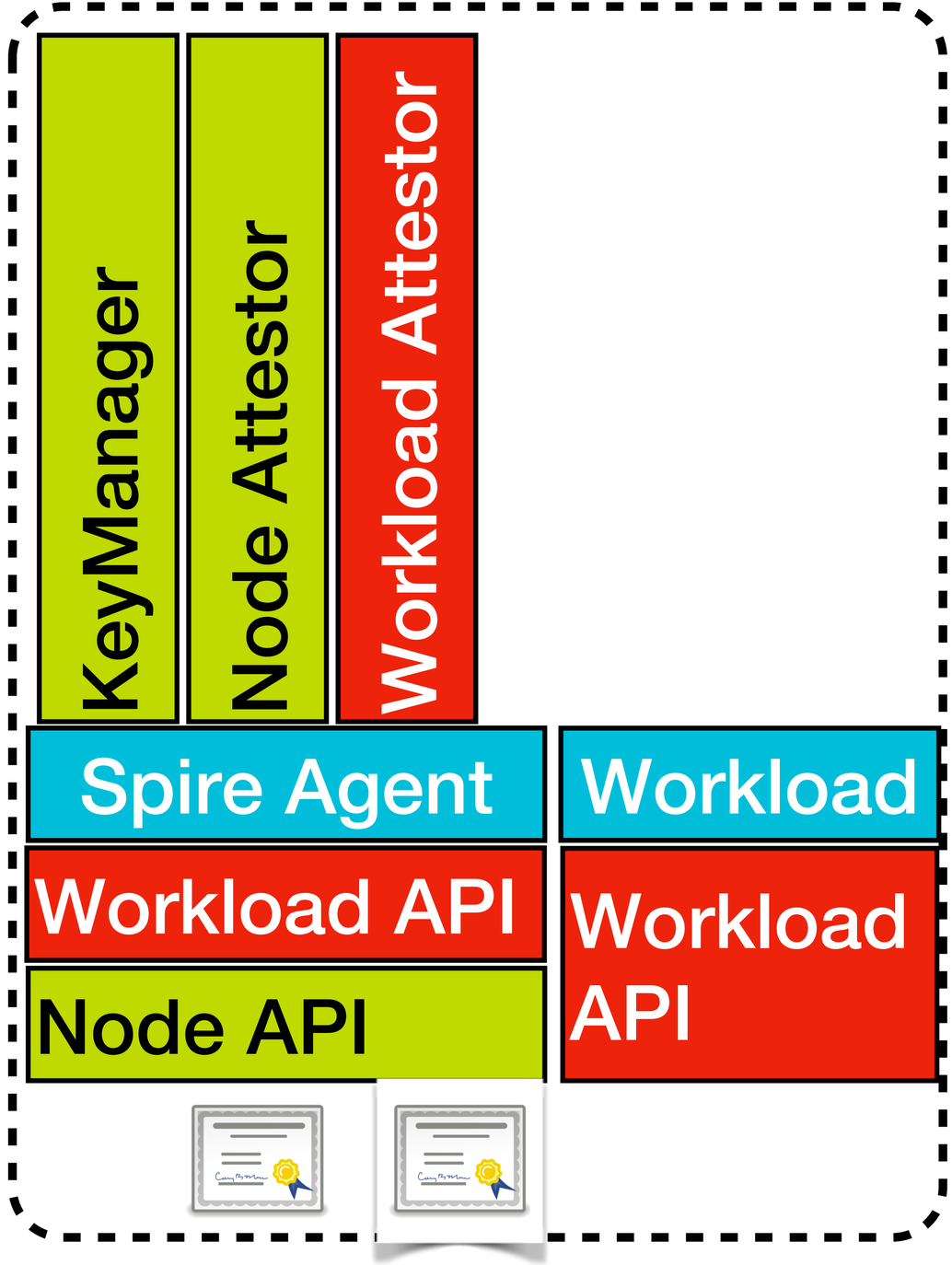
Workload API

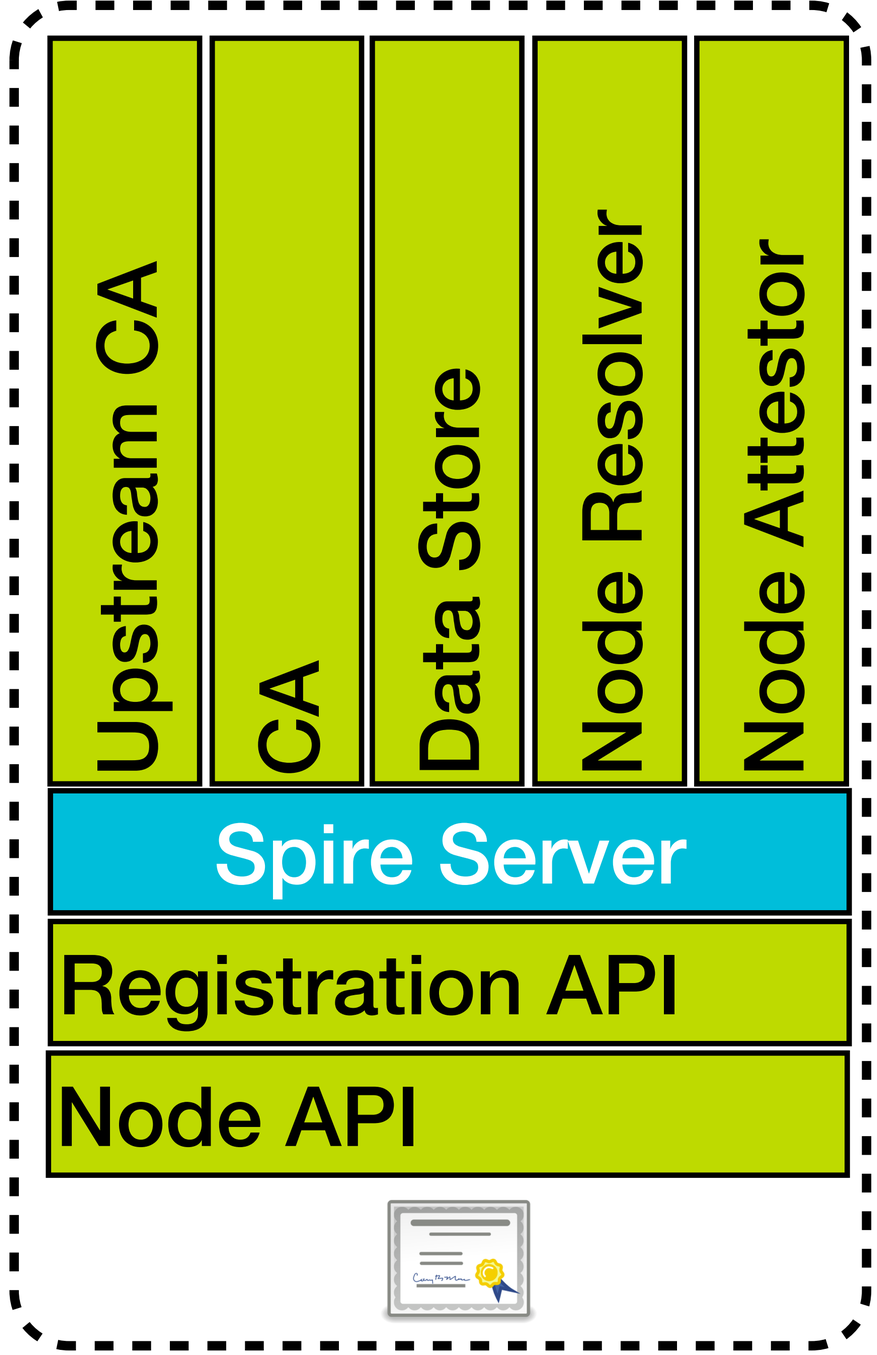
SCYTALE

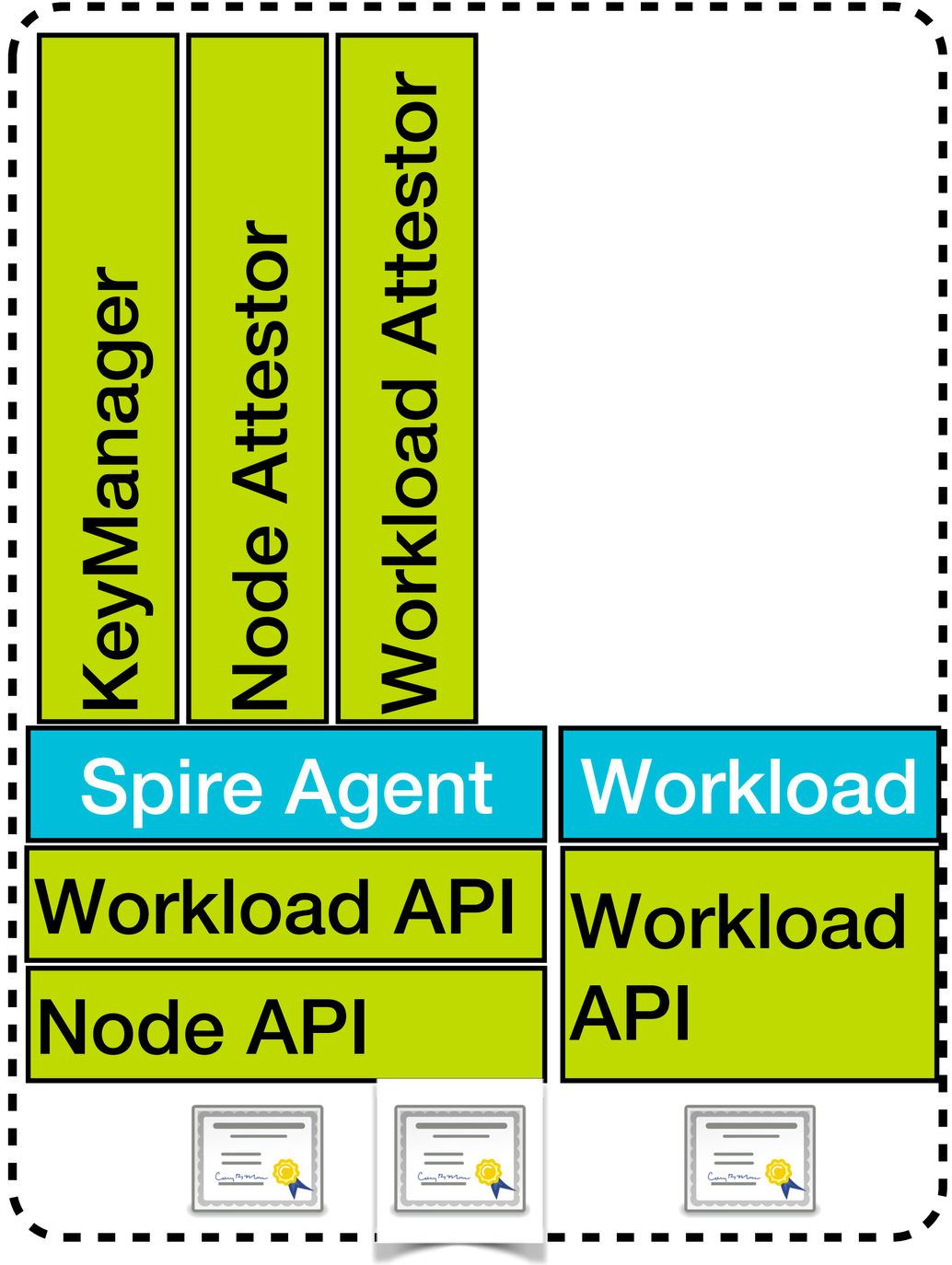

Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API

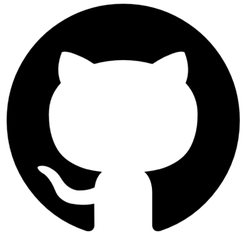

KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload
Workload API
Workload API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload
Workload API
Workload API
Node API


Upstream CA
CA
Data Store
Node Resolver
Node Attestor
Spire Server
Registration API
Node API


KeyManager
Node Attestor
Workload Attestor
Spire Agent
Workload
Workload API
Node API
Workload API



spiffe/plugin-template/SPIRE_PLUGIN_GUIDE.md

Bringing Kerberos to Microservices with SPIRE

Neel Shah
shahneel@vmware.com

Member of Technical Staff
Cloud Native Apps

05/03/2018

vmware®

Agenda

Introduction

Kerberos

Protocol overview

Kerberos within a domain

Project Lightwave

Node Attestation with Kerberos

Demo: SPIRE + Kerberos

Conclusion

Introduction

Enterprise identity and SSO commonly provided by Kerberos

- Microsoft Active Directory
- Heimdal Kerberos
- MIT Kerberos

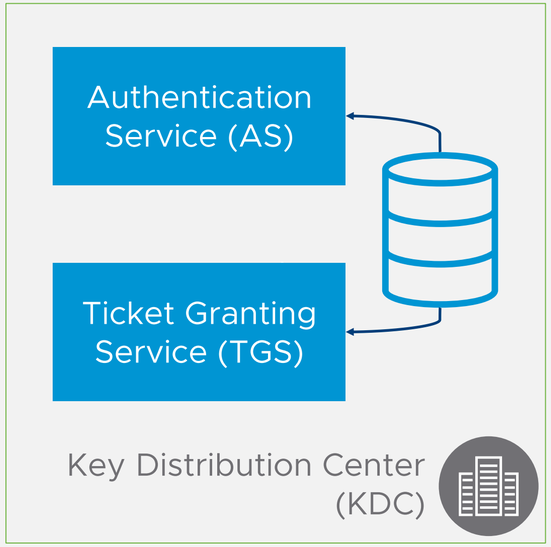
The predominant on-premise authentication protocol is Kerberos through Active Directory

Kerberos is therefore an ideal bootstrap for SPIRE (as a node attestor)

- SPIRE does not have a mechanism to issue identities backed by Kerberos providers
- With Kerberos support, SPIRE can manage identities tied closely to existing enterprise infrastructure

Kerberos

Protocol Overview

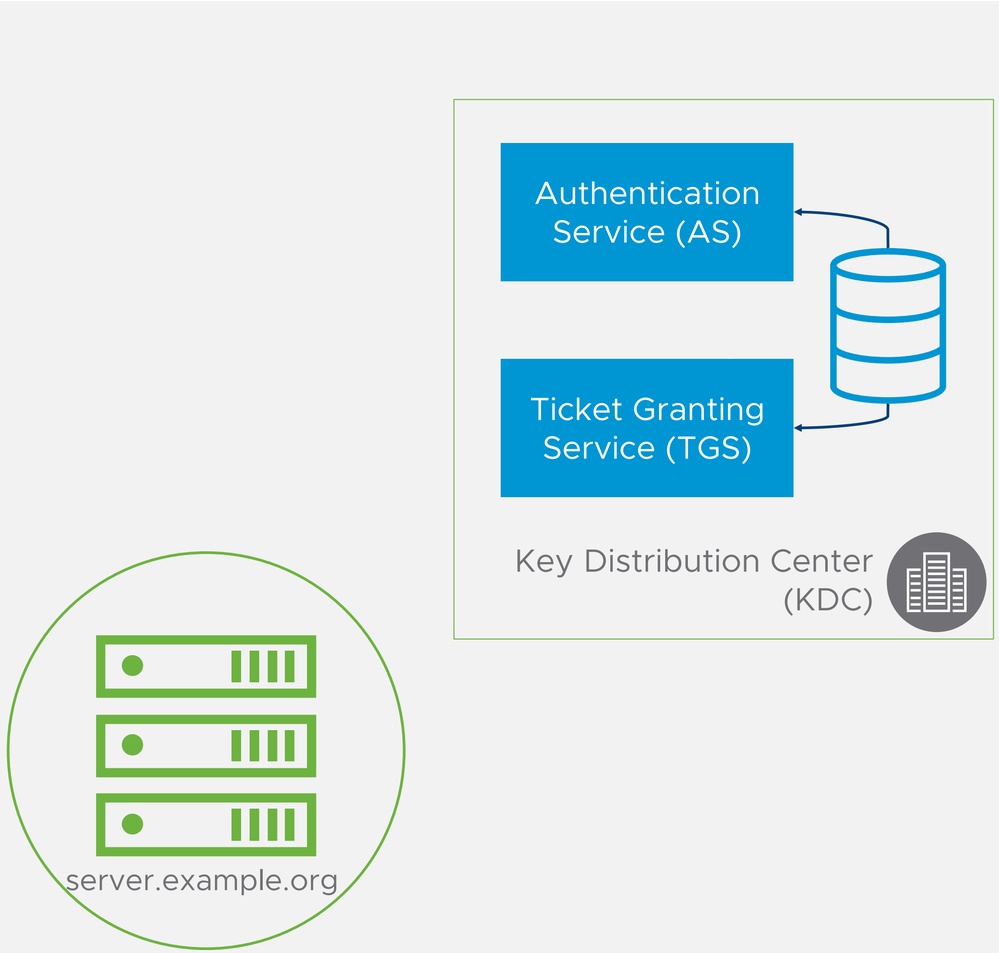


Three Players:

- **Trusted Third Party (KDC)**

Kerberos

Protocol Overview

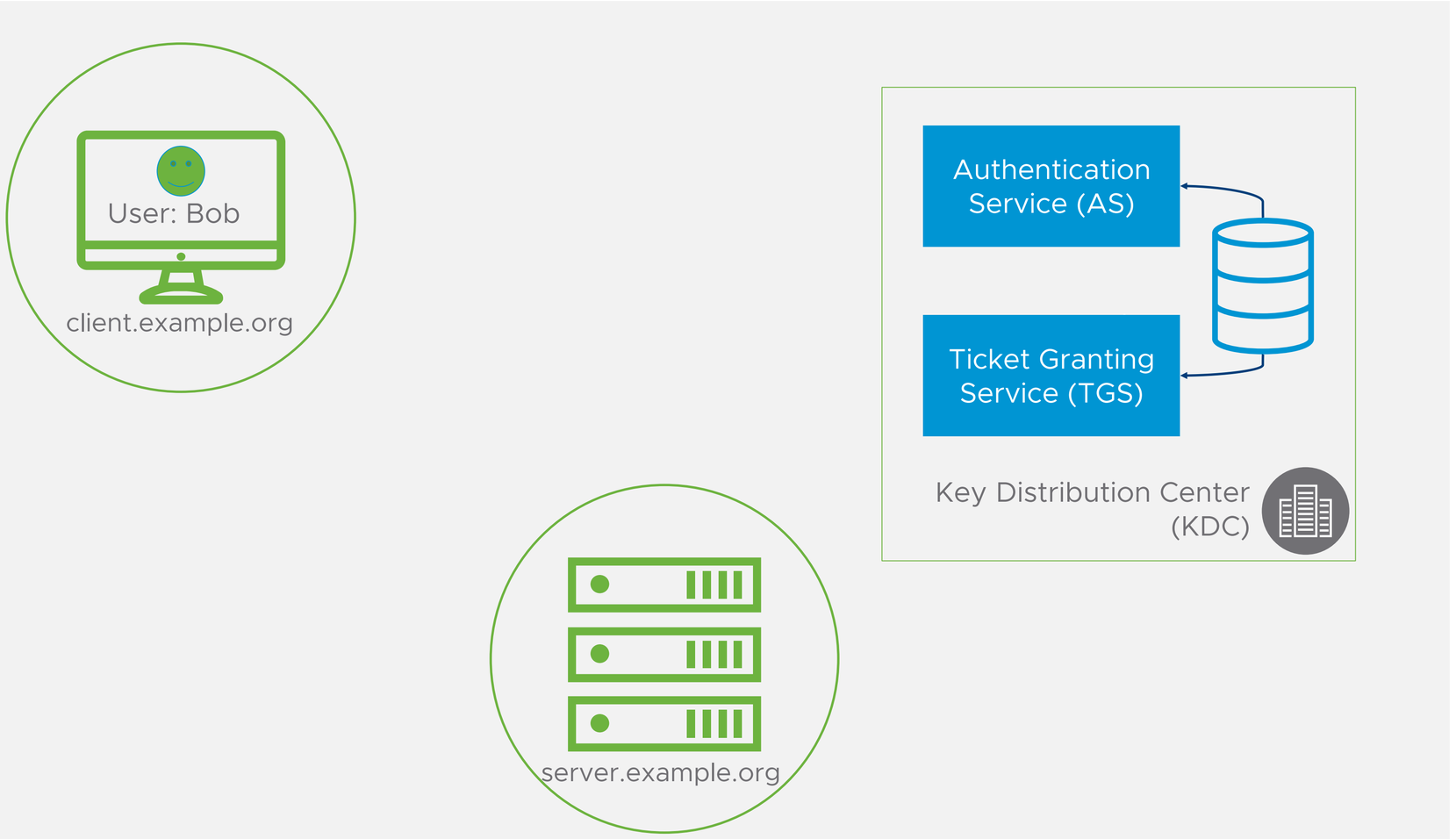


Three Players:

- Trusted Third Party (KDC)
- **Server**

Kerberos

Protocol Overview

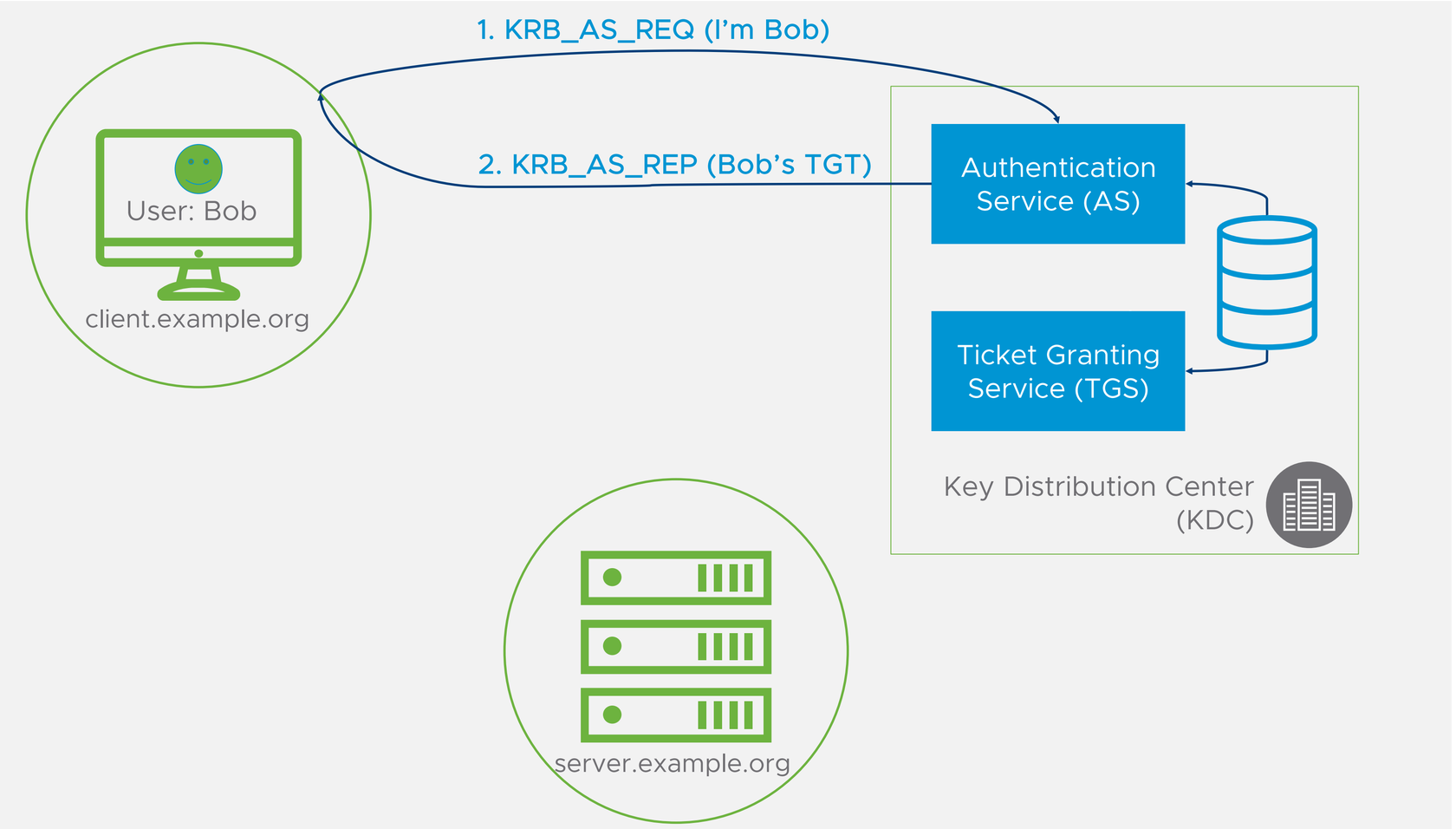


Three Players:

- Trusted Third Party (KDC)
- Server
- **Client**

Kerberos

Protocol Overview



Three Players:

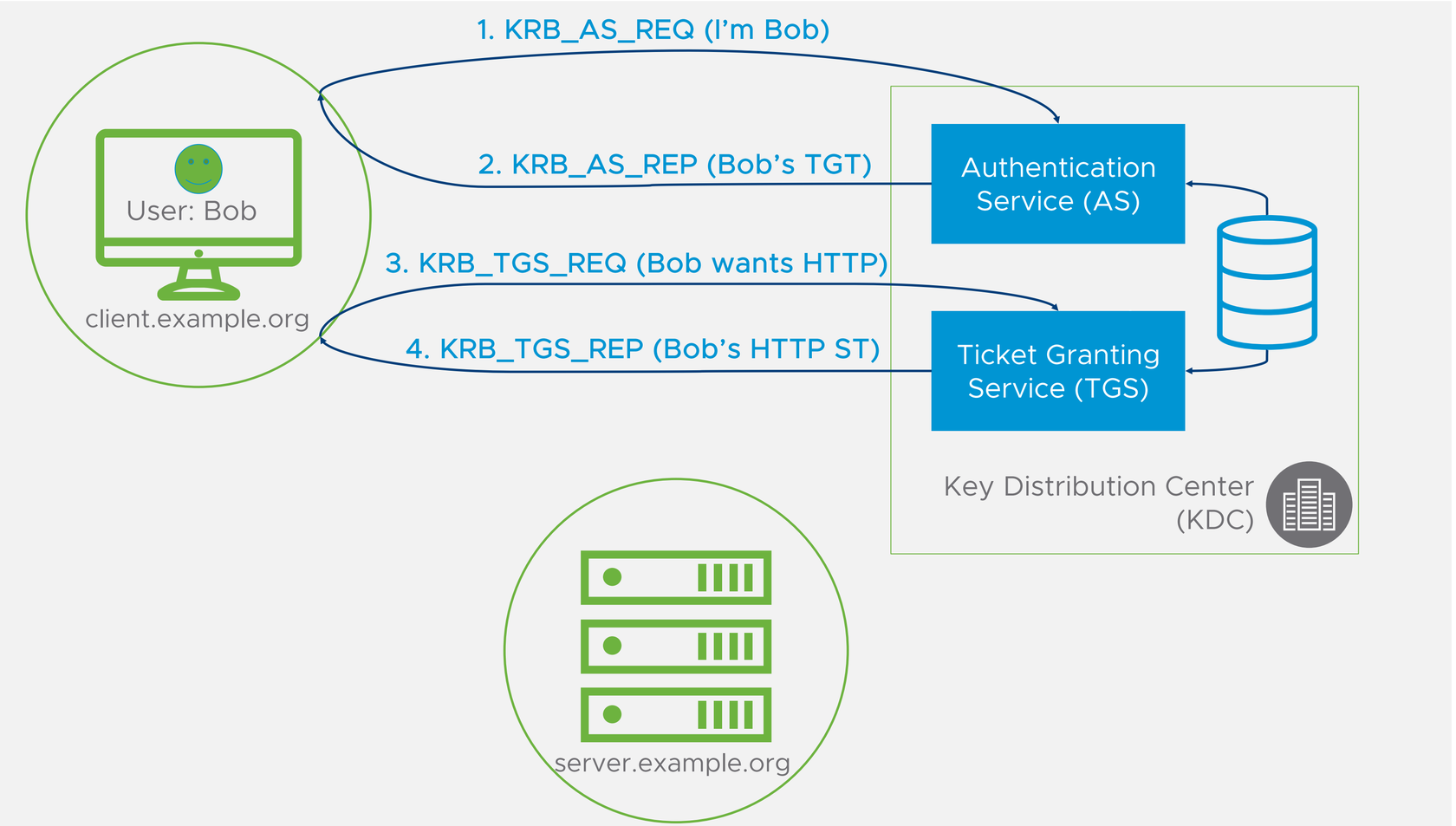
- Trusted Third Party (KDC)
- Server
- Client

Three Steps:

- **"Login"**

Kerberos

Protocol Overview



Three Players:

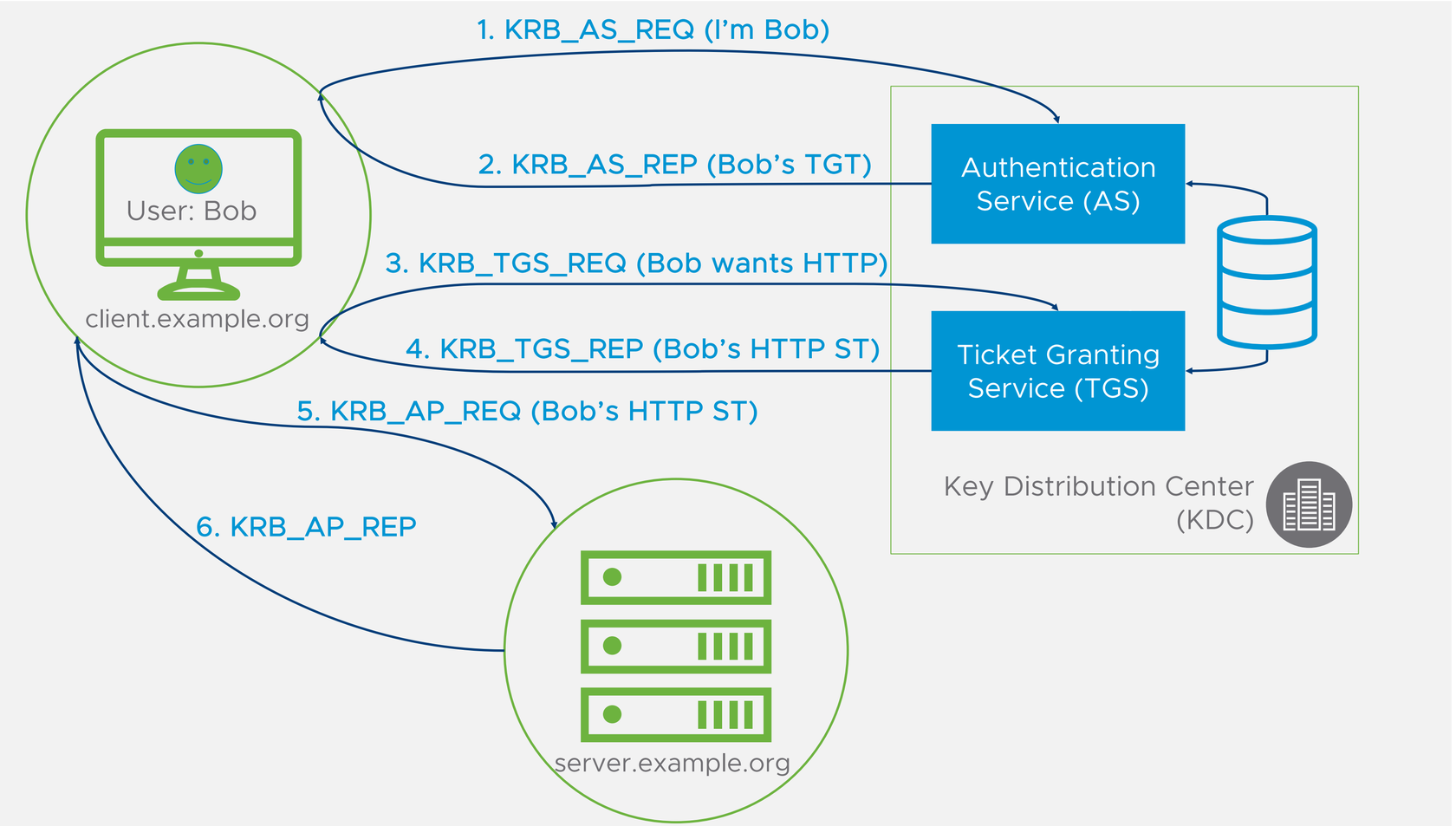
- Trusted Third Party (KDC)
- Server
- Client

Three Steps:

- "Login"
- **"Long Lived Service Ticket"**

Kerberos

Protocol Overview



Three Players:

- Trusted Third Party (KDC)
- Server
- Client

Three Steps:

- "Login"
- "Long Lived Session Ticket"
- **"Service Access"**

Kerberos

Kerberos Within a Domain

Domain Controllers (e.g. Active Directory) automate Kerberos management:

- Active Directory uses Kerberos as native identity provider
- Joining a machine to a domain will automatically create, configure, and manage a **computer account**
- Automatically associates **identity to all machines** within a domain

Active Directory Domains = Kerberos Realms

vmware/lightwave

Lightwave is an open source multi-tenanted cloud directory service from VMware

It is comprised of the following elements:

- Lightwave Directory Service: multi-master eventually consistent LDAP platform (REST+LDAP)
- Lightwave Kerberos: An integrated Kerberos KDC (Kerberos)
- Lightwave Authentication Services: A multi-protocol Secure Token Service (OAuth/OIDC, SAML)
- Lightwave Certification Services: An integrated Certificate Authority (x.509)
- Lightwave DNS Services: An integrated, Kerberized domain name service (DNS)

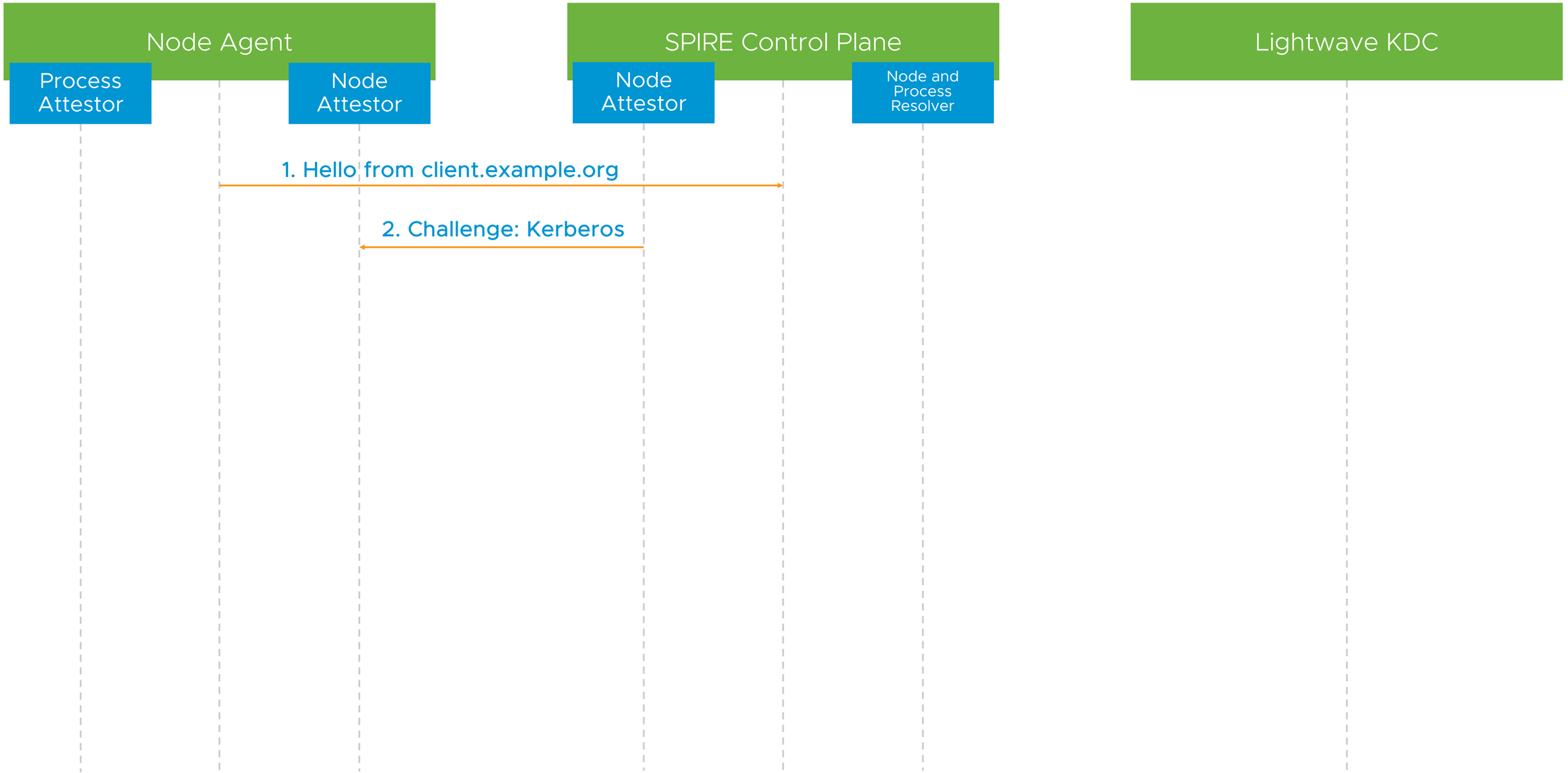
Converged Identity

- Kerberos and OAuth2.0/OIDC come together in the Directory Service

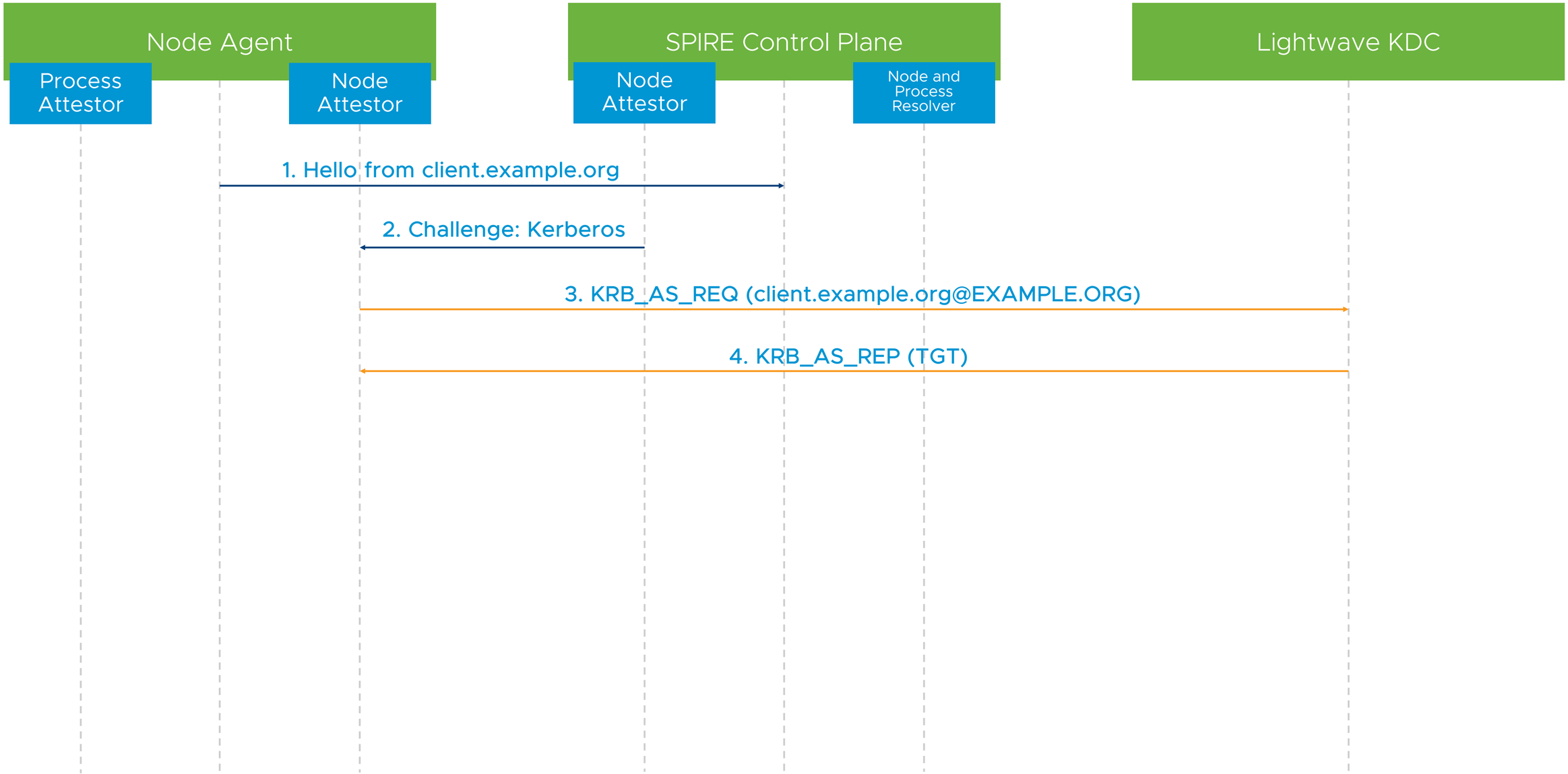
License

- Apache 2.0

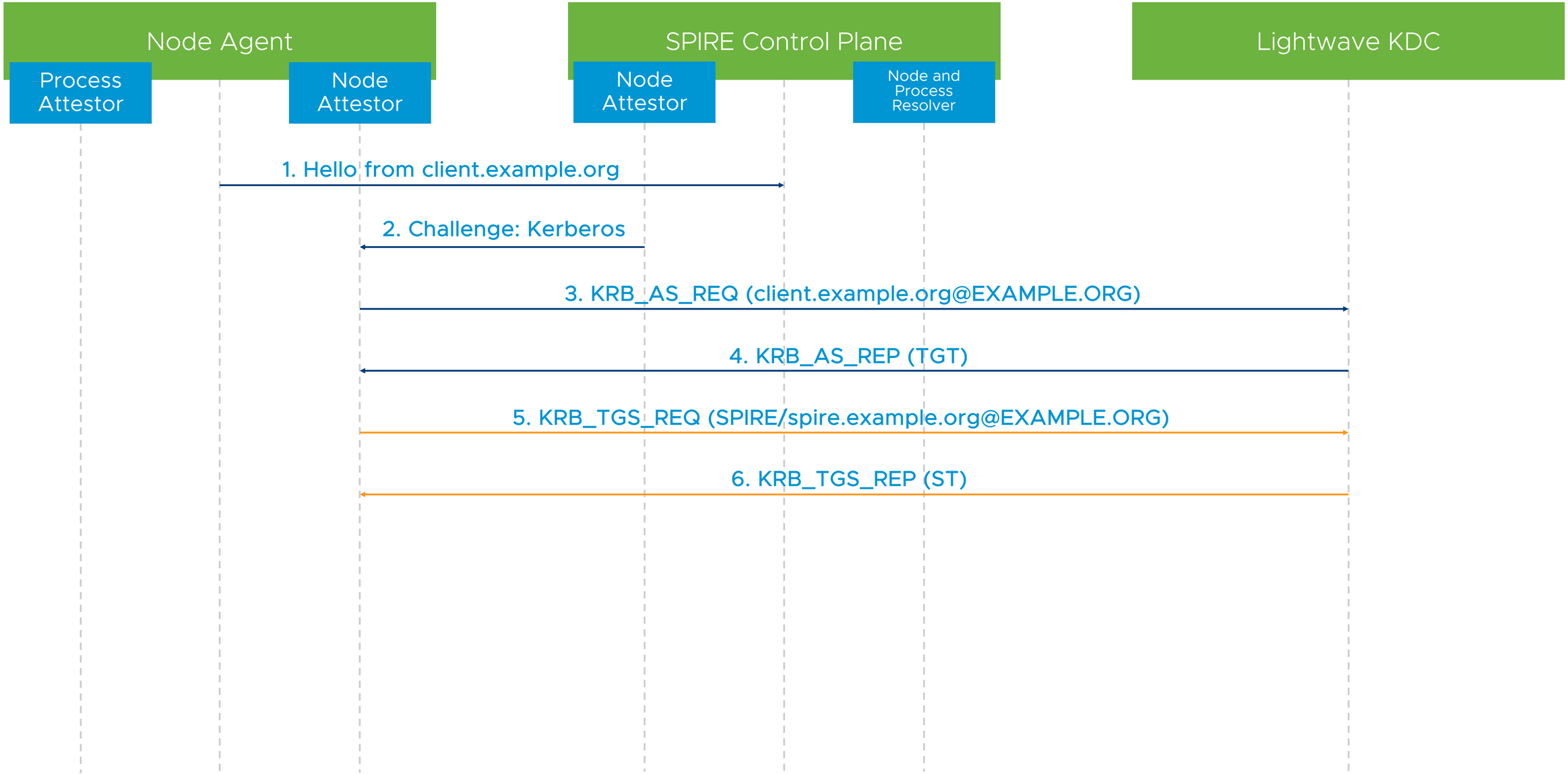
Node Attestation with Kerberos



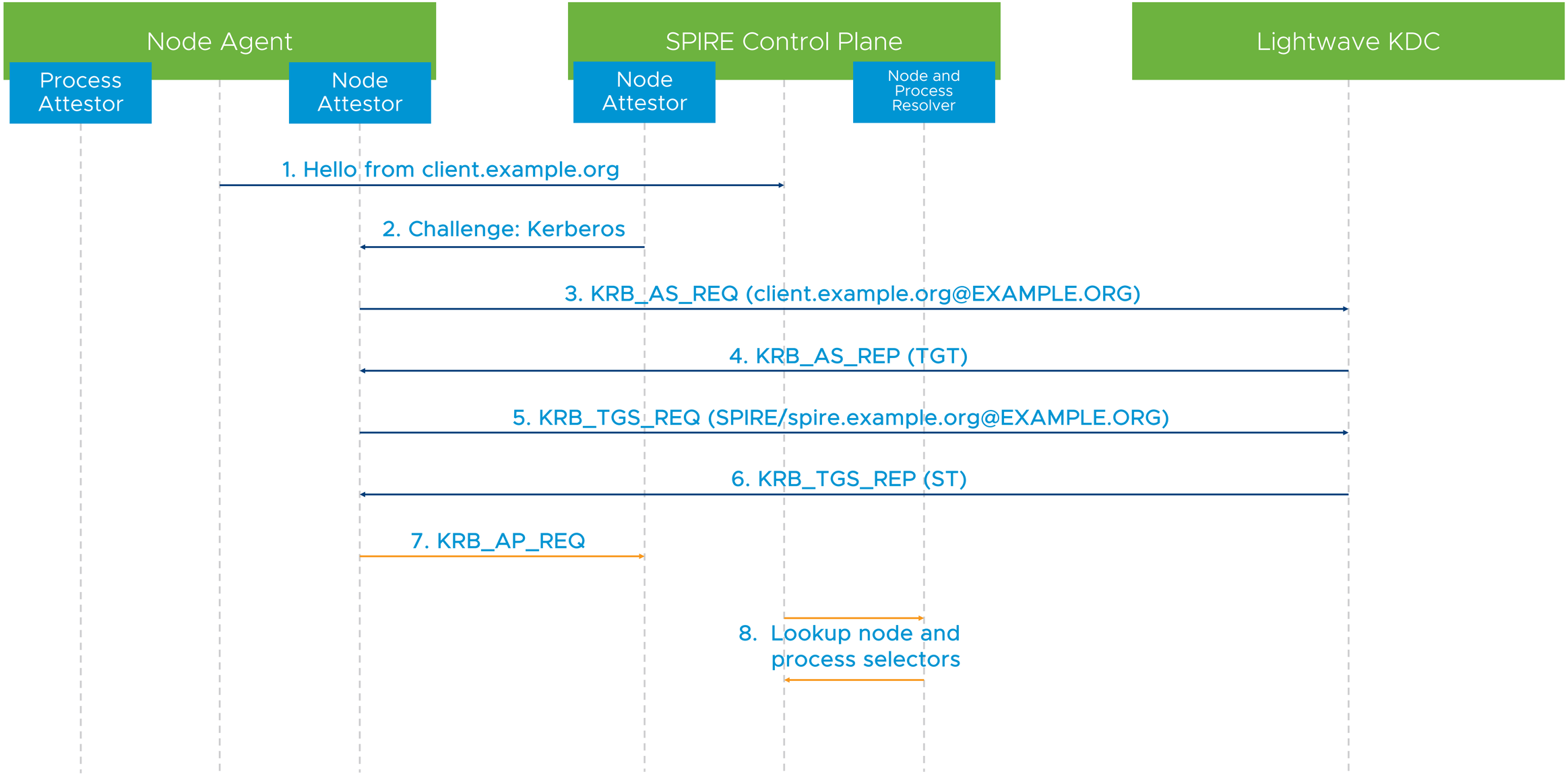
Node Attestation with Kerberos



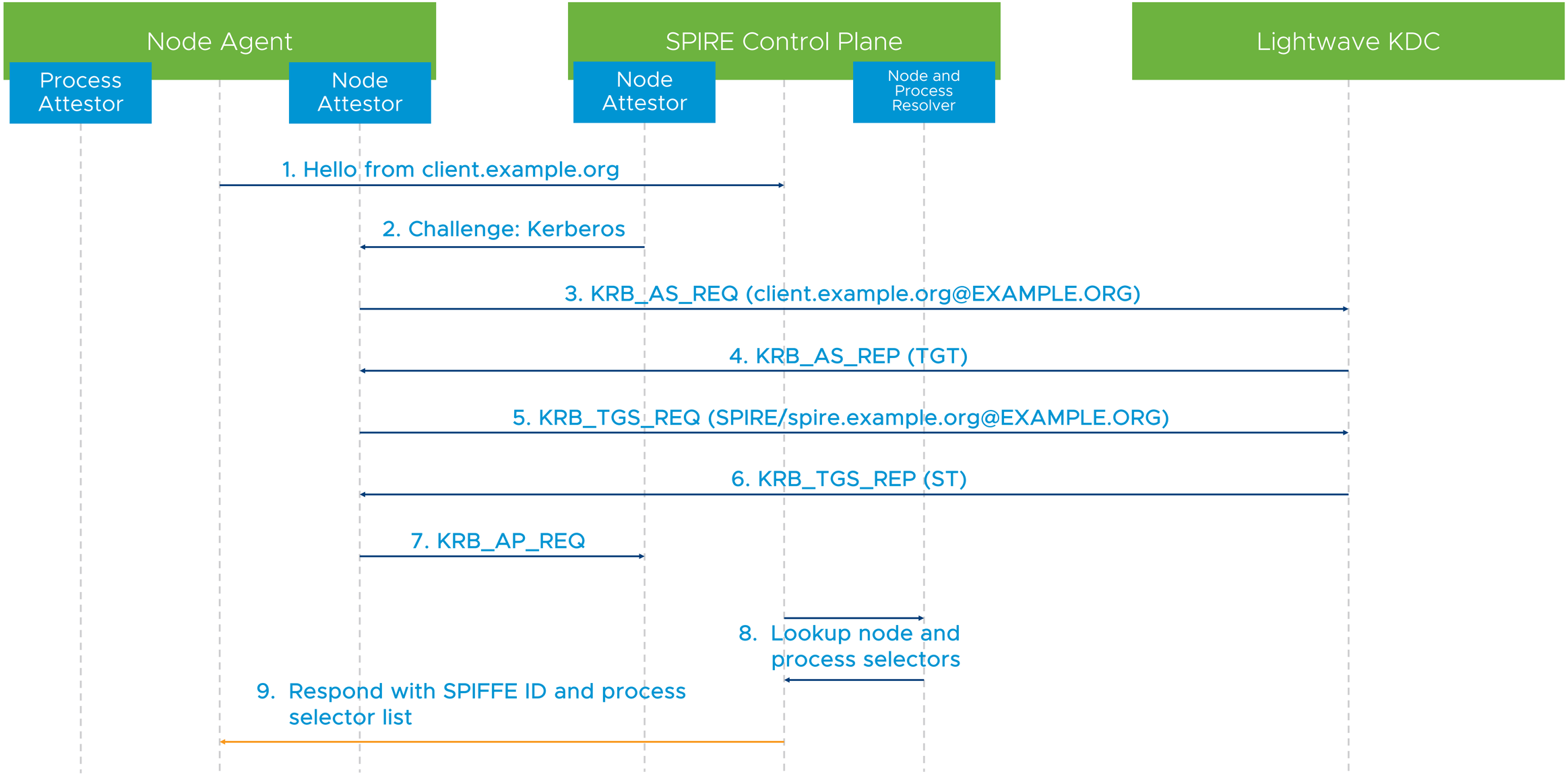
Node Attestation with Kerberos



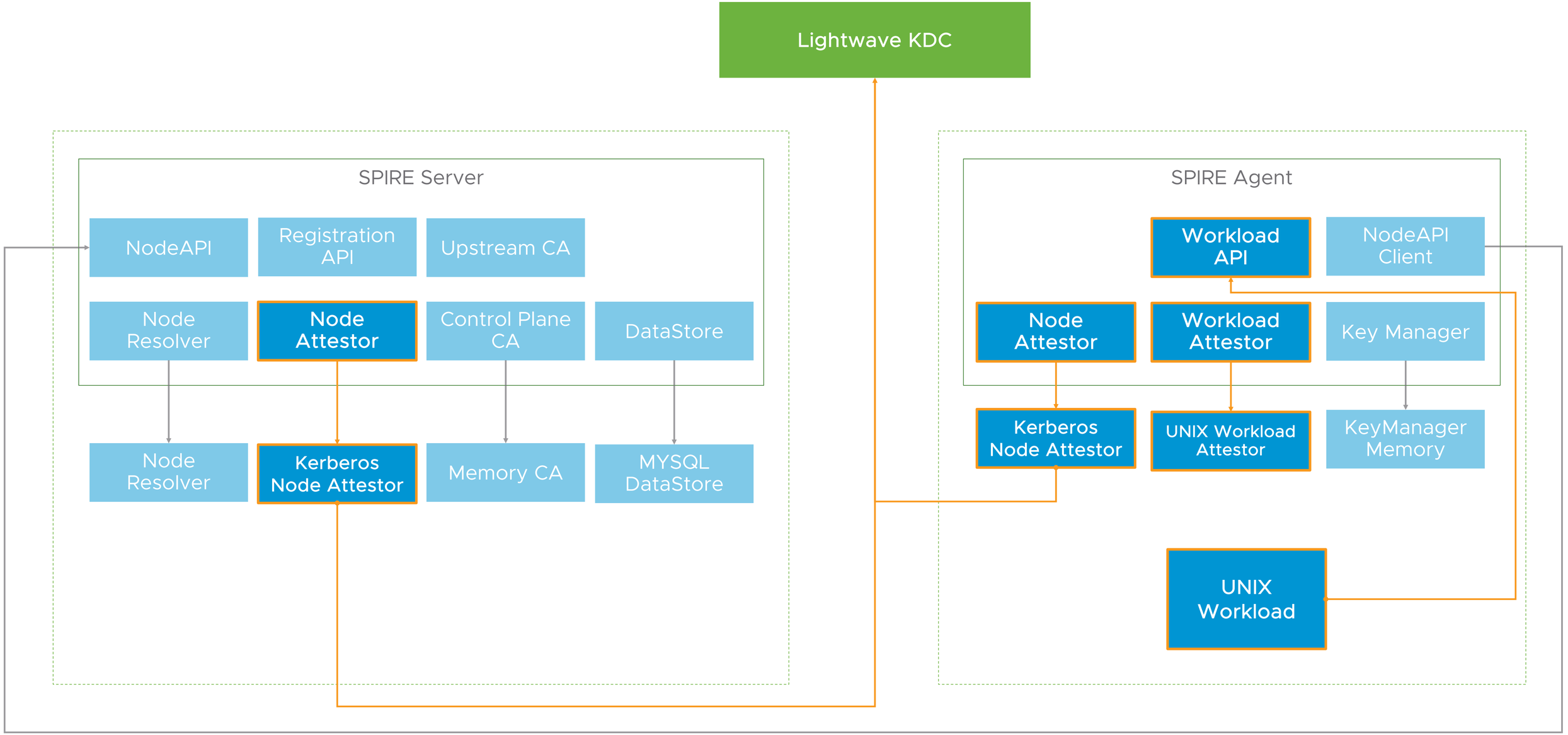
Node Attestation with Kerberos



Node Attestation with Kerberos



Demo: SPIRE + Kerberos



Resources

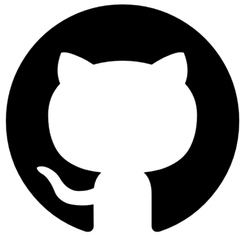
Kerberos-Attestor – github.com/spiffe/kerberos-attestor

Lightwave – github.com/vmware/lightwave

PhotonOS – github.com/vmware/photon

Kerberos:

- github.com/nks5295/gokrb5
- https://tools.ietf.org/html/rfc4120
- https://technet.microsoft.com/en-us/library/cc772815(v=ws.10).aspx
- http://www.zeroshell.org/kerberos/Kerberos-operation/



spiffe/spiffe

spiffe/spire

spiffe/spiffe-example

slack.spiffe.io

SCYTALE

https://blog.scytale.io/nginx-spire-a63ce46d9a5

Questions?

SCYTALE