



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

WIT Happens

Exploring the latest evolution of the SPIFFE
and WIMSE workload identity standards



Who are we?

Noah Stride 

Machine & Workload Identity

@ Teleport

Steering Committee & Maintainer

@ SPIFFE

Arndt Schwenkschuster

Software Engineer & Standards Architect

@ Defakto Security

Steering Committee & Maintainer

@ SPIFFE

OAuth, WIMSE member

@ IETF



KubeCon



CloudNativeCon

Europe 2026

A refresher on SPIFFE



What is SPIFFE?

*Secure **P**roduction **I**ntity **F**ramework **f**or **E**veryone*

“A set of open-source standards for securely identifying software systems in dynamic and heterogeneous environments.”

SPIFFE is a specification, not an implementation. SPIRE (CNCF) and implementations from vendors are available.

What does SPIFFE define?

Lots...

- SPIFFE ID
- SPIFFE Verifiable Identity Document (SVID)
 - X.509-SVID
 - JWT-SVID
- Trust Domain & Trust Bundle
- SPIFFE Workload API & Endpoint
- SPIFFE Federation
- ...

SPIFFE ID

How to encode/represent a workload's identity.

`spiffe://example.com/eu/payments/billing`

Trust domain: `example.com`

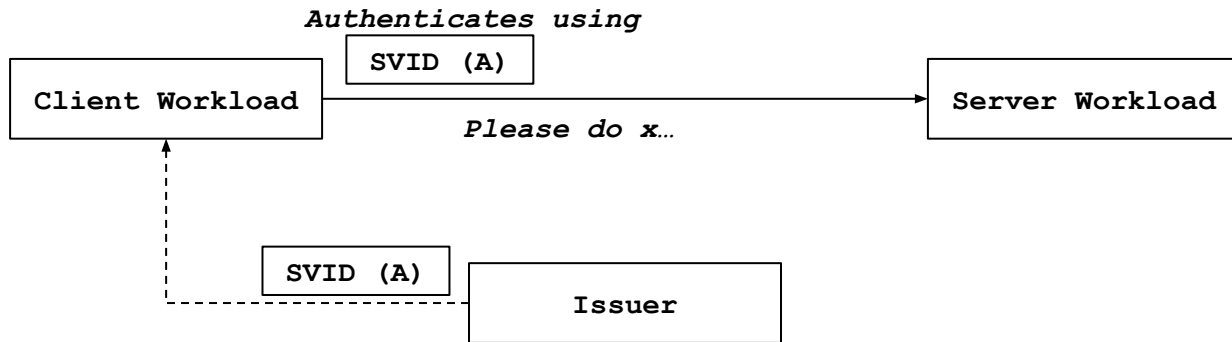
Workload Identifier: `/eu/payments/billing`

SPIFFE ID used for authz decisions and recorded for auditing.

SVID - SPIFFE Verifiable Identity Document

How to place the SPIFFE ID into a document which can be verified by others and used for authentication - a credential!

Currently, X.509-SVID and JWT-SVID...



Why?

Setting the foundation for interoperability between DIY, open-source and proprietary software that issue, consume and validate workload identity.

- Off-the-shelf SDKs
- Off-the-shelf tooling/services (Sidecars, Proxies etc.)
- Compatibility with CSP APIs (AWS, GCP, Azure)
- Reduced lock-in to specific issuer implementations
- A framework for federating trust across organizations.



KubeCon



CloudNativeCon

Europe 2026

WIMSE



WIMSE

- **W**orkload **I**ntity in **M**ulti **S**ystem **E**nvironments
- Working Group of the Internet Engineering Task Force (IETF)
- Established March 2024
- Benefits from related security standards & knowledge (OAuth, SCIM, PKIX, JWT, JOSE & more)
- Current charter
 - Architecture
 - Securing service-to-service traffic
 - Document existing Workload Identity Patterns



KubeCon



CloudNativeCon

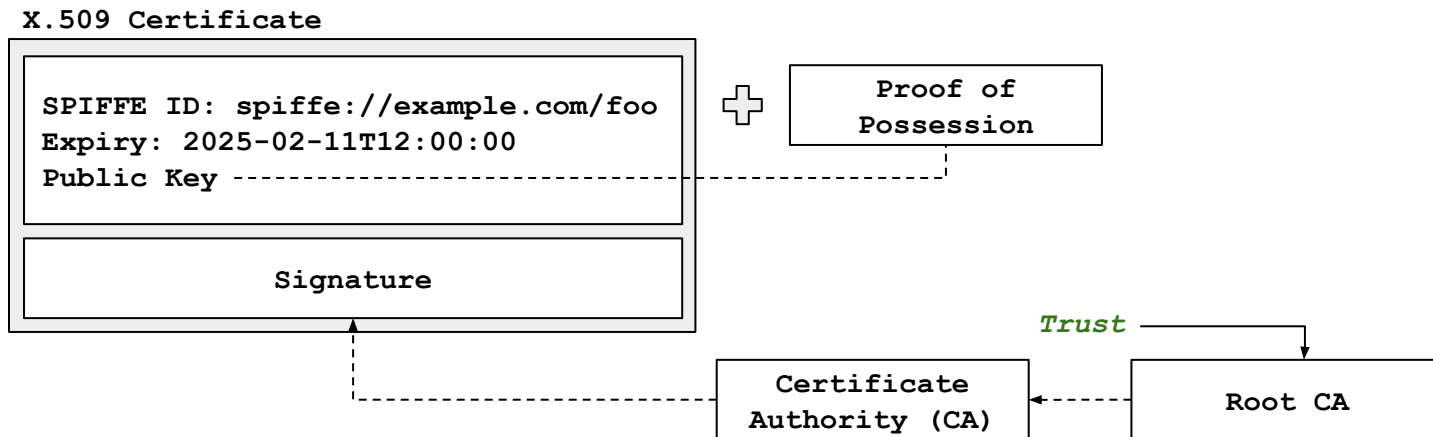
Europe 2026

JWT and X.509 SVID



X.509 SVID

- X.509 certificates bind identity attributes to a key pair.
- Certificate alone is not enough; we must prove we control the key - “proof of possession”.
- Validator trusts certificate because its signed by trusted certificate authority.



X.509 SVID: Example

-----BEGIN CERTIFICATE-----

```
MIID9zCCAt+gAwIBAgIRAJrDAUHUuP0efgncJAJ5Q+EwDQYJKoZIhvcNAQELBQAw
ajEaMBGGA1UEChMRbGVhZi50ZWx1Lm90dHIuc2gxGjAYBgNVBAMTEWx1YWYudGVs
ZS5vdHRyLnNoMTAwLgYDVQQFEyczMjxxOTYyMDc1Mjg4MDE2Nzg5Nzk4NTgyNDM3
NjY0NjM3MTMxNjgwHhcNMjYwMzAzMDk1MDExWhcNMjYwMzAzMTA1MTEeWjBDMRQw
EgYDVQQKEwsyMjYxNzQ4Mzg4MDErMCKGA1UEAxMic3RyaWRleW51dC93b3JrbG9h
ZC1pZGVudGl0eS1jaS1jZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AK6pG/M1fBl6JYwkPZLN5NiXoMFI2NI29jnYwY7xs4rG5Dplq+7oWHbMqFHSKrcF
eb77eyJqBCM4AhX0uG5ivnRXWdi3vqlDgzv29P2cE8e/fe72AP+TzOB+dtiP6kNS
j8uEPWcNKqSIRoJh4vpdBVsw64wLi7pq5raojCEV6JNv+7sprP+J1TRO6EDpDzO+
5PKnUQW0dodH9FswPzbp53HJnm3x5D4fVP4LFzL90vZJEqTk7e1OzIHaHGNvJ1W
V2LQsCICCbHn1JrTK4kiB+9u9vf7P+Tq7AURfw0GNYV/TT7SL25L81W+HOO56dNu
M3cgQWWHgVGZzUIe4fDrNVECAwEAAaOBvjCBuzAOBgNVHQ8BAf8EBAMCA6gWHQYD
VR0lBBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMCAwGA1UdEWEB/wQCMAAwHwYDVR0j
BBgwFoAUS90sNZrJbUnpDq144Qc1Ifqvi8wWwYDVR0RBfQwUoZQc3BpZmZlOi8v
bGVhZi50ZWx1Lm90dHIuc2gxGjYwMzAzMDk1MDExWhcNMjYwMzAzMTA1MTEeWjBDMRQw
bnRpdHktY2ktY2QvMjY2MTc0ODM4ODAwDQYJKoZIhvcNAQELBQADggEBAH5Nd7Gr
GLv0M3U9SDdeuCLQN1vN5JSTBfCmaAXxe/jBVbOm9yVP262kK4+yfHTpe6UhvN8
caq+8ylzJV3ciz3SIj1X3pY1kFUYOuvdGFs59uQJNHghKDDqZiyCubkspPUBYBIn
yIQm1Zml1P3keiHq01Nmd4S6zyKietDbJBoA/JIF8KJLEzyI5/kmlGg7fmlaTz2V
WfJ6PhLcOwm6xXUulYLP5FG9HCeolmyTul4QKbo2TfhkMpa1PSNCmV35xPAZk01+
6118NpGH1Qy5MEq9eJgZ2pJ/ODz3Cf4sPpxC7yS2KrYpKtyAPLocLZ0Gx17D16Qy
pzi+847I3ERn5Rw=
```

-----END CERTIFICATE-----

X.509 SVID: Example

Data:

Version: 3 (0x2)

Serial Number: dd:48:ec:d4:a4:c6:b2:ea:8e:9b:54:35:e8:30:65:7b

Signature Algorithm: ecdsa-with-SHA256

Issuer: C=US, O=SPIFFE, serialNumber=6968729192859147614695638370388029008

Validity

Not Before: May 16 11:26:11 2025 GMT

Not After : May 16 12:26:21 2025 GMT

Subject: C=US, O=SPIRE

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey | Public-Key: (256 bit) | Pub: -snip-

X509v3 extensions:

Key Usage: critical - Digital Signature, Key Encipherment, Key Agreement

Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication

Basic Constraints: critical - CA:FALSE

Subject Alternative Name: URI:spiffe://example.org/my-workload

Signature Algorithm: ecdsa-with-SHA256

Signature Value: -snip-

X.509 SVID: Usage

Typically used with TLS (client certificate, host certificate, both - mTLS).

TLS provides strong security fundamentals:

- Workloads do not “expose” a secret to use their certificate (vs bearer token)
- Confidentiality (encryption)
- Integrity

X.509 SVID: Pros and Cons

Pros:

- Based on mature “battle-tested” technologies: X.509 & TLS.
- TLS provides great security properties.

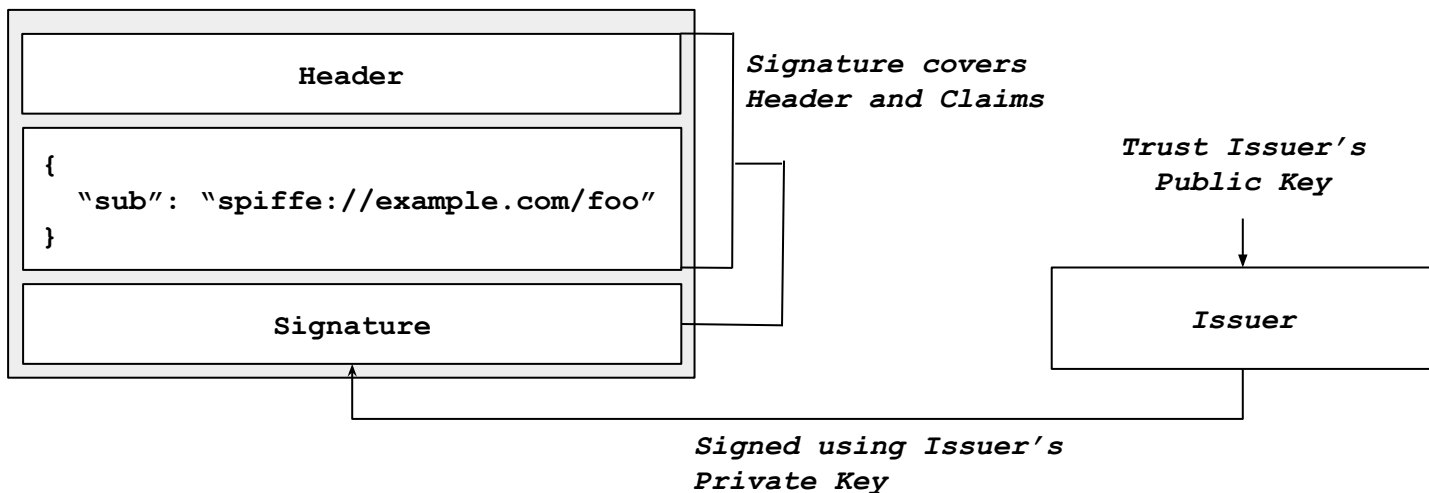
Cons:

- TLS termination (in LBs/Proxies) makes client cert authn tricky.
- Support for client cert authn in off-the-shelf software can be limited.
- X.509 and ASN.1 are complex and difficult to work with.

JWT SVID

JSON Web Token.

Set of claims (JSON object) signed by an issuer.



JWT SVID: Example

eyJhbGciOiJSUzI1NiIsImtpZCI6IlVrcllBTvgyOW5vM0x1Sy03bkNOVFllZ1hnUm1Hazh
weThhLTFjRXpla2siLCJ0eXAiOiJKV1QiLCJ0eXkiOiJleGFtcGxlIiwiaWV4cCI6
MTc3MjUzNTA3MSwiaWF0IjoxNzcyNTMxNDcxLCJpc3MiOiJodHRwczovL2xlYWYudG
VsZS5vdHRyLnNoL3dvcmts2FkLWlkZW50aXR5IiwianRpljoiNDIyNDliMjM1MzdlZGJk
MTVmOGJjM2ZmZTUzMTRmZTliLCJvcmlnaW5hbF9yZXBvc2l0b3J5Ijoic3RyaWRleW5
ldC93b3JrbG9hZC1pZGVudGI0eS1jaS1jZCIsInN1Yil6InNwaWZmZTovL2xlYWYudGVs
ZS5vdHRyLnNoL2dpdGh1Yi9zdHJpZGV5bmV0L3dvcmts2FkLWlkZW50aXR5LWNpL
WNkLzlyNjE3NDgzODgwIn0.GLO9H4UaN3SAGg5AYGu0Pdwsnw9oe7v1C1G9bRZjLa
yAgY0Ald1dlpwO-ySD4FMpAK3-s_pgGeBc0mHk7MPSdsuo7bVBLV-2iLCXbEih63Gcct
1DIJ1QWthposuLScu27-SC5y6nafl-KGqw6HDSdT1dQdqul2OtAlaVM9CJNkBJRYAaa
X4TYrXN76TFvIRKu1stnNx8NwHqhJetSutggeCfVcdstGv7W4qmm0AiUBojXxoRpcKRI
PRmL94ARyz5uyphqiNtAqRiHqp4X9fAJgU879qfeJWc5ZI1IDJLp0TfFqORTI5EiH6ztIMh
Pzmdgmg2R4TwpcJ2WUuAUvVFmg



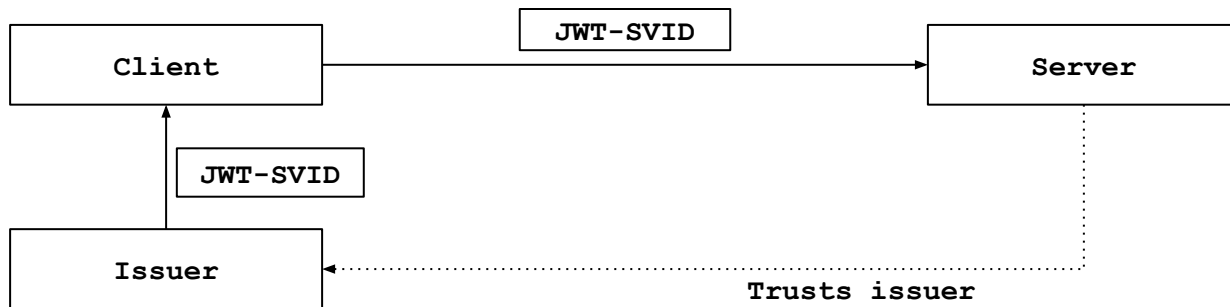
JWT SVID: Example

```
{  
  "alg": "RS256",  
  "kid": "UkrYAMX29no3LuK-7nCNTYHgXgRmGk8py8a-1cEzekk",  
  "typ": "JWT"  
}. {  
  "aud": "example.com",  
  "exp": 1772535071,  
  "iat": 1772531471,  
  "iss": "https://example.com",  
  "jti": "42249b23537edbd15f8bc3ffe5314fe2",  
  "sub": "spiffe://example.com/k8s/payments/billing"  
}. [signature]
```

JWT SVID: Usage

Bearer Token: To use it, we just need to “present” it. Unlike the X.509 certificate, possession of the token alone is enough.

Typically presented in headers - i.e in HTTP “Authorization” header.



JWT SVID: Pros and Cons

Pros:

- Simple - easily used with most transport protocols and infrastructure.
- Compatible with OpenID Connect ID Tokens - wide platform support.

Cons:

- Bearer token - weak security model that is prone to reuse attacks.



KubeCon



CloudNativeCon

Europe 2026

The WIT SVID



Introducing: WIT SVID

Workload Identity Token - defined by WIMSE IETF Working Group

-> SPIFFE WIT-SVID

JOSE-based token to protect a single hop in a call chain with cryptographic binding to the caller's identity.

Prior art / influenced by:

- Existing SVIDs (X.509, JWT)
- "cnf" claim - RFC 7800
- OAuth2 DPoP - RFC 9449

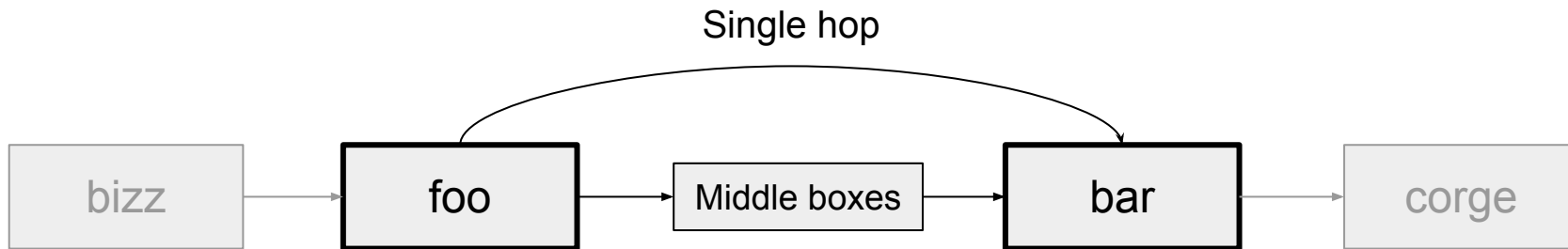
WIT SVID

JOSE-based token to protect a single hop in a call chain with cryptographic binding to the caller's identity.

```
{
  "alg": "ES256",
  "typ": "wimse-id+jwt",
  "kid": "July 4"
}.{
  "iss": "https://example.com/trusted-central-authority",
  "sub": "wimse://example.com/specific-workload",
  "exp": 1717612470,
  "jti": "x-_1CTL2cca3CSE4cwb__",
  "cnf": {
    "jwk": {
      "kty": "OKP",
      "alg": "EdDSA",
      "crv": "Ed25519",
      "x": "1CXXvf1N_LVVsIsYXsUvB03JmlGWeCHqQVuouCF92bg"
    }
  }
}.[Signature]
```

WIT SVID

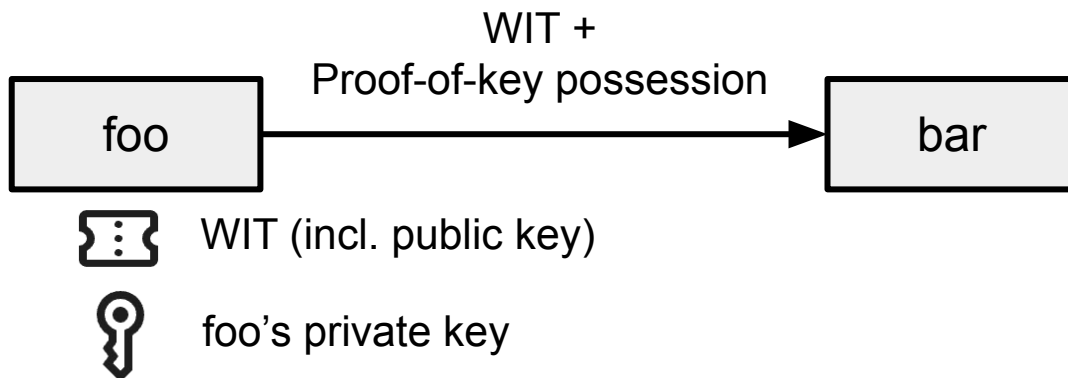
JOSE-based token to protect a single hop in a call chain with cryptographic binding to the caller's identity.



Middle boxes: API-Gateways, Load Balancers, TLS-terminating proxies, ingress controllers, ...

WIT SVID

JOSE-based token to protect a single hop in a call chain with cryptographic binding to the caller's identity.



WIT SVID: Pros and Cons

Pros:

- Key-bound credential
 - requires proof-of-key possession
 - not a Bearer token
- Well-established JWT format

Cons:

- Upcoming standard
- Little adoption, limited SDK support (but not for long)



KubeCon



CloudNativeCon

Europe 2026

Demo



What's next...

Standard procedures

- [Workload Identity Tokens](#) are on their path to become an RFC.
- [WIT-SVIDs](#) to become part of the stable SPIFFE standard. Currently in preview.

Adoption

- SDK support & examples

Interested in learning more? Come visit us in the Project Pavilion this afternoon or join our slack community!