Venafi

Can SPIFFE Help You Solve ‘Secret Zero’?

Mattias Gees
Director of Tech
@MattiasGees / mattias.gees@venafi.com

What is a Workload Identity?

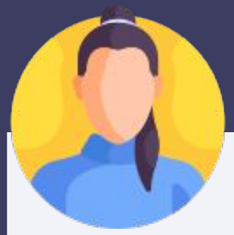
Machine Identities

WORKLOAD

- Container
- Process
- Application
- Service
- Virtual Machine

DEVICE

- Server
- Laptop
- IOT device
- Mobile device



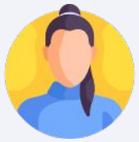
Human Identities

INTERNAL

- Permanent
- Contractors
- Gig workers

EXTERNAL

- Customers
- Partners
- Vendors
- Consultants
- Guests
- Citizens



Who Cares?

“An entity without an identity cannot exist because it would be nothing. To exist is to exist as something, and that means to exist with a particular identity” – Aristotle

What is SPIFFE?

Secure Production Identity Framework for Everyone

spiffe

Secure Production Identity Framework For Everyone

3.) Regulation Protect
Zero Trust Responding to
Mandate Supply Chain attacks

spiffe

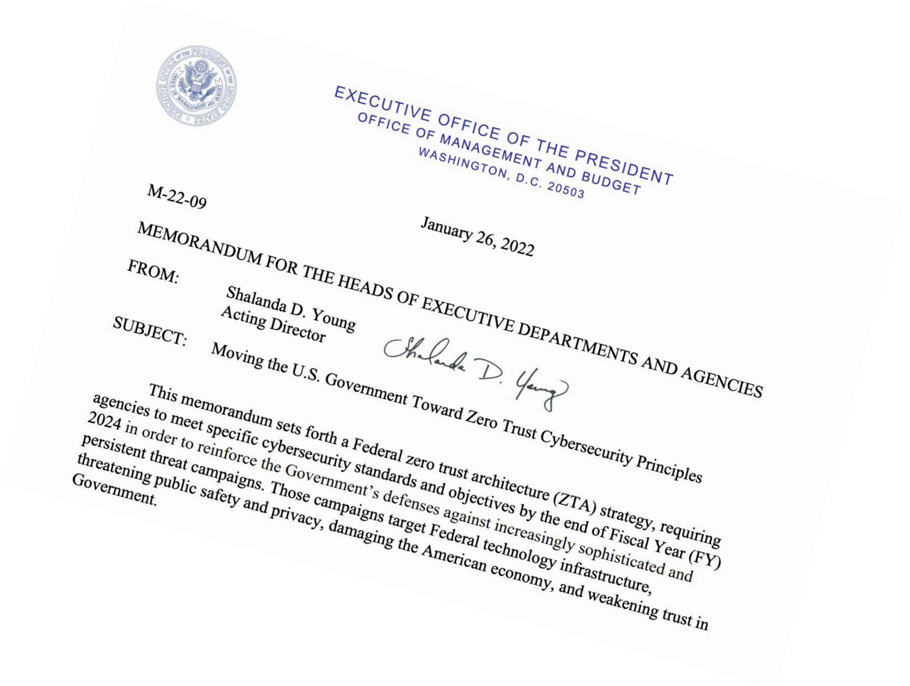
Why Now?

1.) Open Source, Foundation Owned. Graduated

CLOUD NATIVE
COMPUTING FOUNDATION

2.) Being adopted by, and Standardised on by industry

aws


EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-22-09

January 26, 2022

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

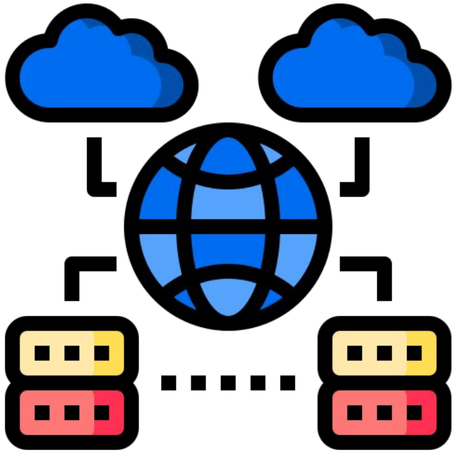
SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

What does SPIFFE solve?

Use-cases

Remove need for API Keys



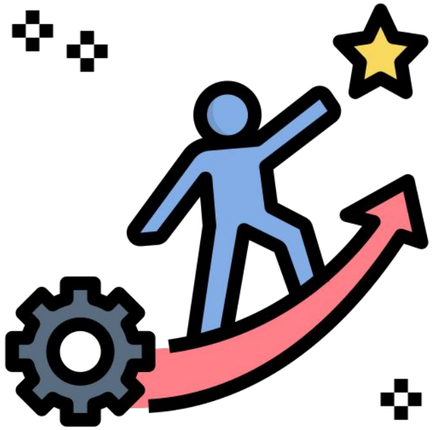
Multi Cloud Authentication

Software Supply Chain Security

Advantages

Zero Trust Security

Improved Auditing



Improved Developer Experience

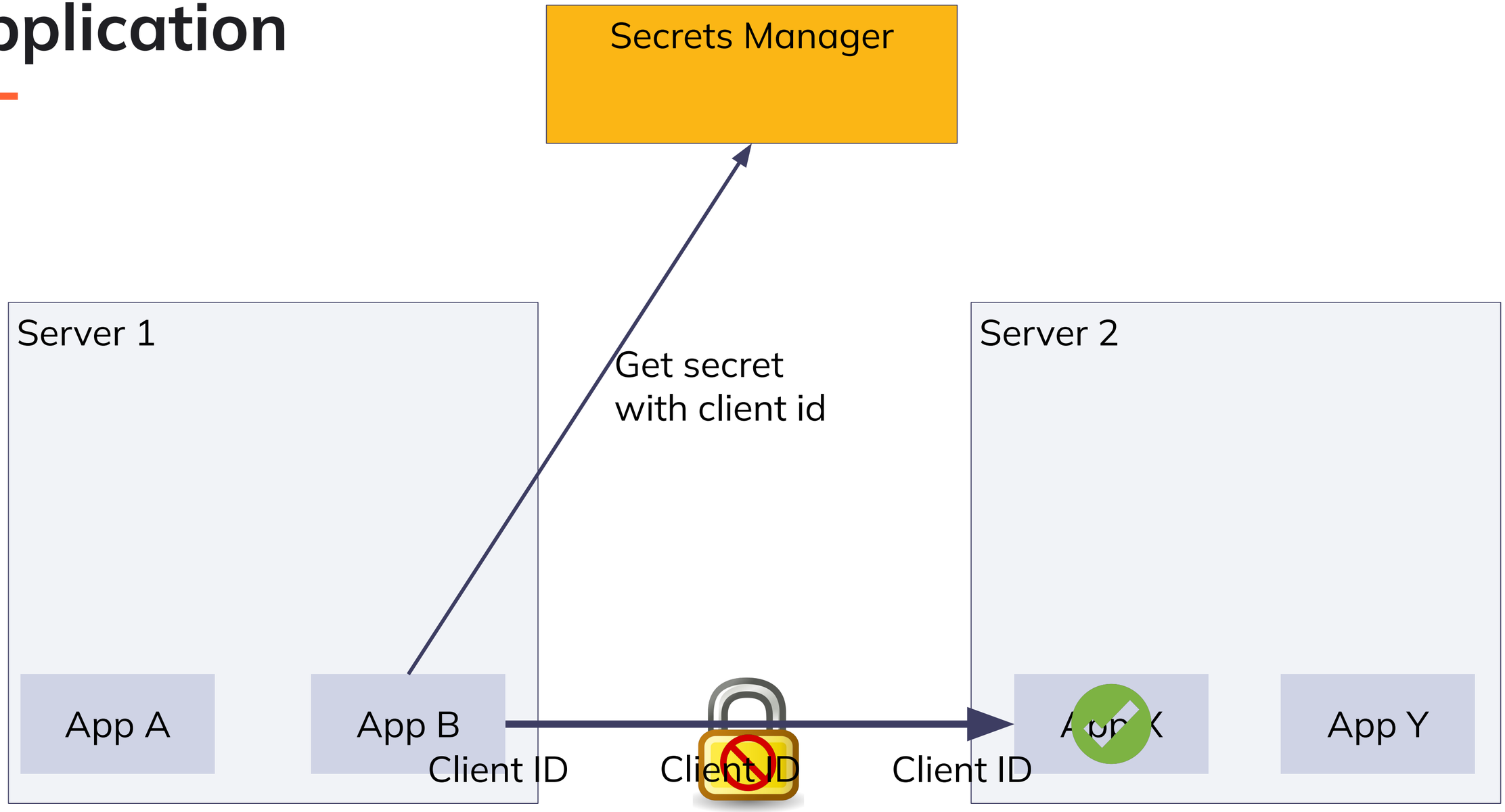
No rotation of secrets

To build software that rises to today's security challenges, we must raise the bar on developer usability. With SPIFFE, cryptographic identity can flow naturally without explicit involvement of users. This enables organizations to easily and uniformly secure complex, heterogeneous infrastructure. Identity also pays dividends across other dimensions like observability, policy enforcement, and development workflows.

Joe Beda - co-creator Kubernetes & SPIFFE's original author

How does it work?

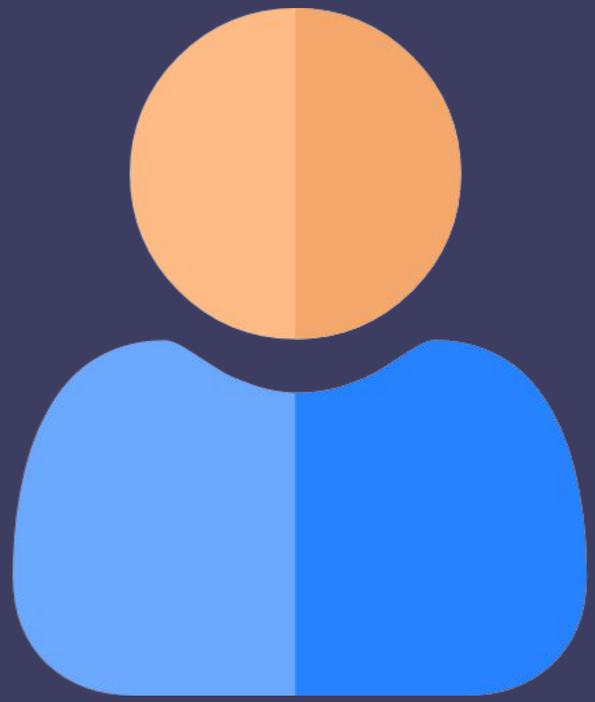
Application



SPIFFE Components

- SPIFFE IDs
- SPIFFE Verifiable Identity Document (SVID)
- SPIFFE Workload AP
- SPIFFE Workload Attestation
- SPIFFE Federation

SPIFFE ID



SPIFFE ID

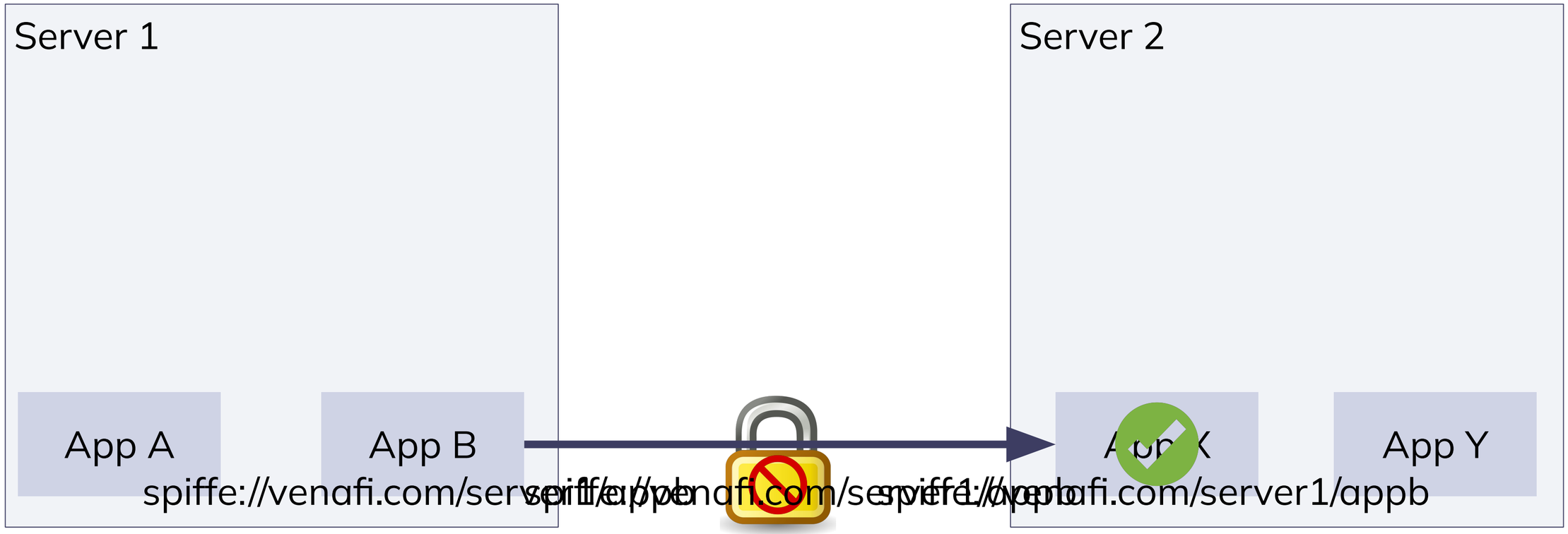
Scheme

Trust Domain

Path

spiffe://venafi.com/dc1/node10/frontend/webserver

Application



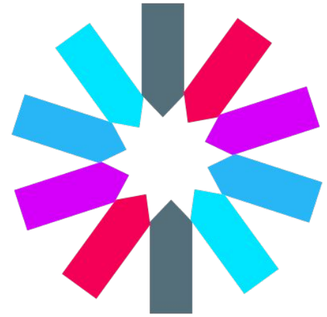
SPIFFE SVID

SPIFFE SVID

SVID

Cryptographic key material

X.509



JWT

SPIFFE SVID X.509

SPIFFE ID: spiffe://example.org/dev/frontend/webserver

Certificate:
    Data:
        Version: 3 (0x2)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O = Venafi, CN = venafi.com L = cluster 1
...
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                URI:spiffe://venafi.com/dc1/node10/frontend/webserver

SPIFFE SVID JWT

JWT Header:

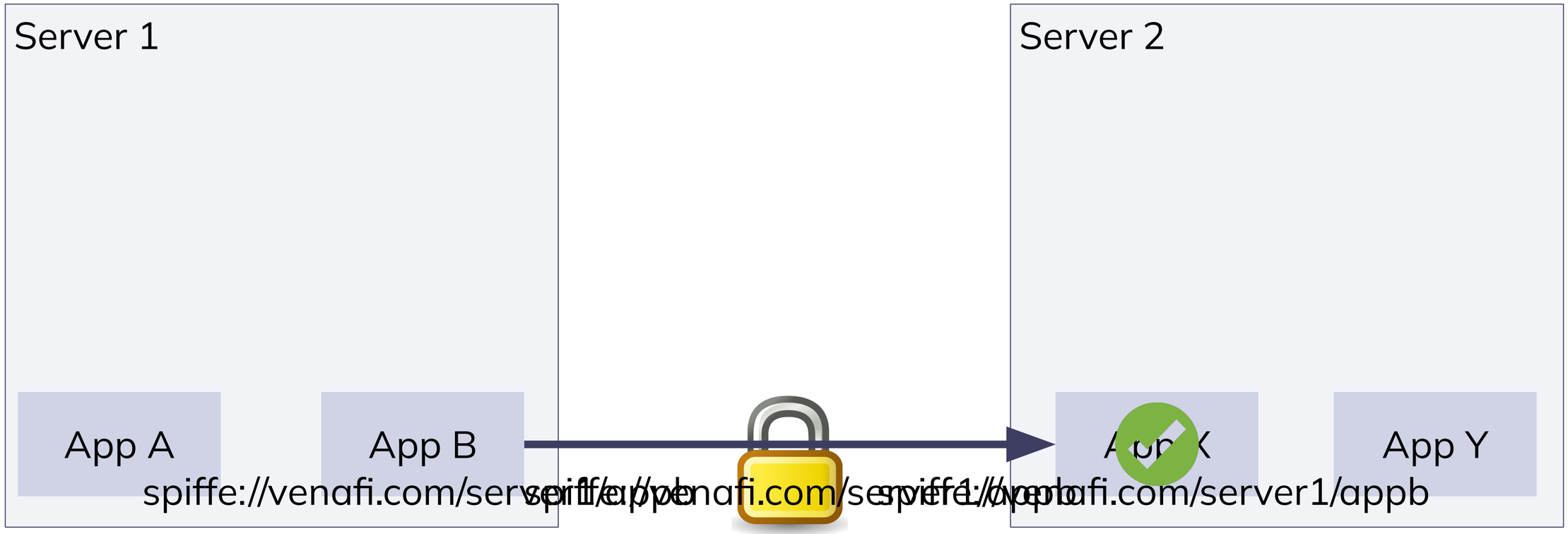
```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Payload:

```
{
  "spiffe_id": "spiffe://venafi.com/dc1/node10/frontend/webserver",
  "iss": "SPIFFE Intermediate CA",
  "sub": "dc1/node10/frontend/webserver",
  "aud": "https://api.example.com",
  "exp": 1679760000,
  "iat": 1679760000
}
```

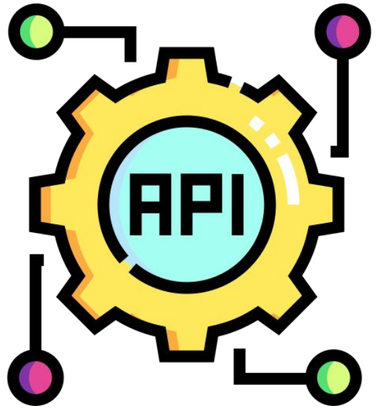
JWT Signature: <Digital Signature>

Application



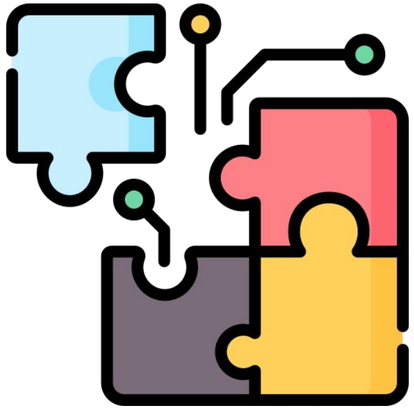
SPIFFE Workload API

SPIFFE Workload API



Request SPIFFE SVIDs

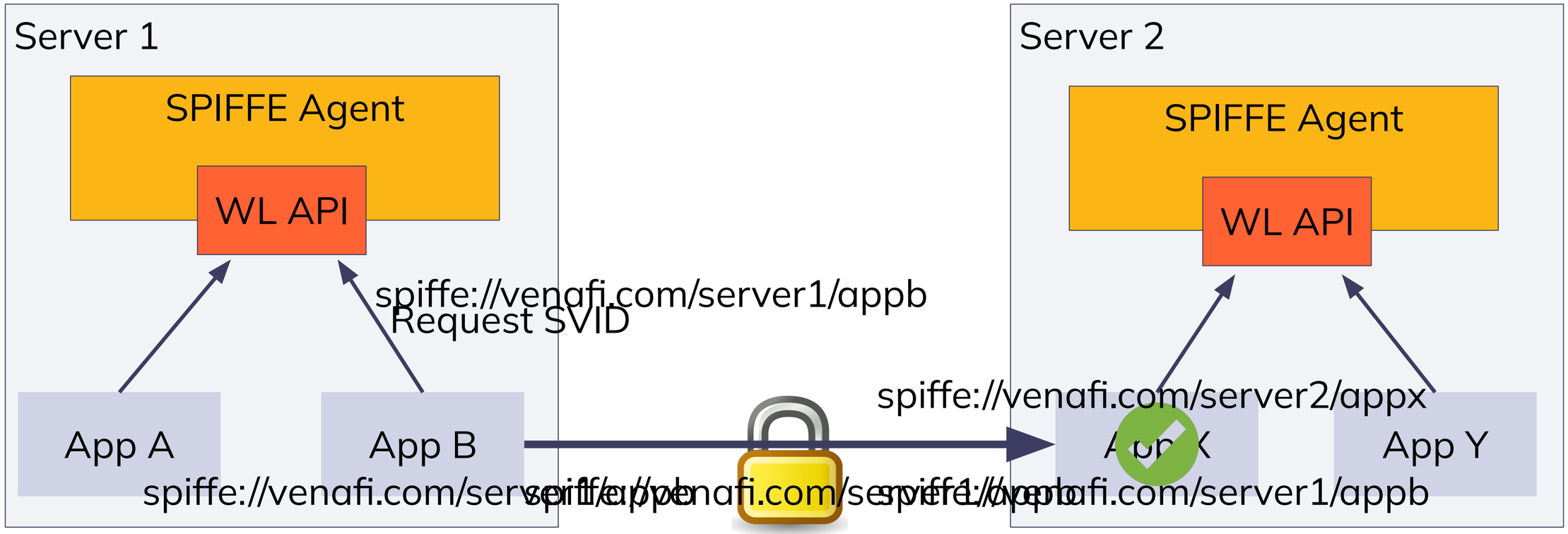
Automatic renewal & rotation



Platform Integration

Attestation & Validation

Application

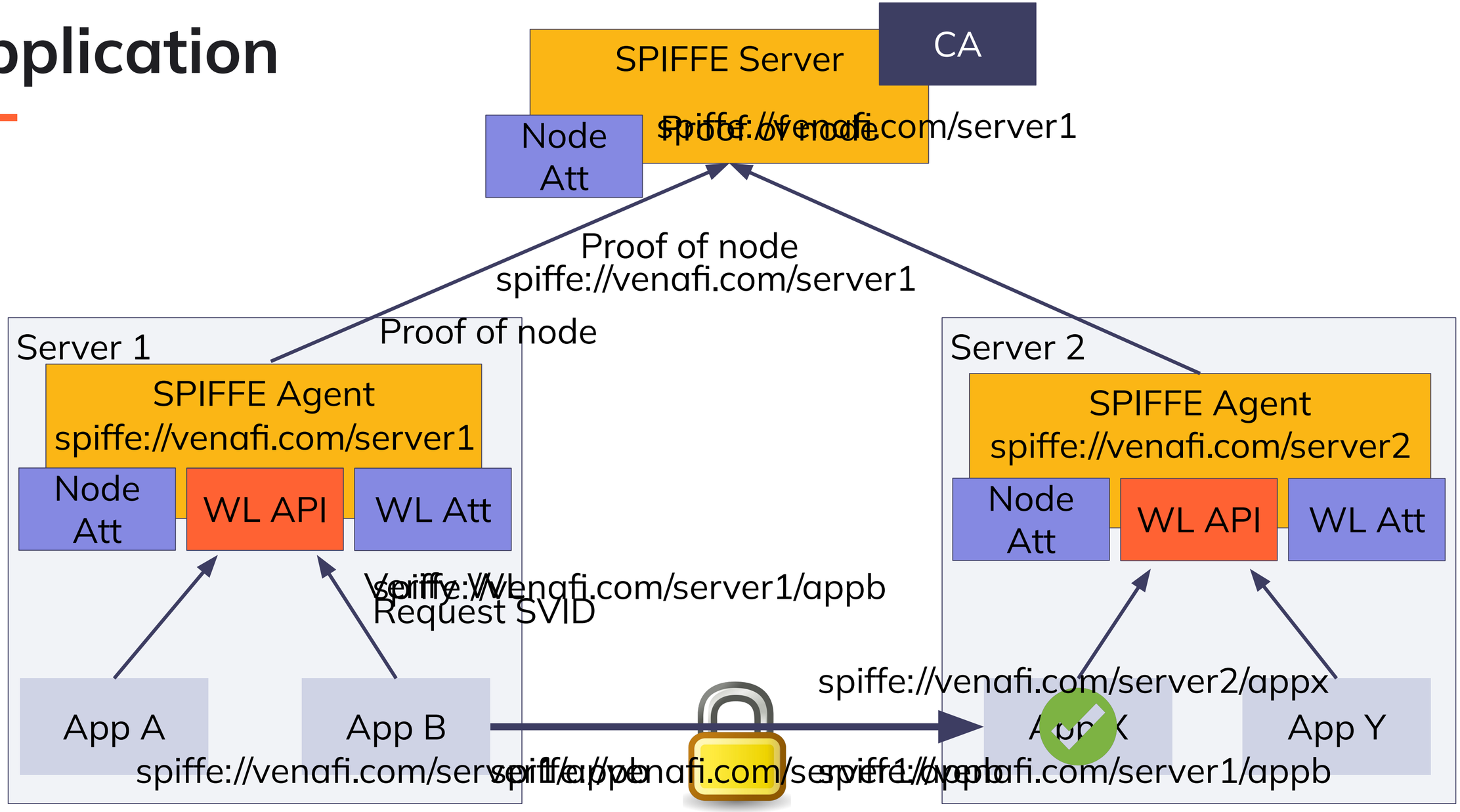


SPIFFE Workload Attestation

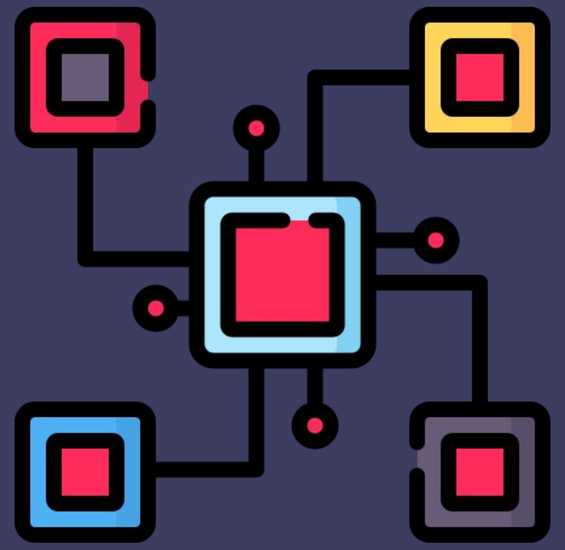
SPIFFE Workload Attestation

- Gather proof for the device
  - TPM
  - Cloud APIs
- Verify the device
- Gather proof for the workload
  - Kubernetes API
  - Unix socket
  - Windows
- Verify the workload

Application

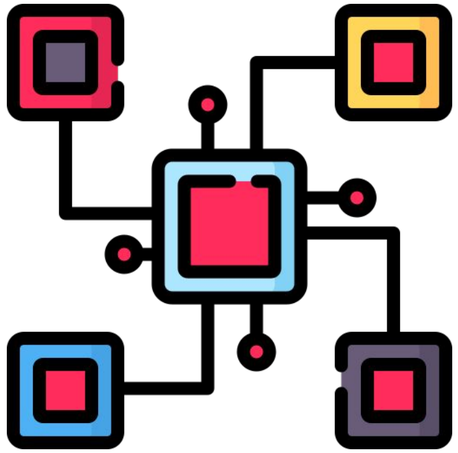


SPIFFE Federation



SPIFFE Federation

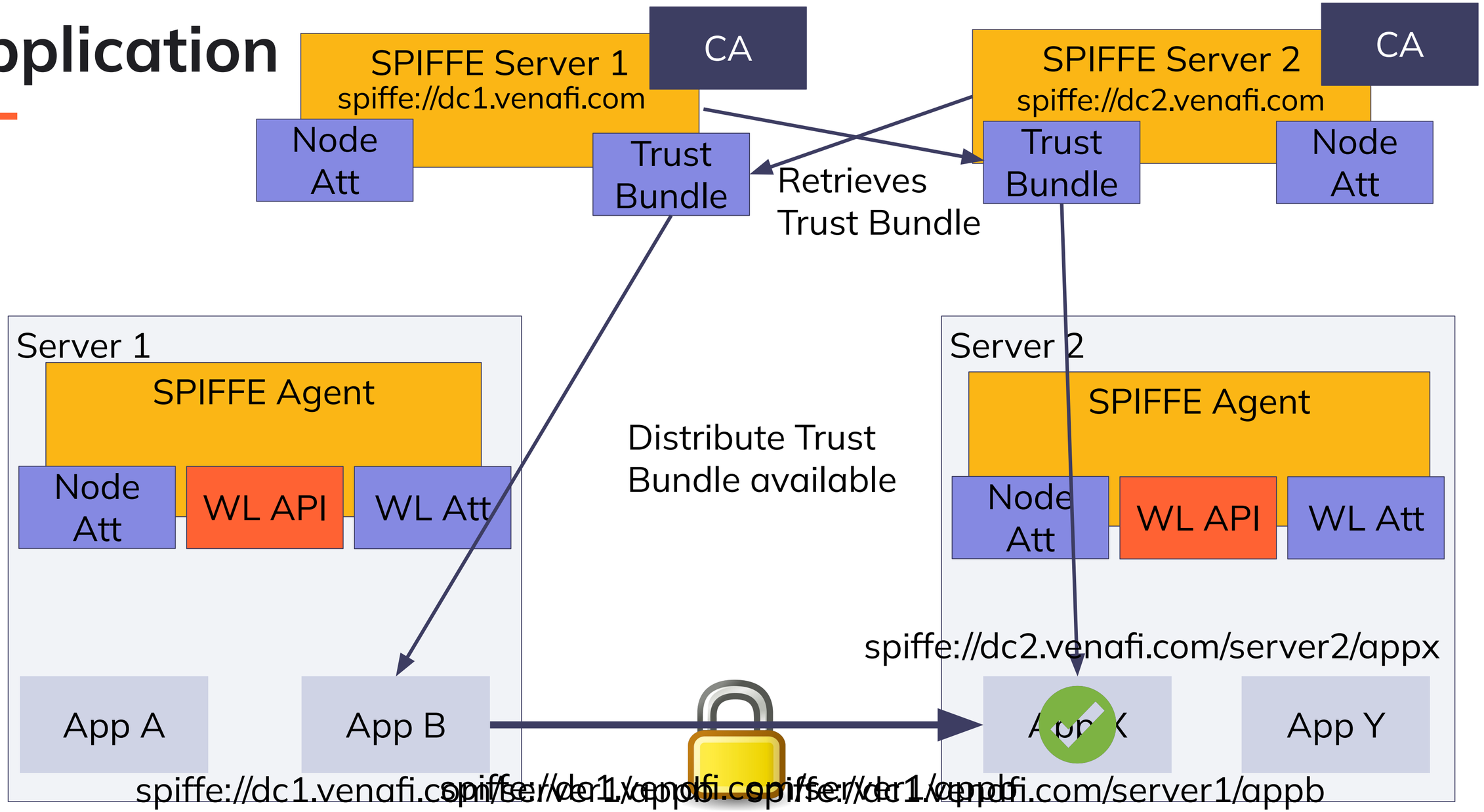
Trust Bundle



Distribution

Rotation

Application



Demo

SPIFFE and SPIRE are game changers. Managing shared secrets between microservices, and distributing TLS to hosts is a serious operational challenge for growing organizations like ours. It's a point of contention between our security and operations teams, and it detracts from other valuable security improvements. SPIFFE and SPIRE will simplify all of this for us.

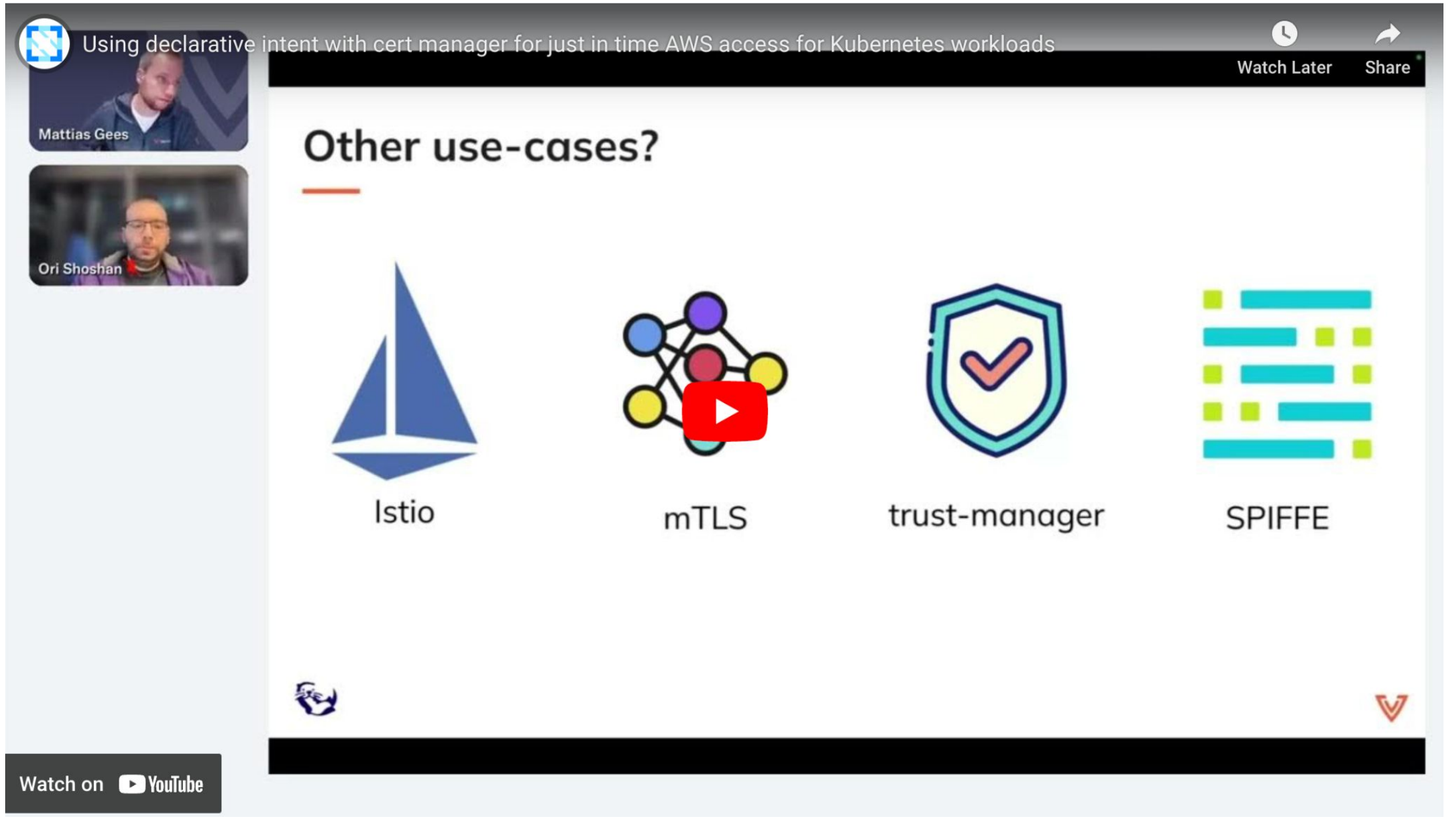
Jon Debonis - Head of Security / CISO Notable

Summary

- SPIFFE provides foundational identity
- Reduce need for API key distribution
- Short-lived identity that automatically gets renewed
- Out of band attestation
- Making lives easier for Developers
- SPIRE is an open-source implementation of SPIFFE

Implementation

https://tinyurl.com/cert-manager-aws



Thank you!

Reach out if you are interested in workload identity!

Mattias Gees
Director of Tech
@MattiasGees / mattias.gees@venafi.com