



KubeCon



CloudNativeCon

North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

Don't Mind the Gap



KubeCon



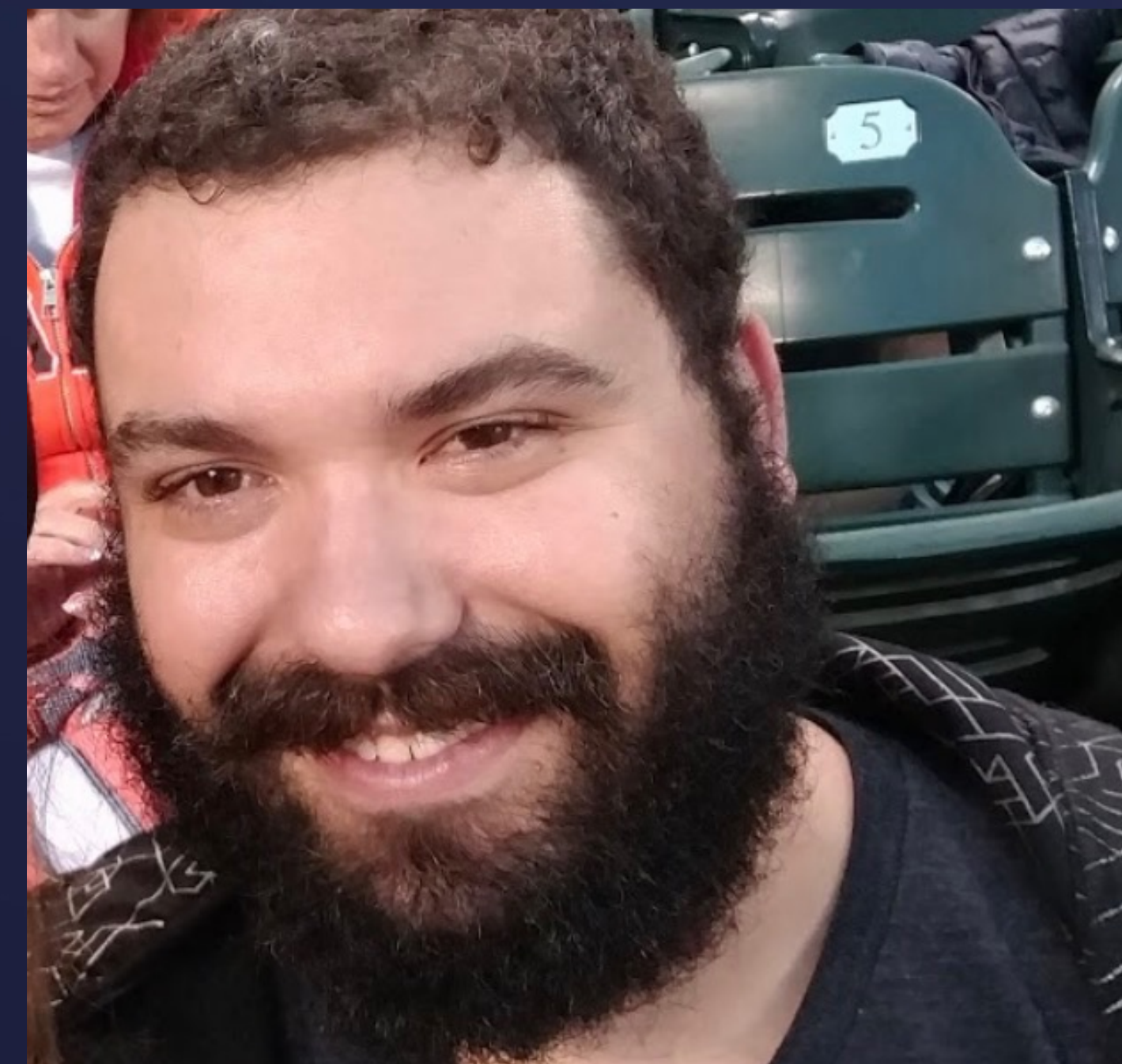
CloudNativeCon

North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022

October 24-28, 2021



Evan Gilman

@evan2645

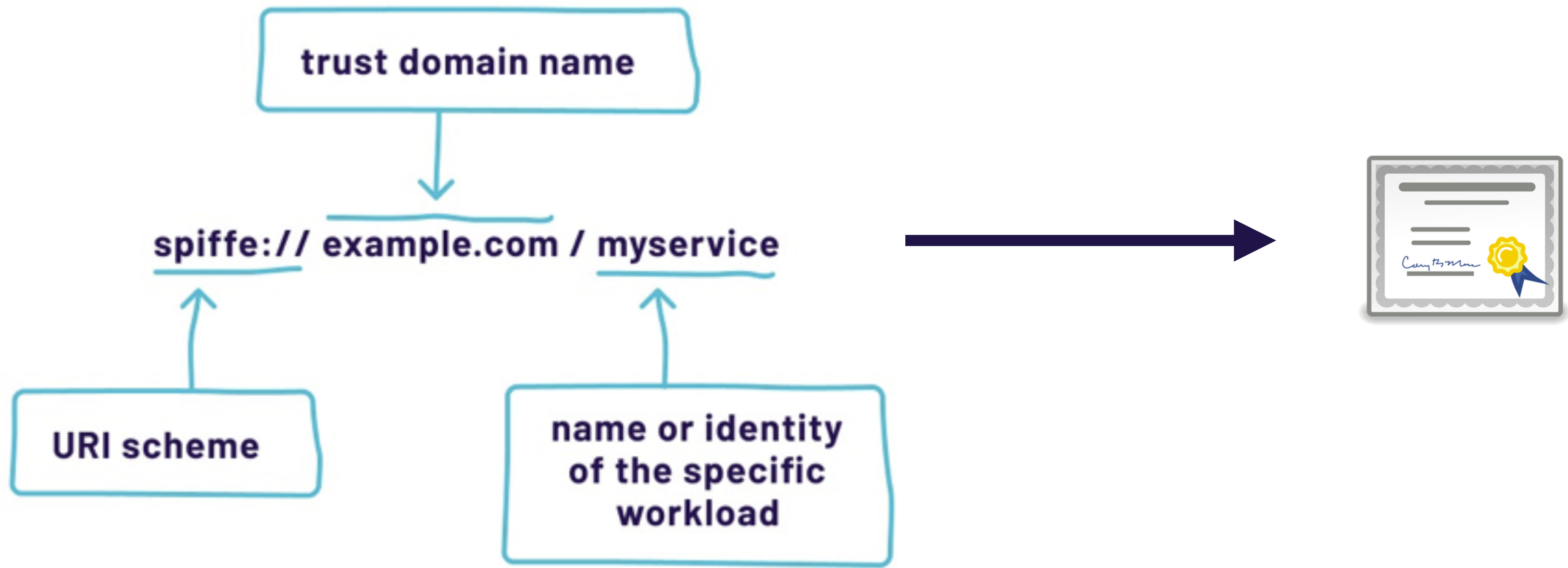
SPIFFE Basics (IDs, Bundles, Federation)

SPIRE Basics (Components, Registration)

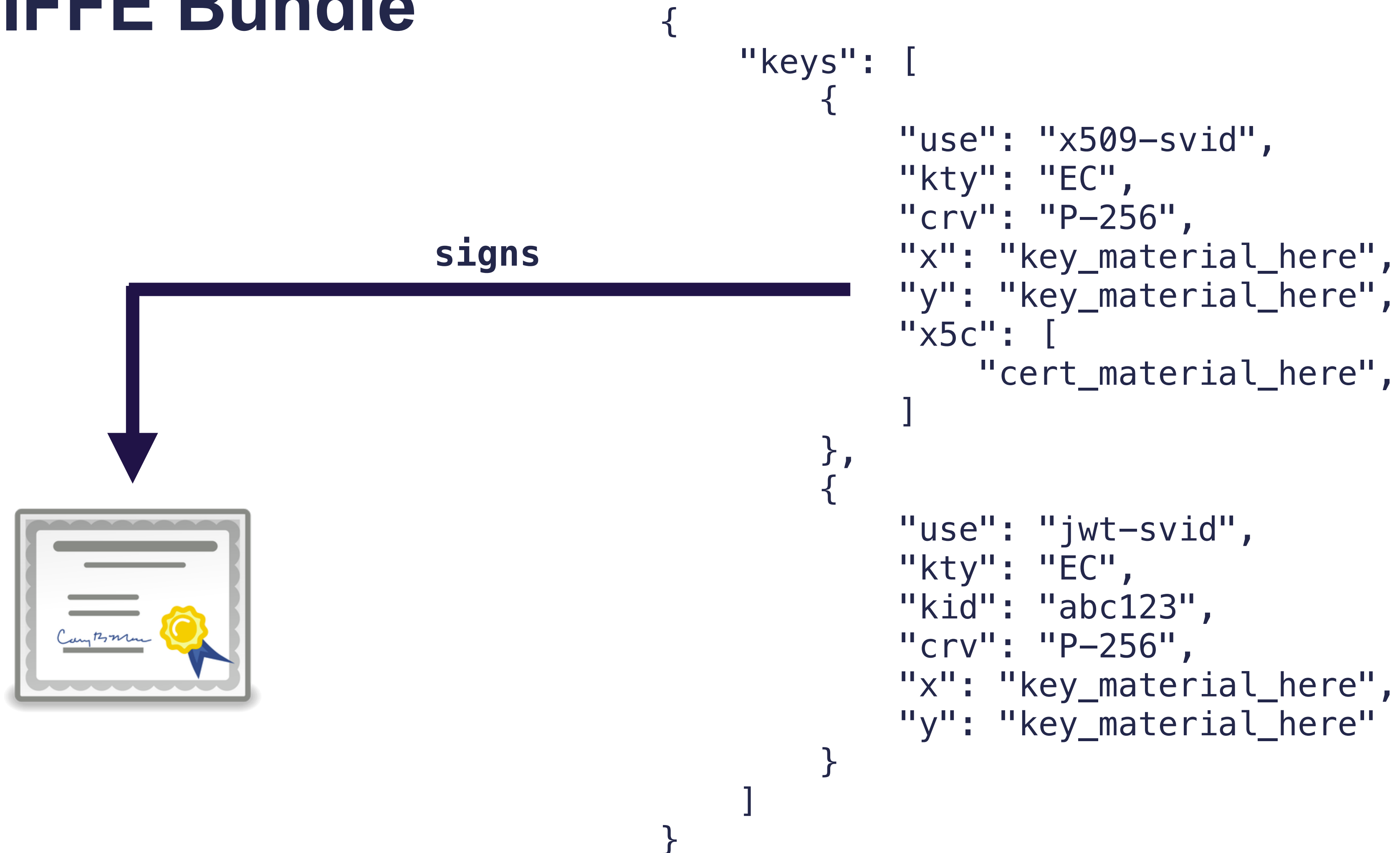
Auth to [AWS, Azure, GCP] w/ SPIRE

Q&A

The SPIFFE ID



The SPIFFE Bundle



SPIFFE Federation

`spiffe://example.com/foo`



`bundles["example.com"] => com_bundle_data`
`bundles["example.net"] => net_bundle_data`
`bundles["example.org"] => org_bundle_data`

`spiffe://example.net/bar`

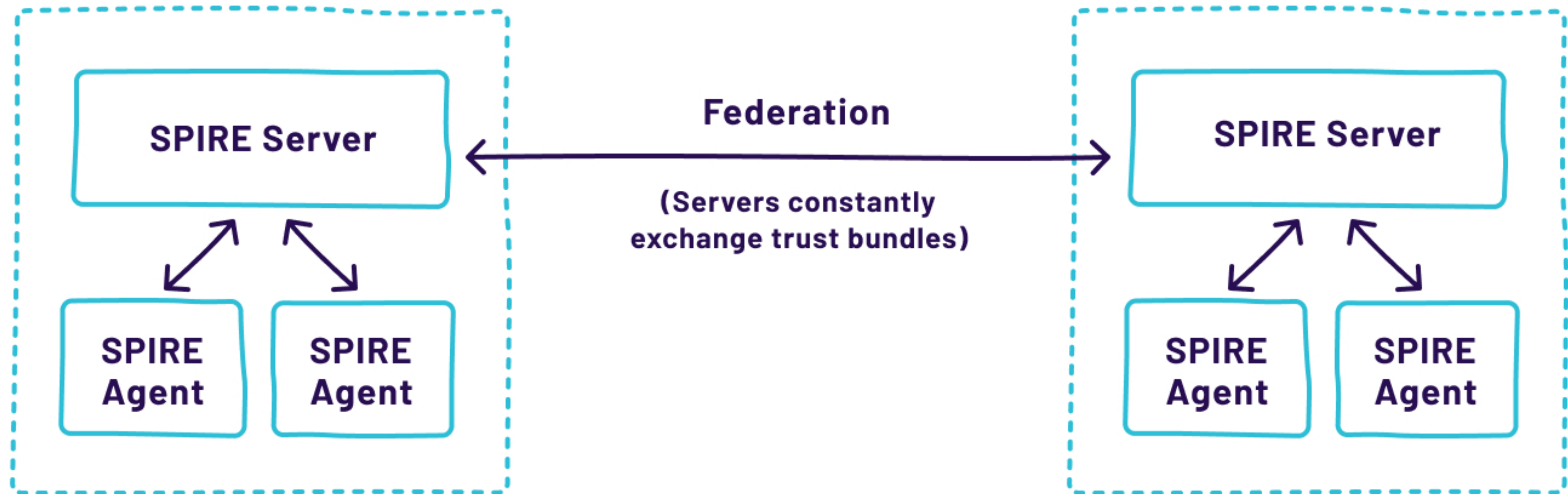


`spiffe://example.org/baz`



SPIRE

SPIRE Components



SPIRE Registration

Parent ID: `spiffe://example.org/k8s/cluster/foo`

Selector: `k8s:ns:backups`

Selector: `k8s:sa:uploader`

Selector: `docker:image-id:746b819f315e`

SPIFFE ID: `spiffe://example.org/backups/uploader`

SPIRE OIDC Discovery Provider

- Serves OIDC discovery doc
- Projects SPIFFE bundle
- Co-locate w/ agent or server
- Supports ACME

```
{
  "keys": [
    {
      "use": "x509-svid",
      "kty": "EC",
      "crv": "P-256",
      "x": "key_material_here",
      "y": "key_material_here",
      "x5c": [
        "cert_material_here",
      ]
    },
    {
      "use": "jwt-svid",
      "kty": "EC",
      "kid": "abc123",
      "crv": "P-256",
      "x": "key_material_here",
      "y": "key_material_here"
    }
  ]
}
```

SPIRE Federation w/ CSP

(OIDC Discovery Provider not pictured)



SPIFFE/SPIRE AuthN to AWS

Roles > spire-s3-test

Summary

Delete role

Role ARN	arn:aws:iam::XXXXXXXXXXXX:role/spire-s3-test
Role description	Edit
Instance Profile ARNs	
Path	/
Creation time	2020-03-21 17:05 PDT
Last activity	2020-03-21 18:42 PDT (Today)
Maximum CLI/API session duration	1 hour Edit

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities

arn:aws:iam::XXXXXXXXXXXX:oidc-provider/spire.example.com


Conditions

The following conditions define how and when trusted entities can assume the role.

Condition	Key	Value
StringEquals	spire.example.com:aud	spire
StringEquals	spire.example.com:sub	spiffe://example.com/s3-test-app

SPIFFE/SPIRE AuthN to AWS

 The Corner APIs Engineering Data Science All Posts

 Build on Square ›

AUGUST 26TH, 2021 | 8 MINUTE READ

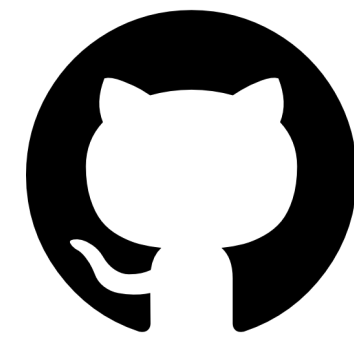
AWS OIDC Authentication with SPIFFE

Easy authentication with automated AWS credentials



As part of Square's migration to the cloud, we found that we needed an easy way for our datacenter applications to communicate with services in AWS. A majority of our applications are still in the datacenter and often use services in AWS such as SQS and S3. Our applications on AWS are split into separate

SPIFFE/SPIRE AuthN to AWS



square/spiffe-aws-assume-role

~/.aws/config

```
[default]
credential_process = spiffe-aws-assume-role credentials \
--sts-region us-west-2 \
--sts-endpoint https://sts.us-west-2.amazonaws.com \
--role-arn arn:aws:iam::123456789123:role/spiffe-oidc-test \
--spiffe-id spiffe://trustdomain.com/spiffe-oidc-test \
--audience 123456789123 \
--workload-socket unix:///agent.sock
```


Identity in the cloud

About

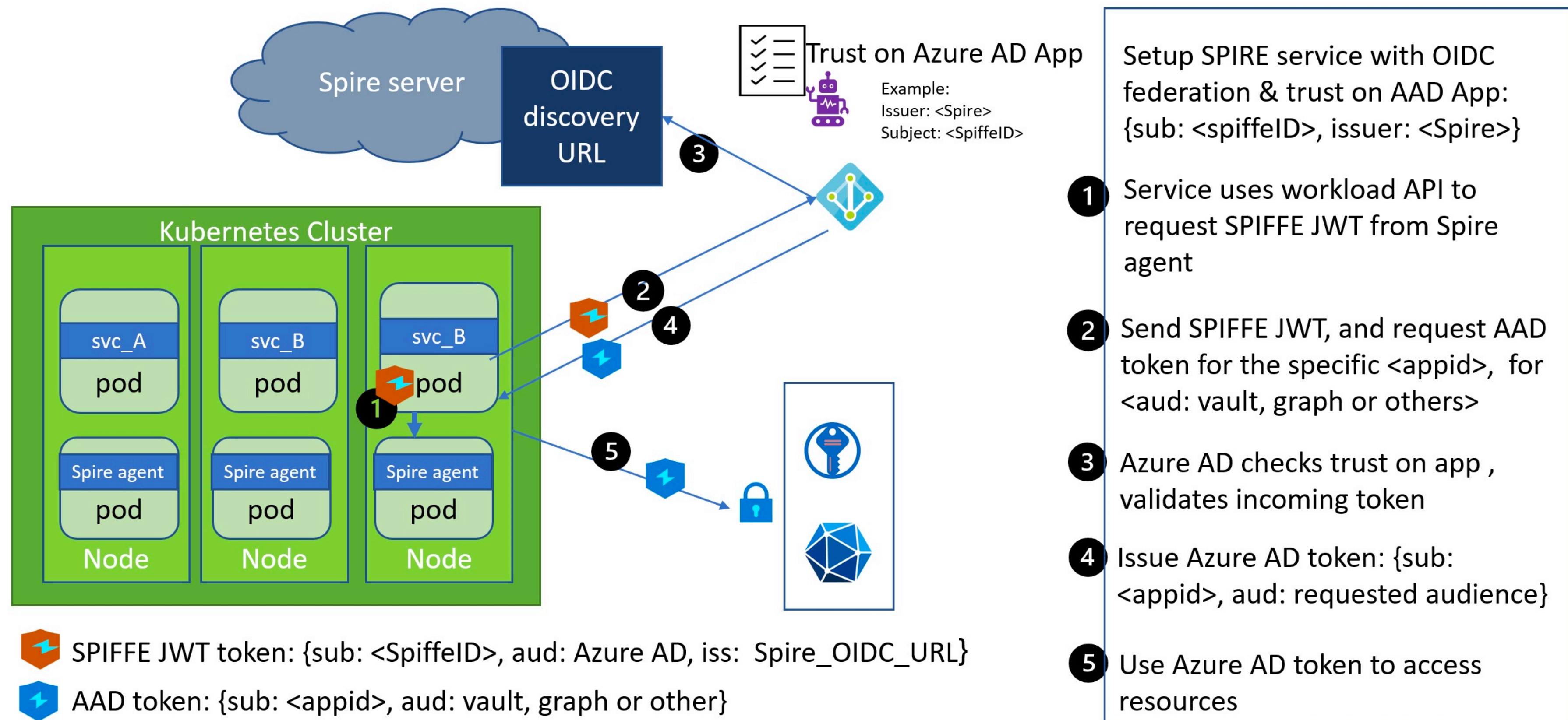
Azure AD workload identity federation with SPIFFE and SPIRE

Jan 14, 2022 • uday

SPIFFE is a set of open-source standards for providing identities to your software workloads. Since it is platform agnostic with possibilities such as mTLS, it is an attractive option for services deployed across platforms and cloud vendors. The [Kubernetes blog post](#) discussed how services running in a Kubernetes cluster can use Azure AD workload identity federation to access Azure resources without needing secrets. This blog post explores how services relying on SPIFFE can also use this capability to access Azure resources. No secrets are necessary.

SPIFFE/SPIRE AuthN to Azure

Azure AD tokens using SPIFFE JWT



SPIFFE/SPIRE AuthN to GCP



Christoph Grotz

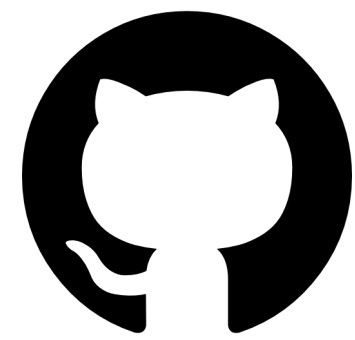
Apr 9 · 5 min read · [Listen](#)



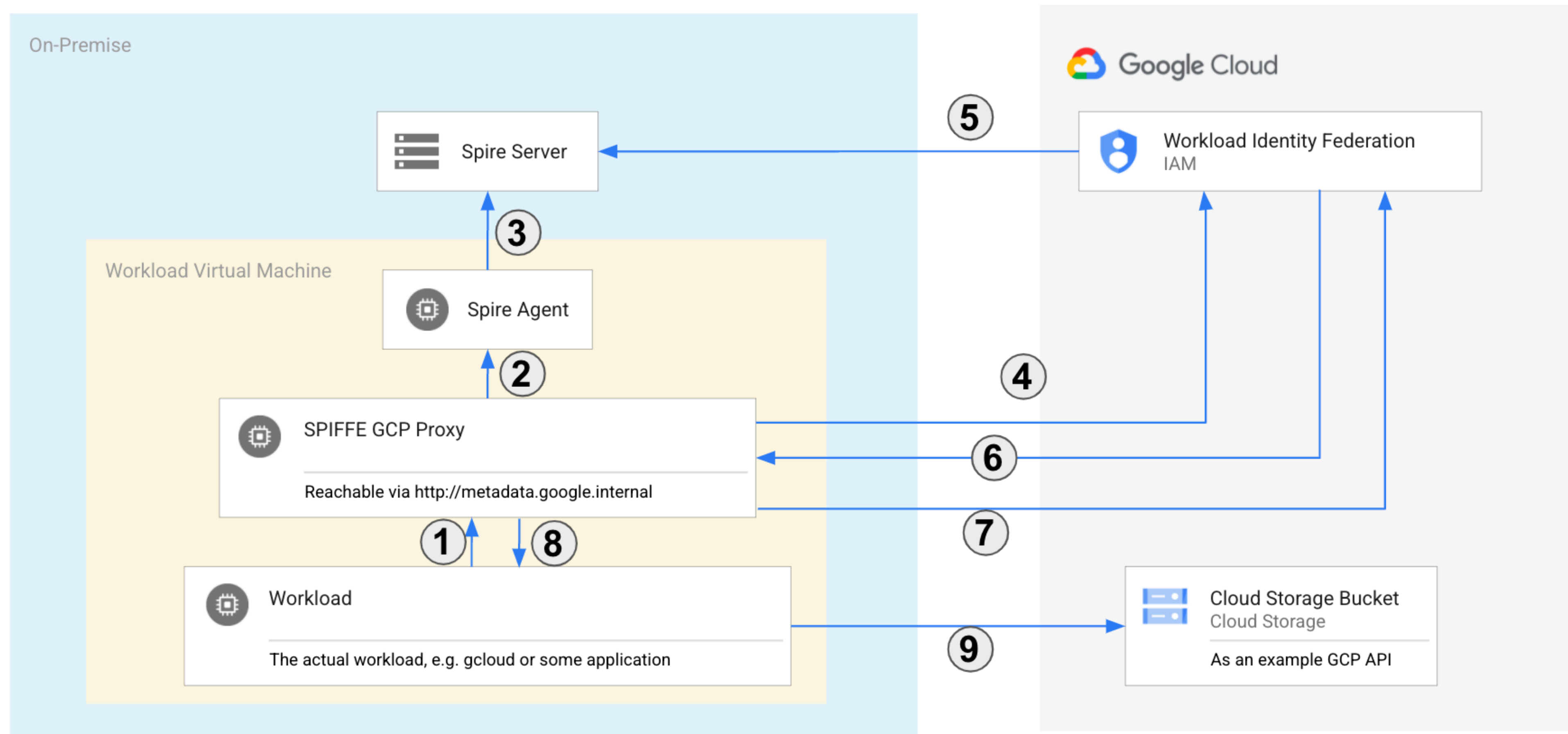
Workload Identity Federation for On-Premise Workloads with SPIFFE

Today I wanted to share a very cool project from the [CNCF](#) with you: Secure Production Identity Framework for Everyone (SPIFFE) is a universal identity control plane for distributed systems. I can highly recommend you watch the great [keynote](#) Kelsey Hightower gave at KubeCon two years ago, which gives a great overview over SPIFFE and what it's used for.

SPIFFE/SPIRE AuthN to GCP



GoogleCloudPlatform/professional-services



Key Takeaways

SPIFFE JWTs are OIDC-compatible

Many services/projects support OIDC-based authN

SPIFFE/SPIRE is platform agnostic and can run anywhere

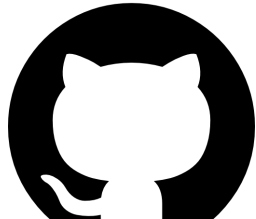
One weird trick to eliminate secrets and related mgmt

Learn More

 [spiffe/spire](#)

 [spiffe/spiffe](#)

 [slack.spiffe.io](#)

 [square/spiffe-aws-assume-role](#)

 [GoogleCloudPlatform/professional-services](#)





Please scan the QR Code above to
leave feedback on this session



KubeCon



CloudNativeCon

North America 2022

BUILDING FOR THE ROAD AHEAD

DETROIT 2022