
KubeCon
CloudNativeCon
North America 2024

KubeCon | CloudNativeCon

North America 2024

SPIRE: Intro & In-Depth Exploration of the Forced Rotation and Revocation Feature

Marcos Yacob, HPE

Agustín Martínez Fayó, HPE

Agenda

Introduction to SPIRE

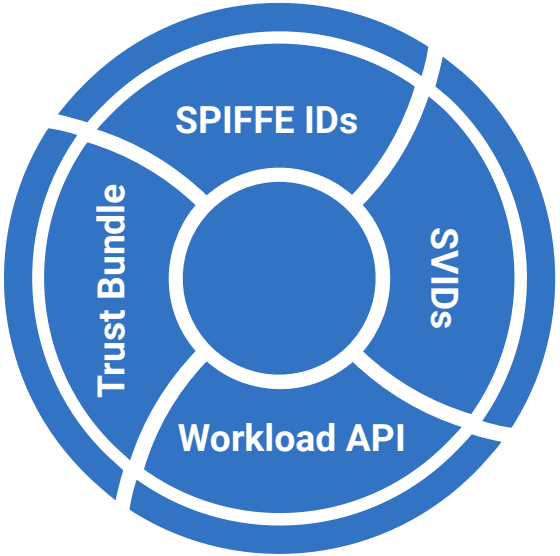
- SPIFFE Overview
- SPIRE In a Nutshell

Forced Rotation of Signing Keys

- X.509 and JWT Signing Keys
- Lifecycle of Signing Keys
- Force the Rotation of a Key
- Demo!

SPIFFE Overview

- Defines a framework and a set of standards for identifying and securing communications between workloads
  - How services identify themselves to each other
  - Encoding SPIFFE IDs in a cryptographically-verifiable document
  - An API specification for issuing and retrieving SVIDs
  - A format for representing the collection of public keys in use by a given SPIFFE issuing authority

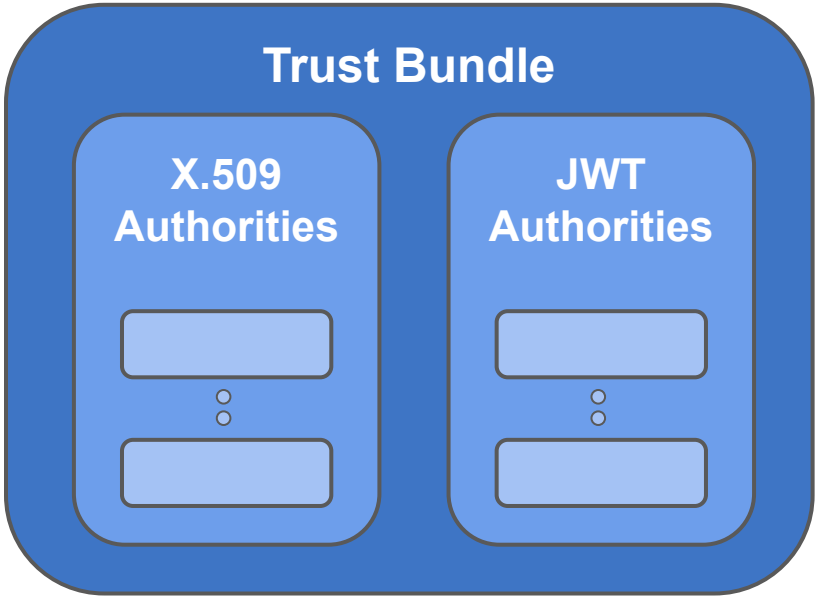


SPIRE In a Nutshell

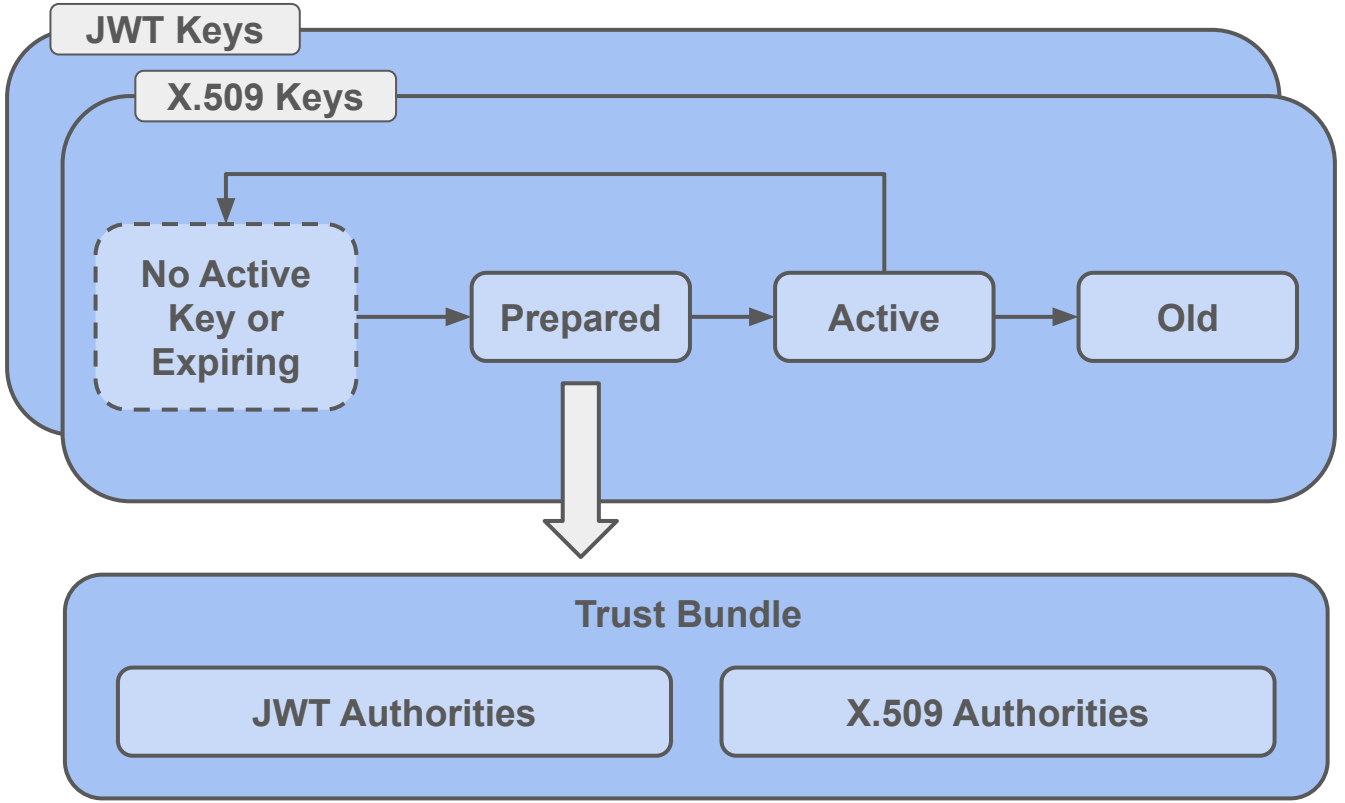
- Implementation of the SPIFFE standards
- Performs node and workload attestation
- Two major components
  - SPIRE Server
    - Authenticate agents and mint SVIDs
  - SPIRE Agent
    - Serve the SPIFFE Workload API

SPIRE - Signing Keys

- Signing Keys are managed by SPIRE Server
  - X.509 Signing Keys
    - SPIRE Server X509-SVID
    - SPIRE Agent X509-SVID
    - Workload X509-SVIDs
  - JWT Signing Keys
    - Workload JWT-SVIDs

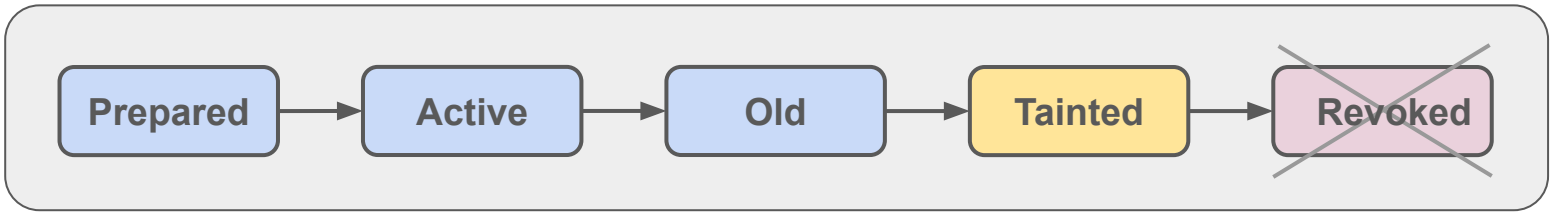


SPIRE - Lifecycle of Signing Keys



SPIRE - Force the Rotation of a Key

- Current active keys can be forced to be rotated
- Steps to taint and revoke a key
  a. Prepare a new key if needed
  b. Activate the prepared key
  c. Taint the old key
  d. Revoke the tainted key

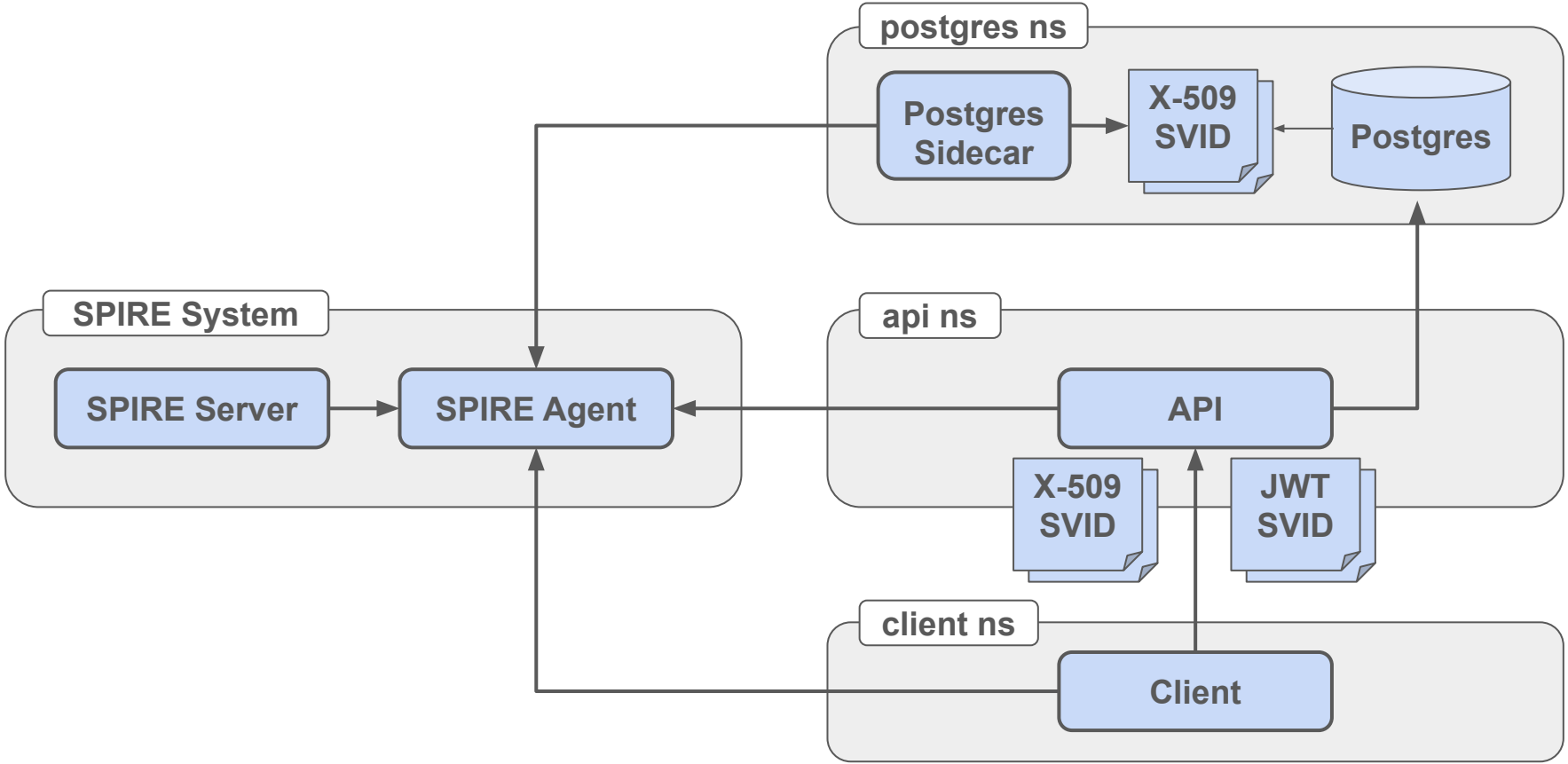


SPIRE - Force the Rotation of a Key

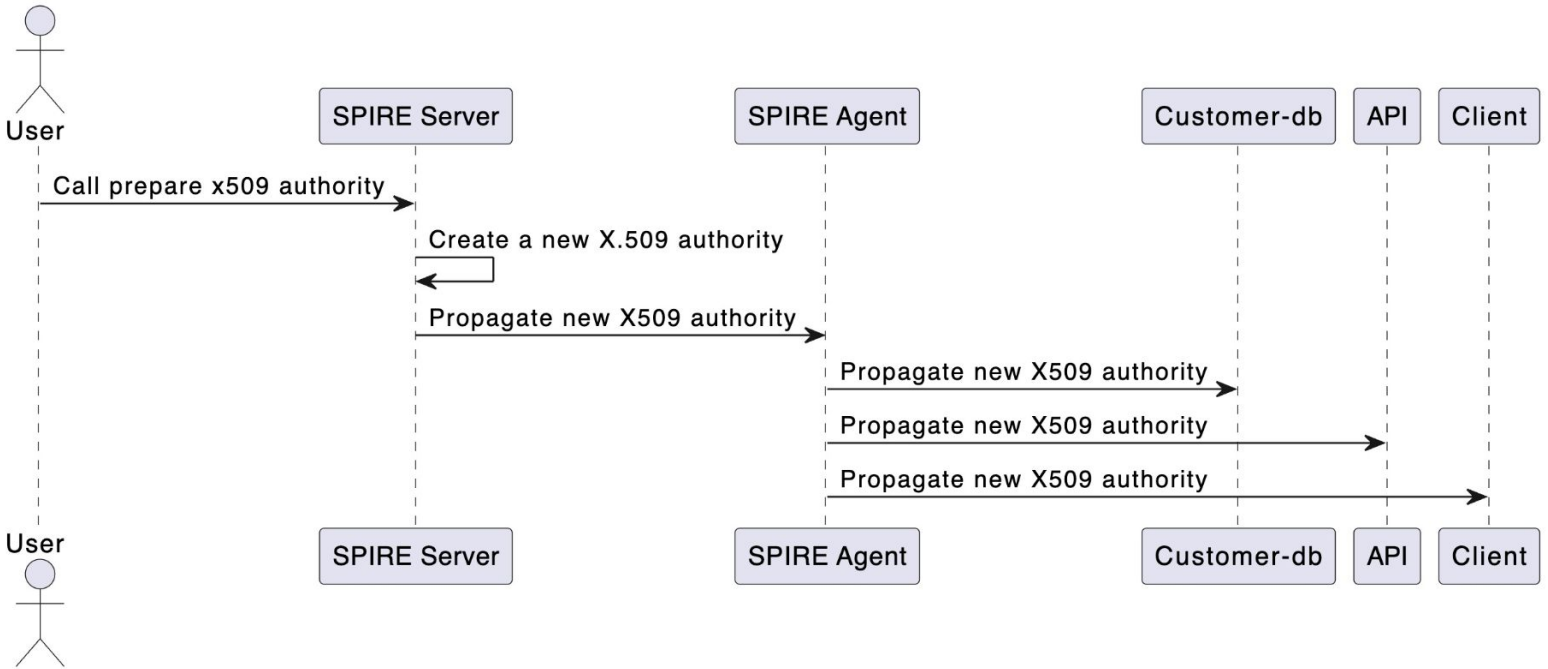
- LocalAuthority Server API
  - GetX509AuthorityState
  - PrepareX509Authority
  - ActivateX509Authority
  - TaintX509Authority
  - TaintX509UpstreamAuthority
  - RevokeX509Authority
  - RevokeX509UpstreamAuthority
  - GetJWTAuthorityState
  - PrepareJWTAuthority
  - ActivateJWTAuthority
  - TaintJWTAuthority
  - RevokeJWTAuthority

- Server CLI commands
  - localauthority and upstreamauthority commands

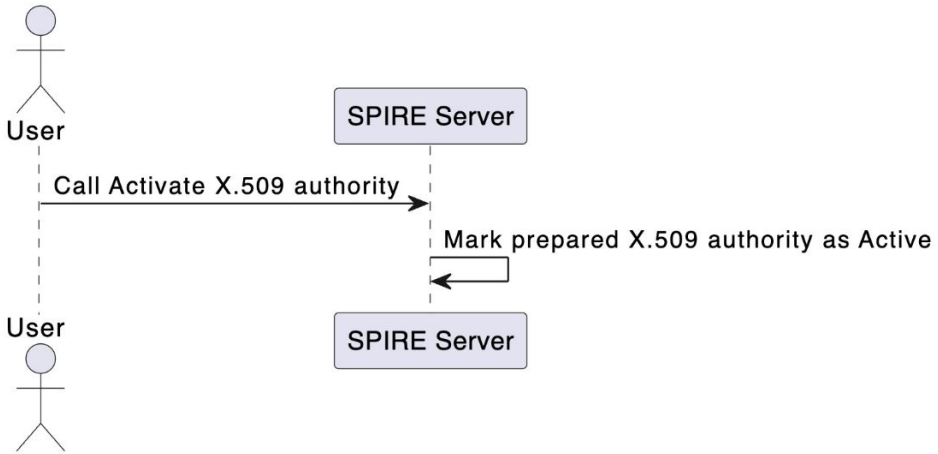
Demo


postgres ns
Postgres Sidecar
X-509 SVID
Postgres
SPIRE System
SPIRE Server
SPIRE Agent
api ns
API
X-509 SVID
JWT SVID
client ns
Client

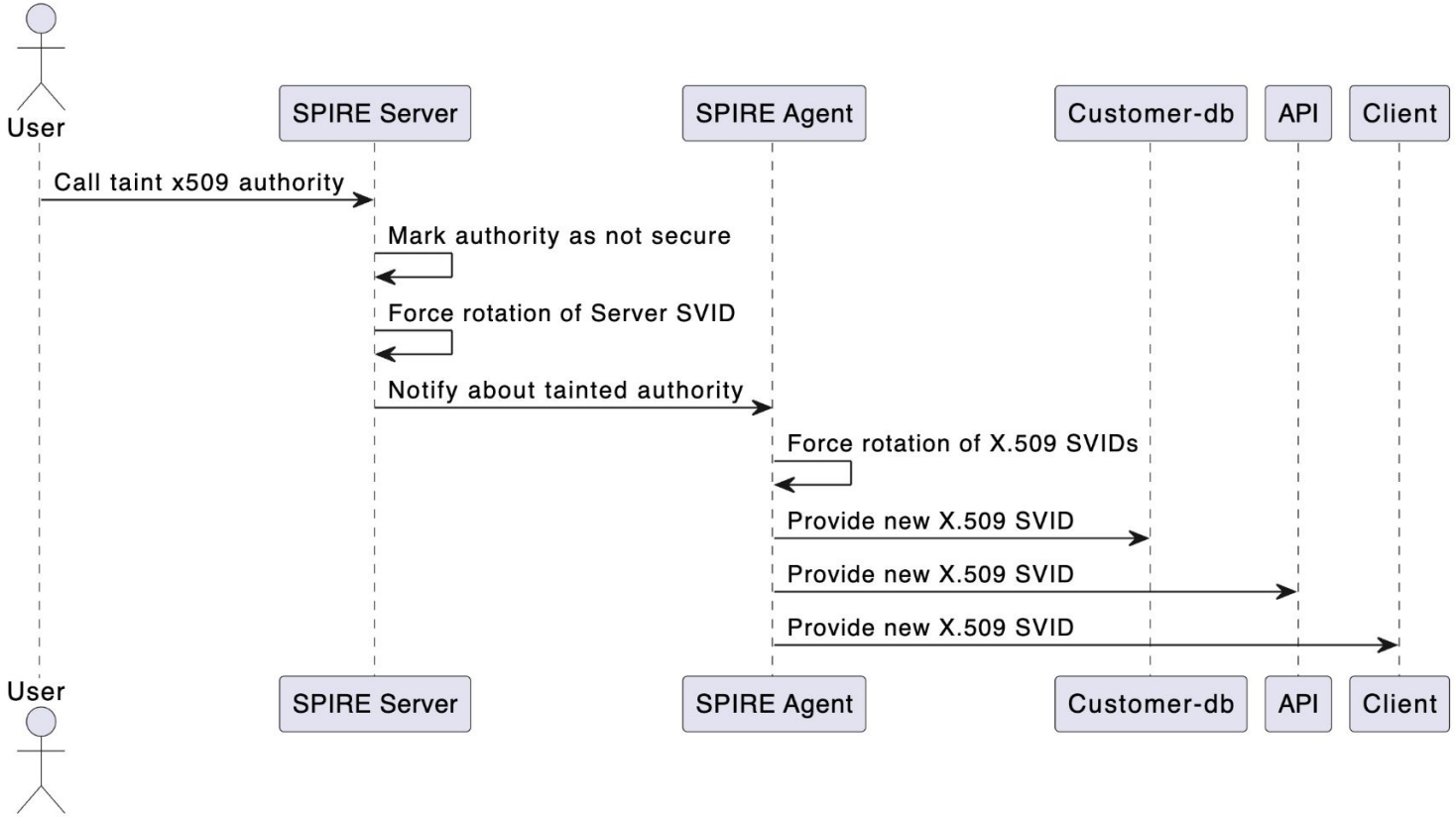
Prepare X.509 Authority



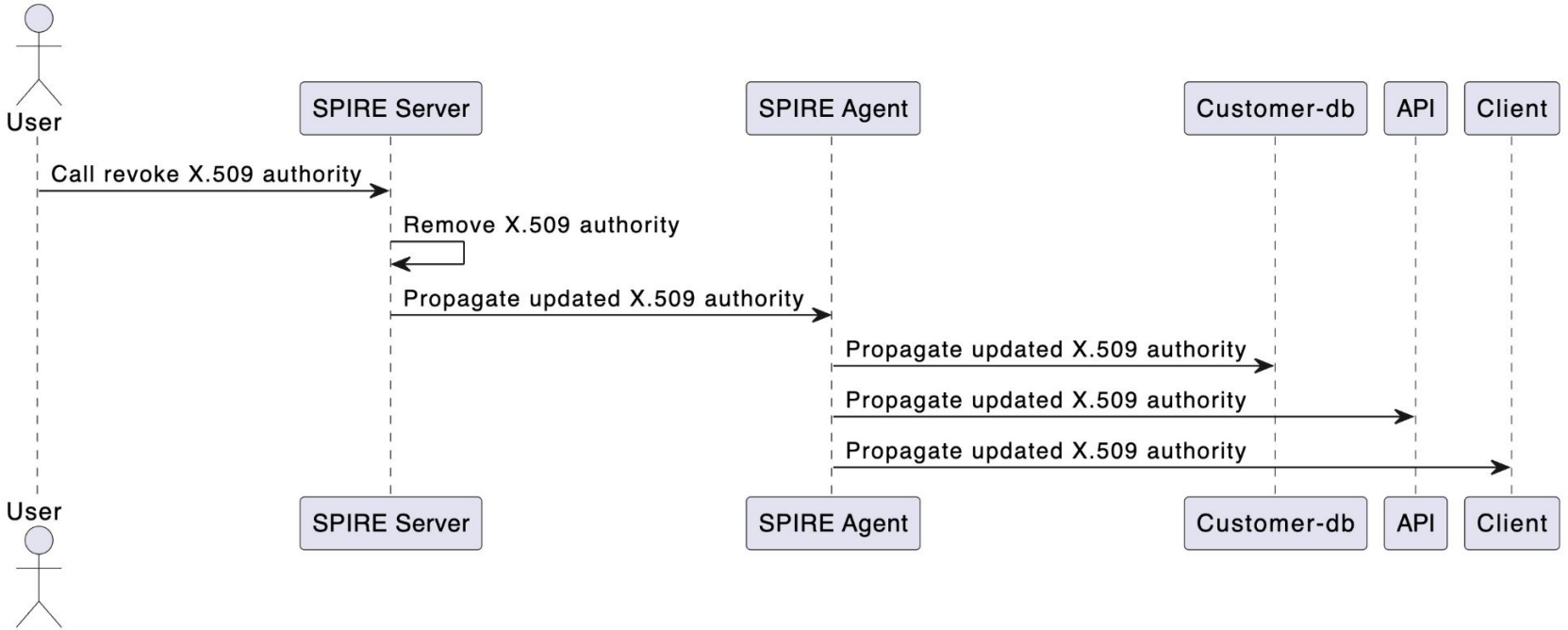
Activate X.509 Authority



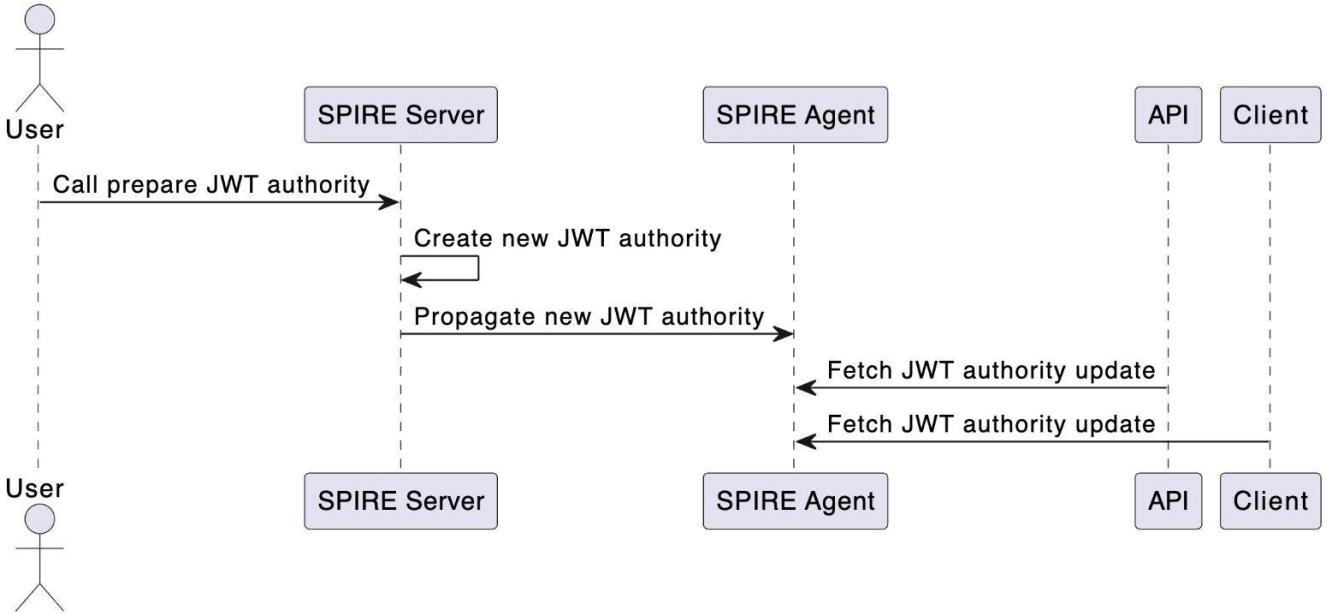
Taint X.509 Authority



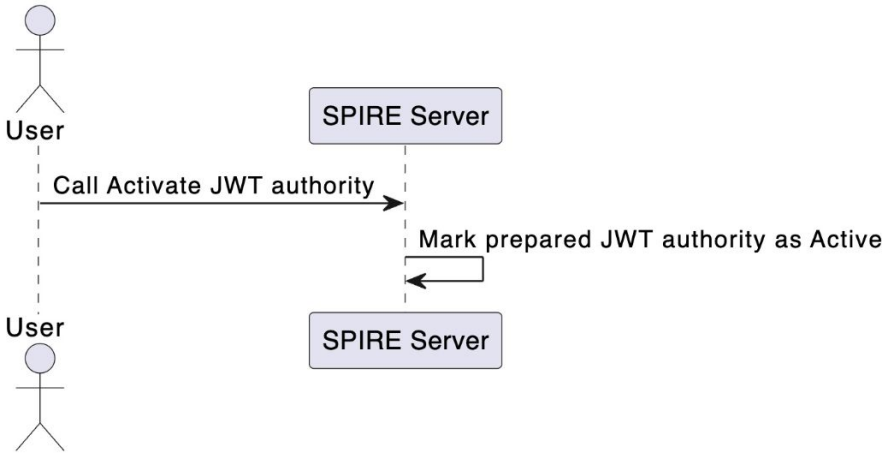
Revoke X.509 Authority



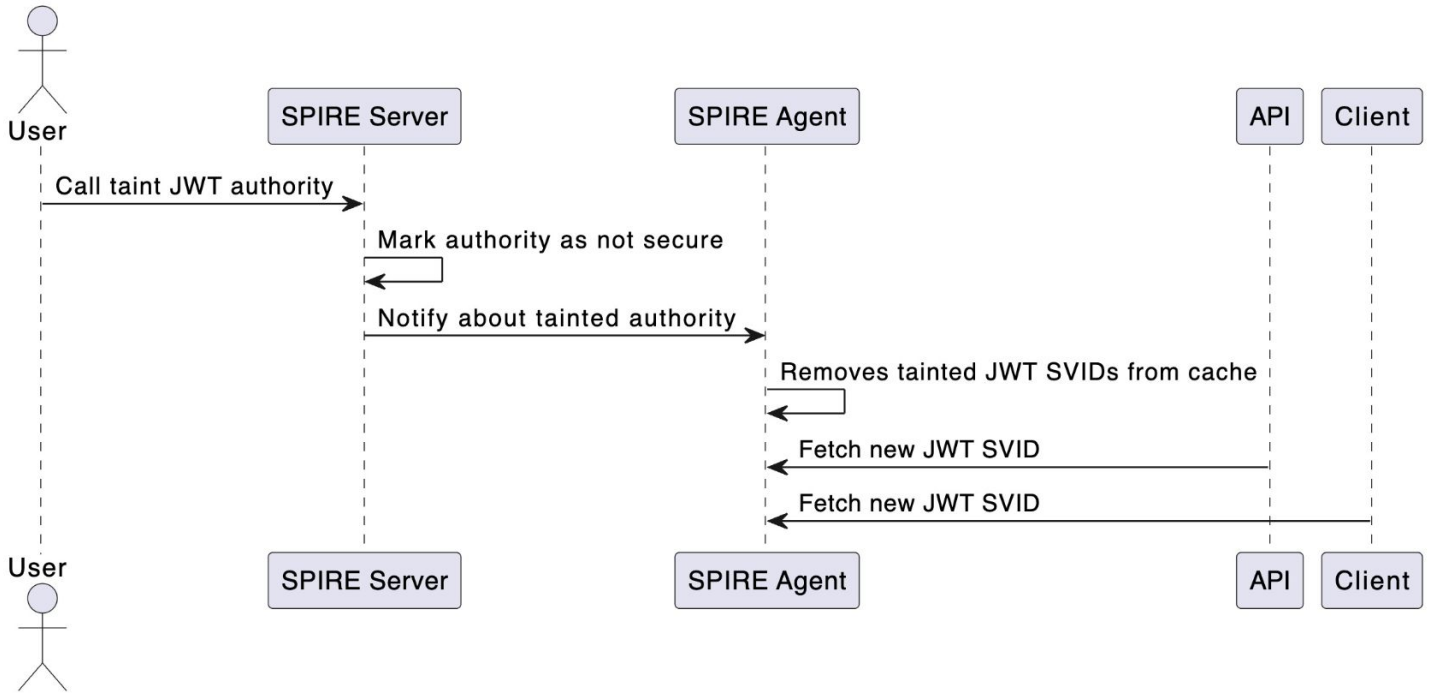
Prepare JWT Authority



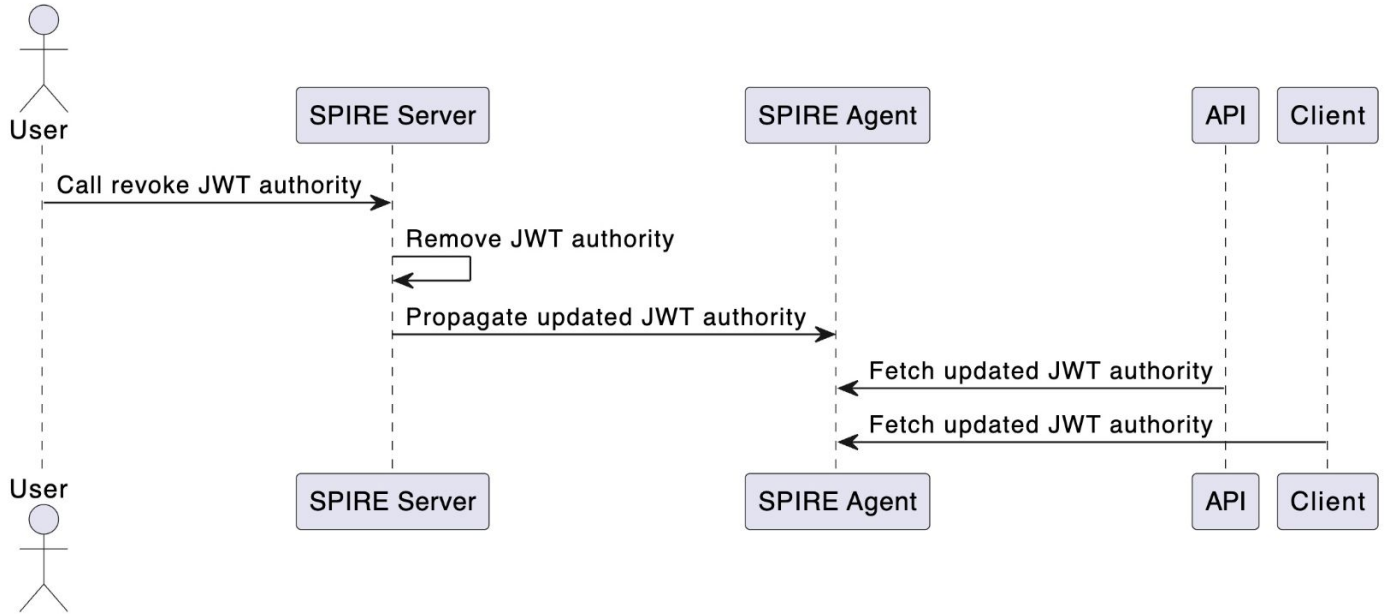
Activate JWT Authority



Taint JWT Authority



Revoke JWT Authority



Join Our Community!

KubeCon CloudNativeCon North America 2024

spiffe.slack.com

#@Marcos Yacob

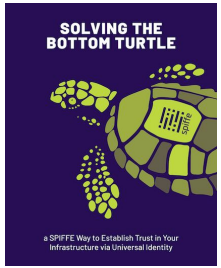
#@agustin

spiffe.io

github.com/spiffe/spiffe

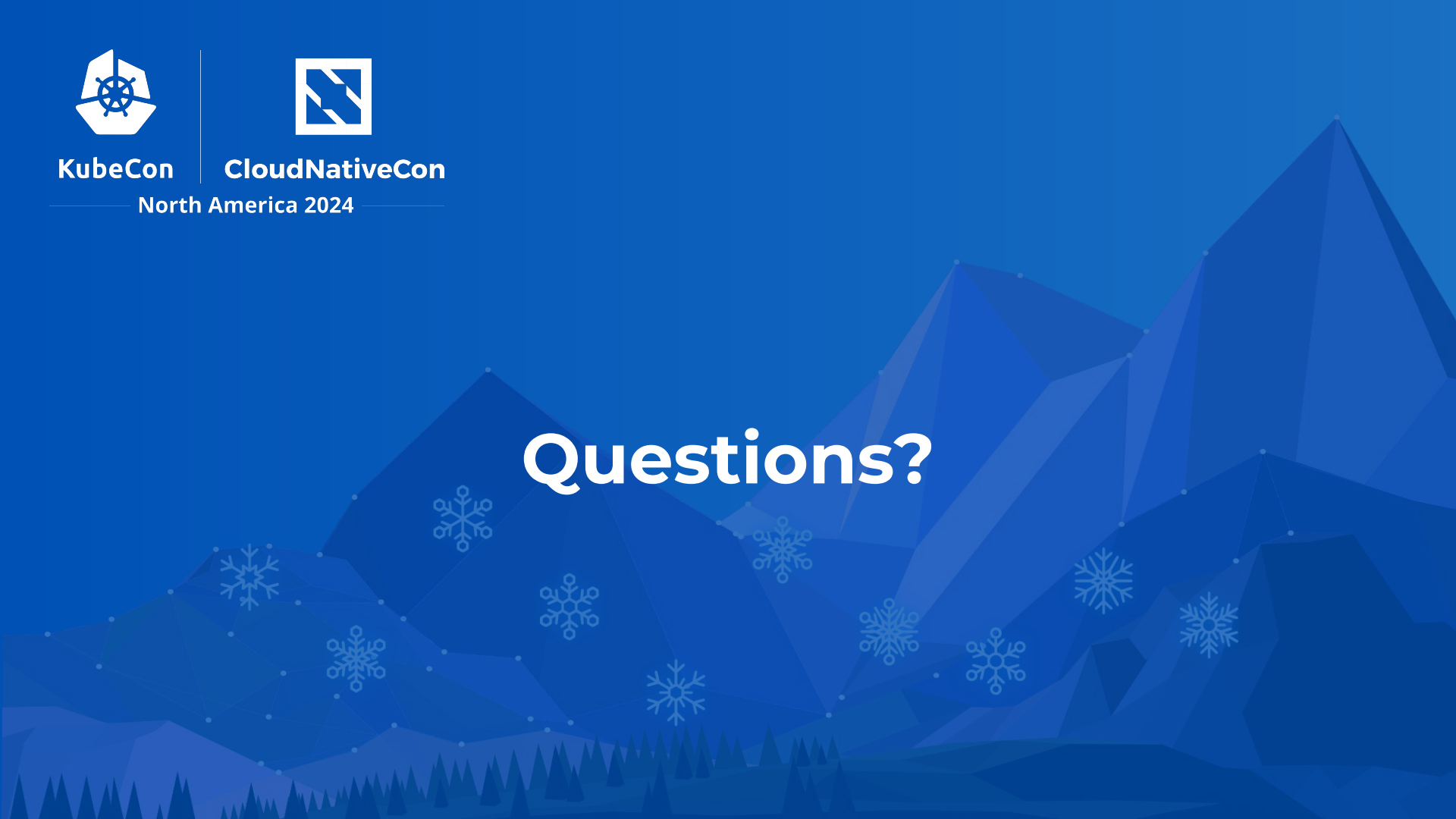
github.com/spiffe/spire

https://github.com/MarcosDY/spire-force-rotation-demo



spiffe.io/book

Leave us your feedback!


KubeCon
CloudNativeCon
North America 2024
Questions?