KubeCon | CloudNativeCon

North America 2023

Back to the Future:
Managing Trust in a Cloud-Native Environment

Eli Nesterov

SPIRL

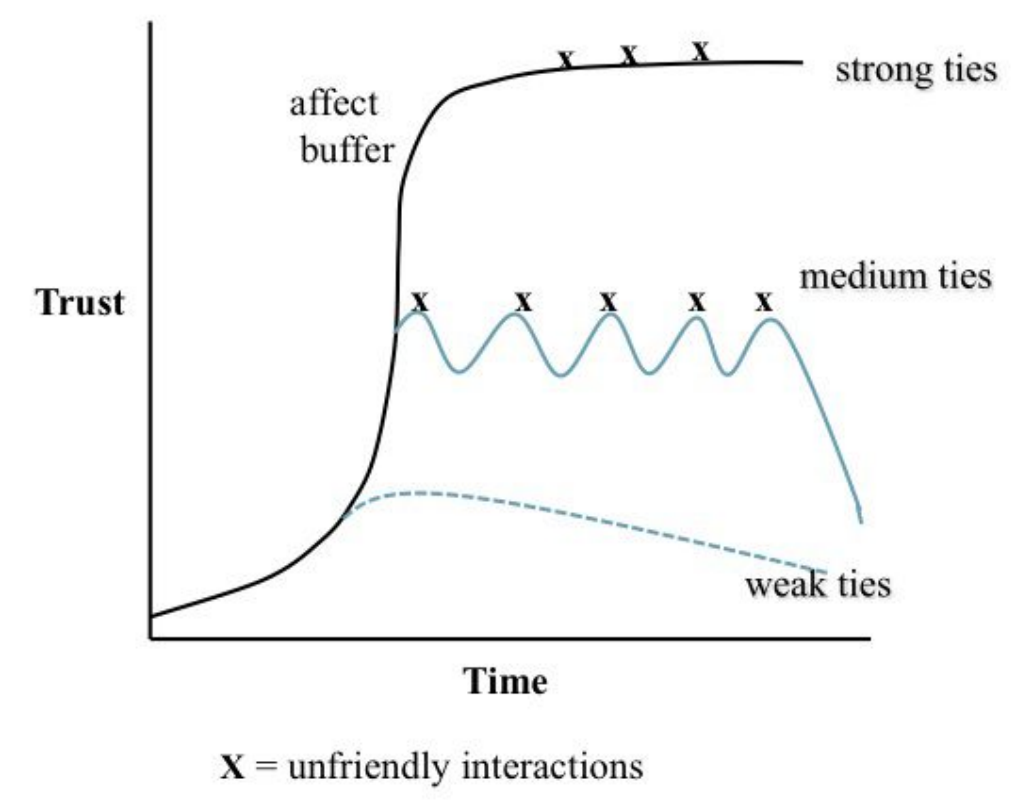
Hi, I an Eli!

eli@spirl.com

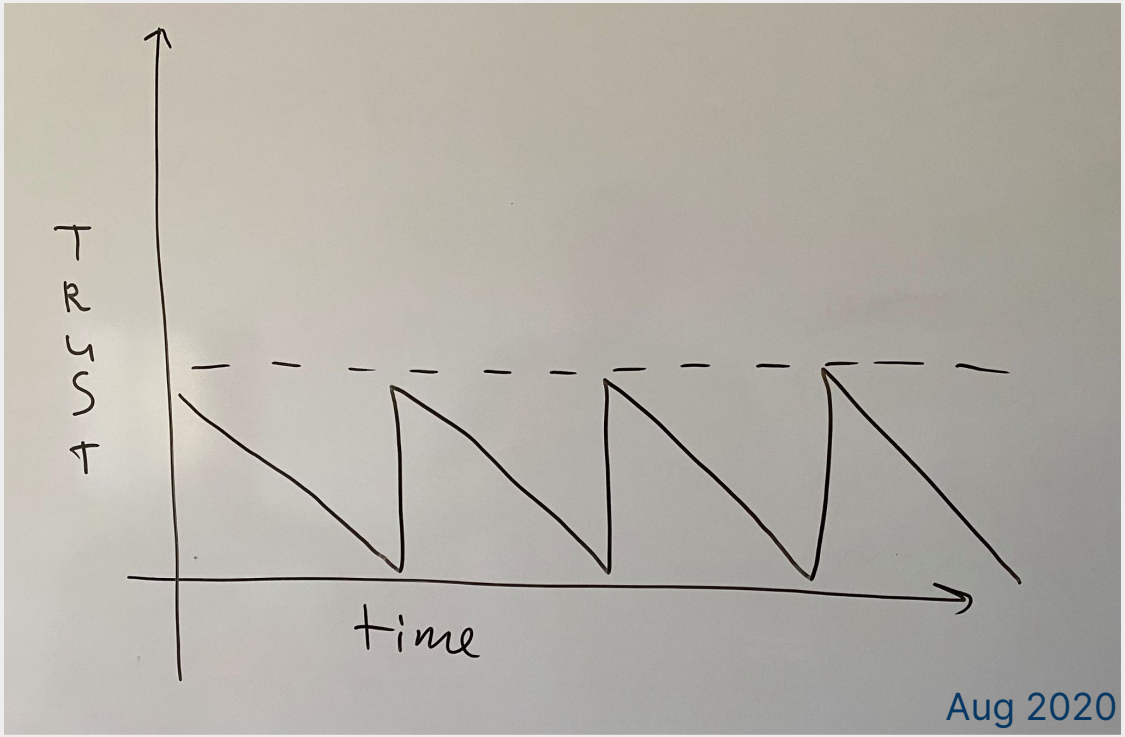
@elinesterov

- Co-author “Solving the Bottom Turtle”
- Built and scaled SPIRE infrastructure beyond 1M+ nodes
- Co-founder and CTO SPIRL

Trust in the Real World



Trust in the Digital World



SPIRL

Navigating Trust in a Cloud-Native World

- Managing trust = managing trust anchors
- Browsers
- Operating Systems
- Containers
- Cloud-native environment

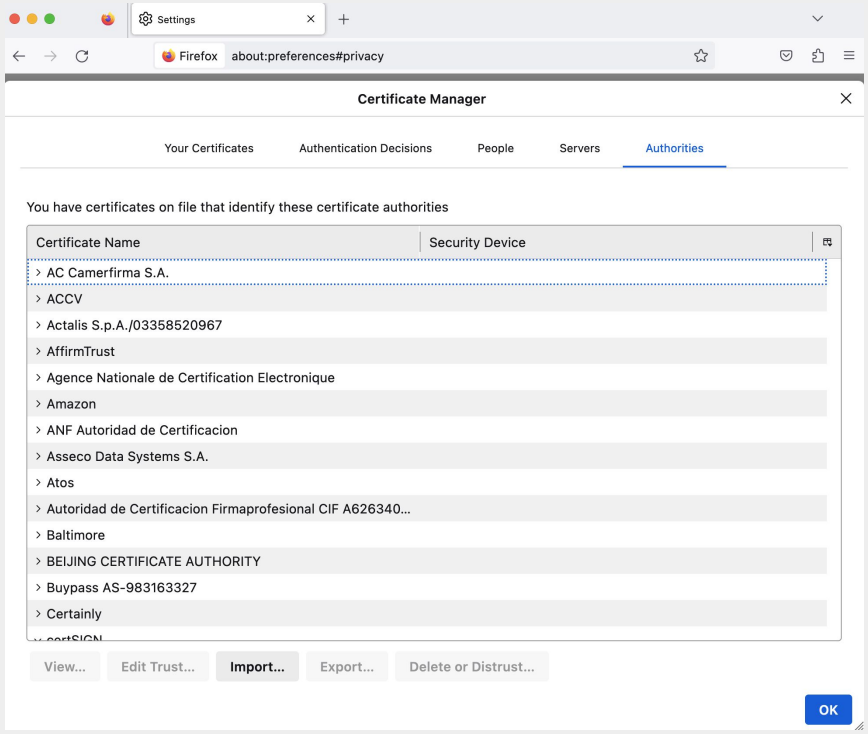
What is a Trust Anchor?

*A **trust anchor** is an authoritative entity represented by a public key and associated data.*

RFC 5914

WebPKI Trust Anchors in Browsers

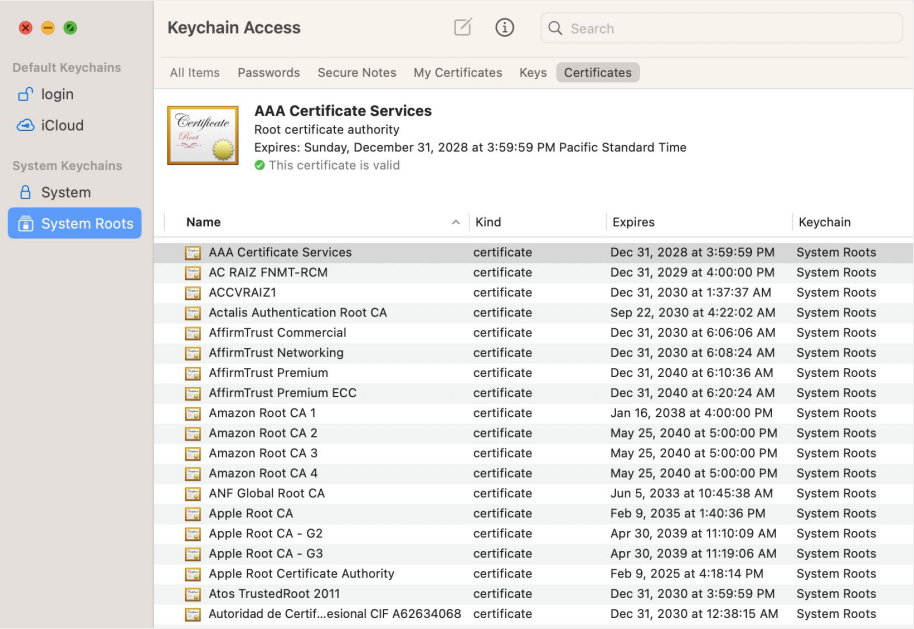
- Google Chrome
- Apple Safari
- Microsoft Internet Explorer and Edge
- Mozilla Firefox
- Update relies on OS (except FF) for WebPKI
- User can add/remove (corp CA)



SPIRL

WebPKI Trust Anchors in OS

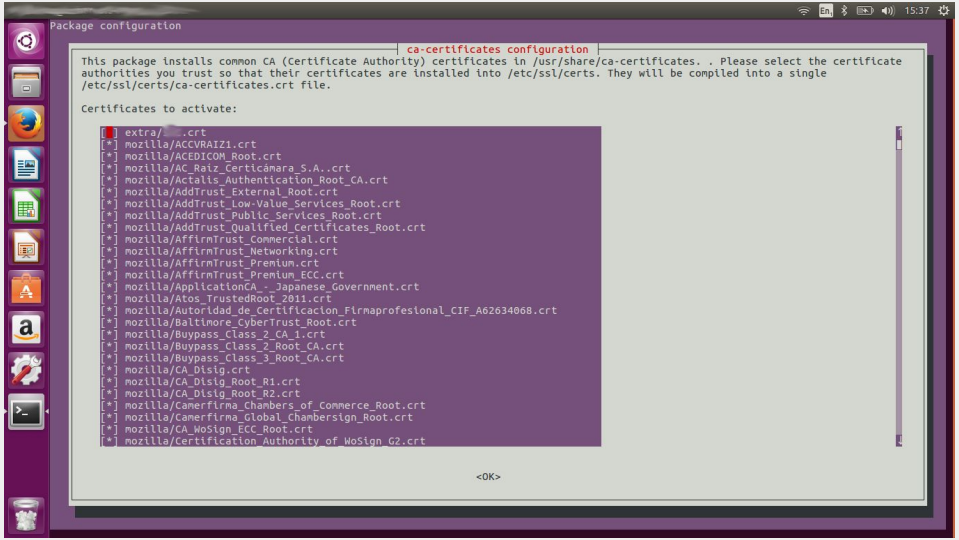
- Each OS have a trust store
- Users can add or delete certificates
- Updates delivered via OS update
- Disallowed certificates list (Windows)



SPIRL

WebPKI Trust Anchors in Linux

- Based on Mozilla NSS List
- /etc/ssl/certs/
- /etc/pki/tls/certs/ca-bundle.crt
- ca-certificates package
- Update depends on package



SPIRL

WebPKI Trust Anchors in Containers

- Depends on the container image/os/distribution
- Require ca-certificates pkg
- RUN install/add ca-certificates
- distroless requires COPY

SPIRL

How About My Company PKI?

- Browsers
- Machines/OS (users, on-pem HW, VMs, Cloud)
- Users (for authentication)
- Java keystore
- NSS

What About Containers?

Managing Trust Anchors for Containers Using CI

- Containers are ephemeral
- Cannot use the same pattern as VMs
- Web PKI: apk add ca-certificates
- Private CA: update-ca-certificates
- Try https://github.com/dlorenc/incert
- JKS: build and copy it

Example

```
FROM alpine:3.18.0 as add-cert

RUN apk add --no-cache ca-certificates

ADD custom-ca.pem /usr/local/share/ca-certificates/custom-ca.crt

RUN update-ca-certificates
```

Managing Trust Anchors for Containers at Runtime

- Volume mount
- Download bundle(s) at start
- CSI Driver
- trust-manager

  https://cert-manager.io/docs/trust/trust-manager/

```
if [ ! -f /etc/ssl/certs/ca-certificates.crt ]; then
  # Insecurely download the root certificate for the CA_URL server
  curl -ks -o /tmp/root-ca.crt "${CA_URL}"
  # Confirm the certificate matches the hardcoded fingerprint
  fingerprint=$(openssl x509 -in /tmp/root-ca.crt -noout -sha256 -fingerprint \
                | tr -d ":" \
                | cut -d "=" -f 2 \
                | tr "[:upper:]" "[:lower:]")
  if [[ "$fingerprint" != "$CA_FINGERPRINT" ]]; then
    echo >&2
    echo >&2 "error: CA certificate fingerprint $fingerprint does not match expected valu
    echo >&2
    exit 1
  fi
  # Now download the full CA bundle, without -k
  curl -s --cacert /tmp/root-ca.crt -o /etc/ssl/certs/ca-certificates.crt "${CA_BUNDLE_UR
fi
```

SPIRL

Should You Worry About WebPKI Trust Anchors?

- You consume API or services that use Web PKI
- What if your trust anchors are outdated (expired, compromised)
- Harder to exploit (MiTM, know your target)
- Compromised vs Expired
- What if someone injects the public key of a rouge CA?

Enter Paranoia

Example: chainguard/curl:latest

```
➜ ~ paranoia inspect cgr.dev/chainguard/curl:latest
Certificate CN=E-Tugra Certification Authority,OU=E-Tugra Sertifikasyon Merkezi,O=E-Tuğra EBG Bilişim
├ 🚨 expired ( expired on 2023-03-03T12:09:48Z, 34 weeks 2 days since expiry)
└ 🚨 removed from Mozilla trust store, no reason given
Certificate CN=E-Tugra Global Root CA ECC v3,OU=E-Tugra Trust Center,O=E-Tugra EBG A.S.,L=Ankara,C=TR
└ 🚨 removed from Mozilla trust store, no reason given
Certificate CN=E-Tugra Global Root CA RSA v3,OU=E-Tugra Trust Center,O=E-Tugra EBG A.S.,L=Ankara,C=TR
└ 🚨 removed from Mozilla trust store, no reason given
Certificate CN=Hongkong Post Root CA 1,O=Hongkong Post,C=HK
├ 🚨 expired ( expired on 2023-05-15T04:52:29Z, 23 weeks 6 days since expiry)
└ 🚨 removed from Mozilla trust store, no reason given
Certificate OU=Security Communication RootCA1,O=SECOM Trust.net,C=JP
└ 🚨 expired ( expired on 2023-09-30T04:20:49Z, 4 weeks 1 day since expiry)
Found 141 certificates total, of which 5 had issues
```

Date: 11/01/2023

Get it: https://github.com/jetstack/paranoia

SPIRL

How Long Will It Take to Update Your Images?

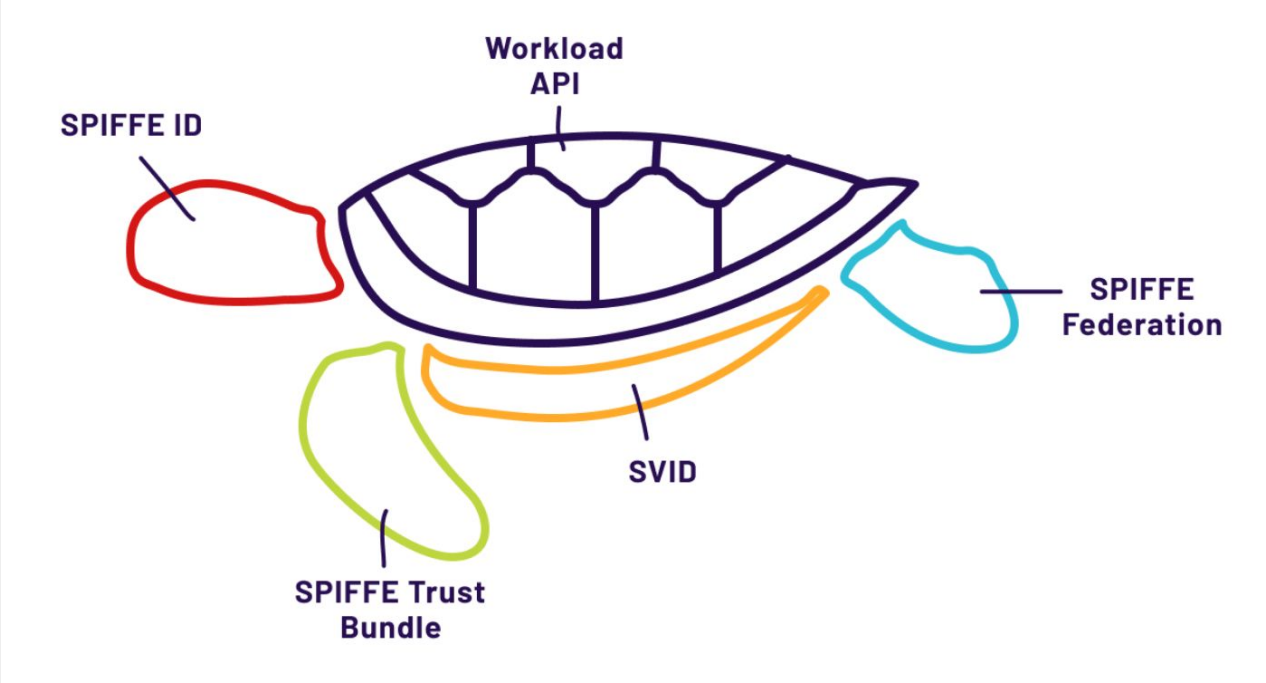
- Your CA is compromised. How long would it take to propagate changes and rebuild?
- Public CA is compromised. What images should you update?
- What to do with the containers and services at runtime?

Enter SPIFFE
where
Everything is Automated

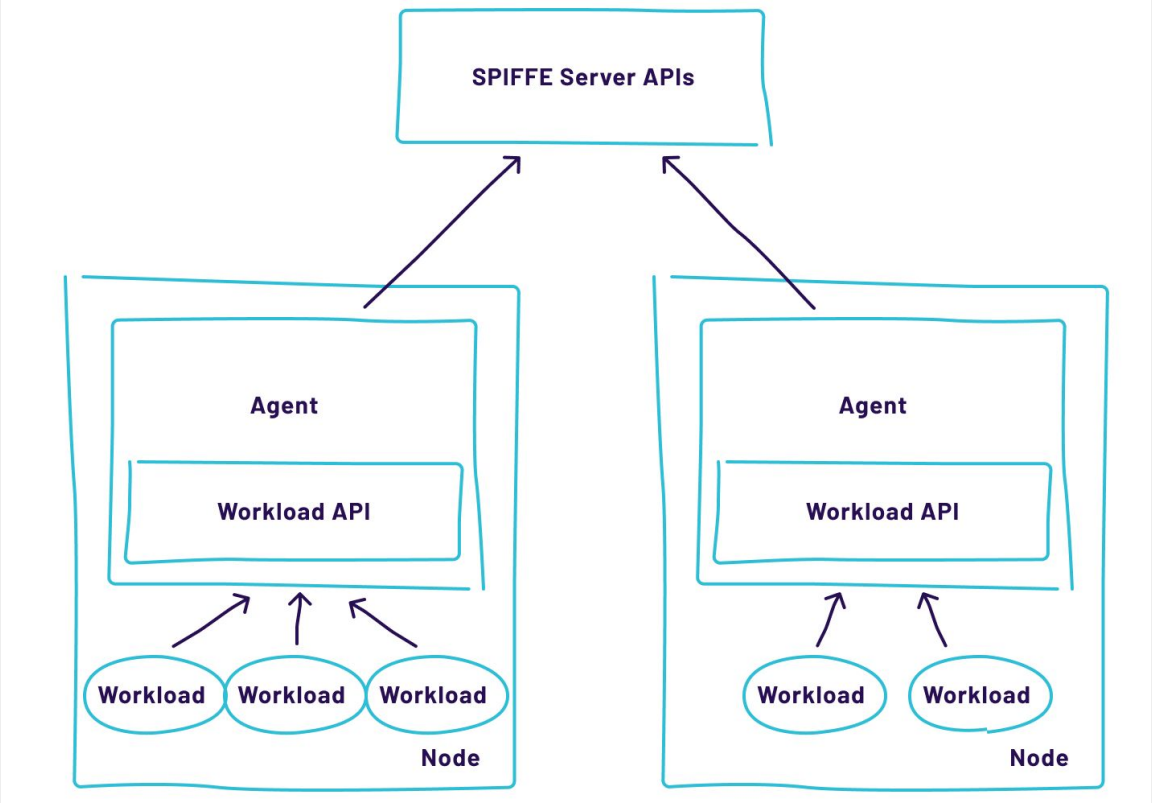
spiffe

What is SPIFFE

Secure
Production
Identity
Framework
For
Everyone

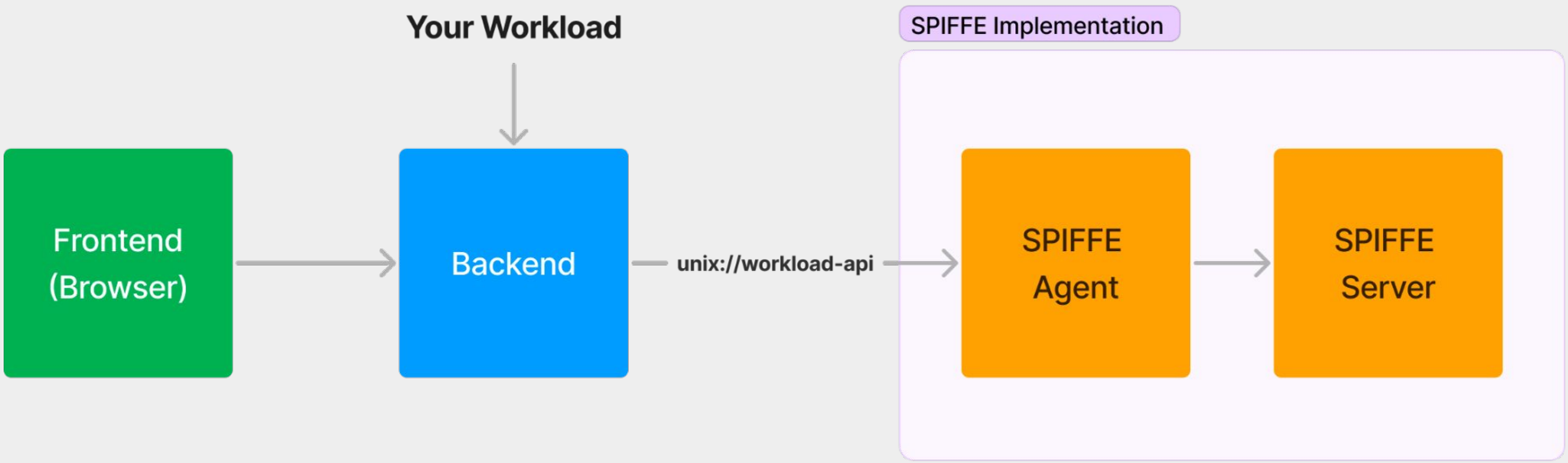


SPIFFE Implementation



Demo Time

Demo Architecture



What SPIFFE Solves

- Workload Identity not Human Identity
- Manage SPIFFE Trust Bundle not Web PKI
- Implementation can be extended to deliver Private PKI Trust Anchors as a separate API

Take Away

- Private PKI vs Web PKI
- Build a golden image(s)
- Automation is a key
- Speed of changes (CI vs runtime)
- Use SPIFFE

Thank you