Hewlett Packard
Enterprise

PROJECT GALADRIEL

SPIRE Federation at Scale

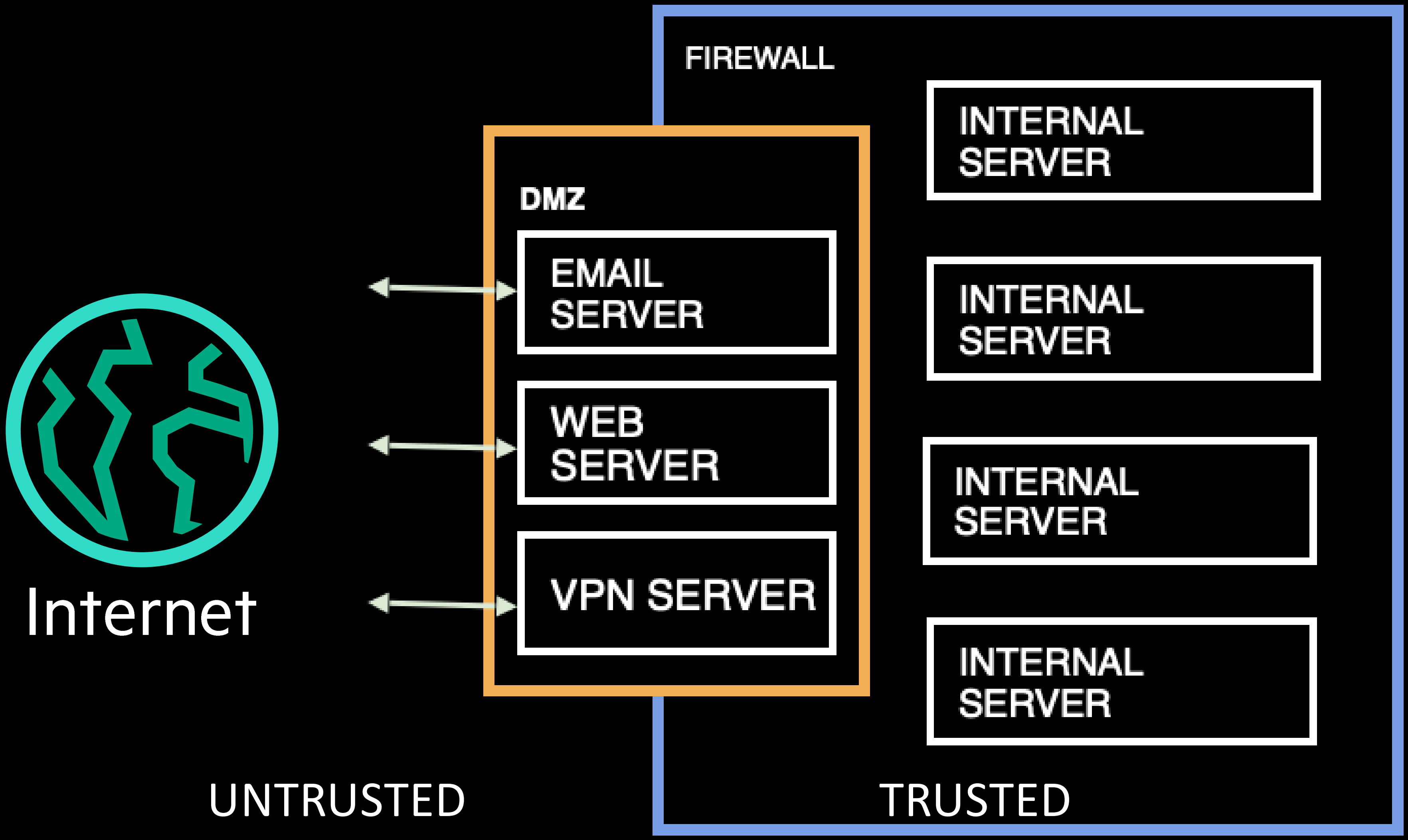
Max Lambrecht
Maximiliano Churichi

Security Engineers

AGENDA

- Zero Trust and Workload Identity
- SPIFFE and SPIRE
- SPIRE Federation
- Project Galadriel + demo

PERIMETER BASED SECURITY



FIREWALL

DMZ

EMAIL SERVER

WEB SERVER

VPN SERVER

INTERNAL SERVER

INTERNAL SERVER

INTERNAL SERVER

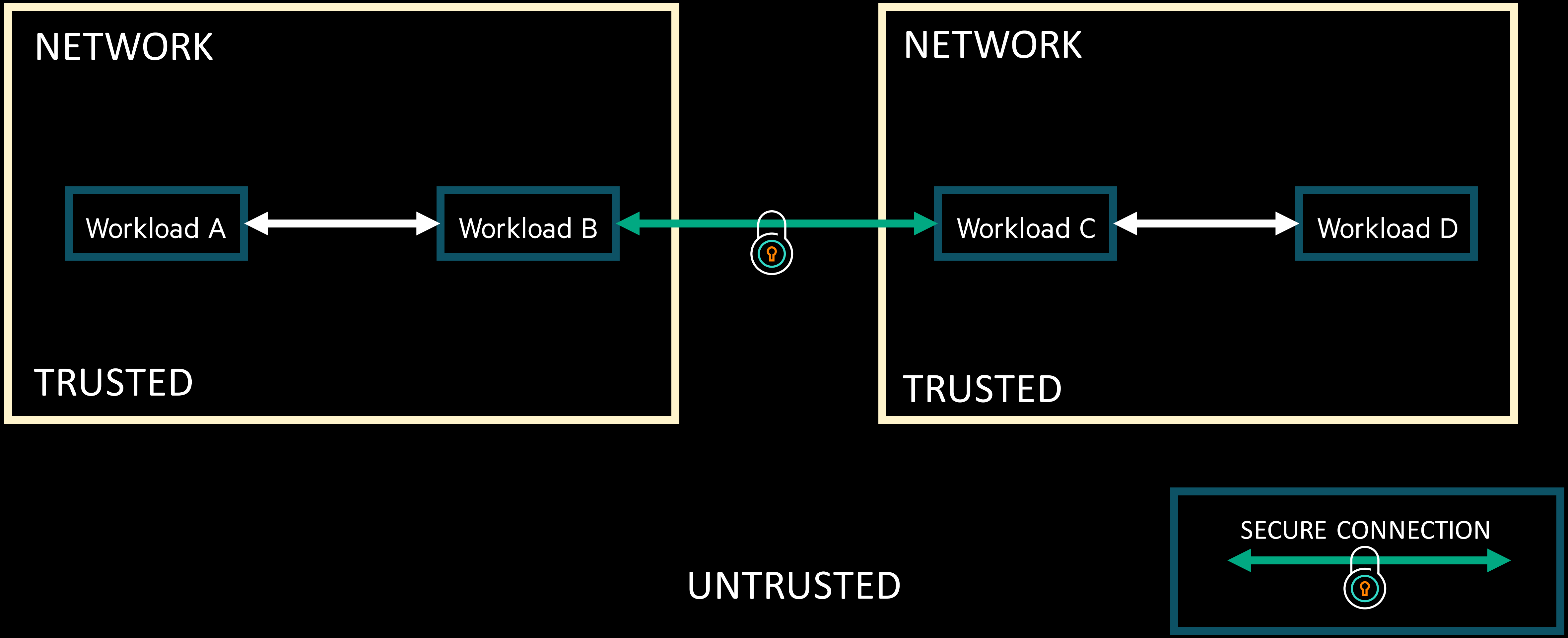
INTERNAL SERVER

Internet

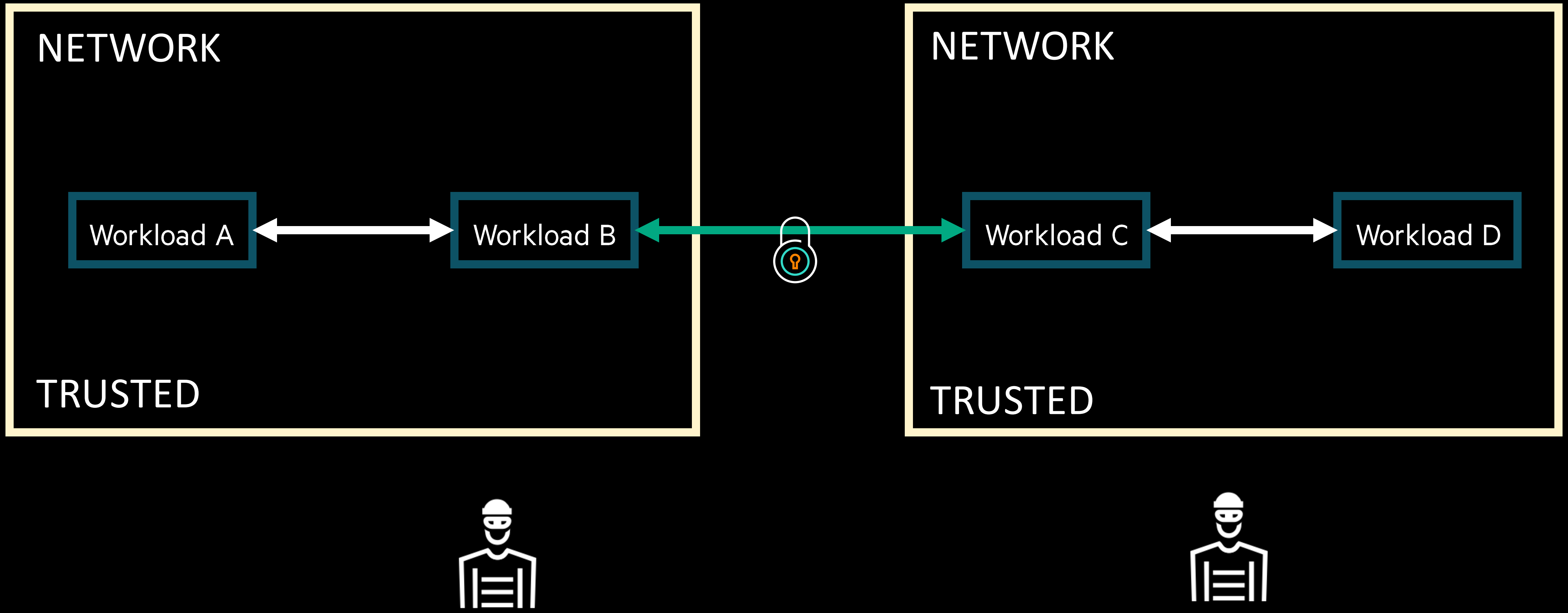
UNTRUSTED

TRUSTED

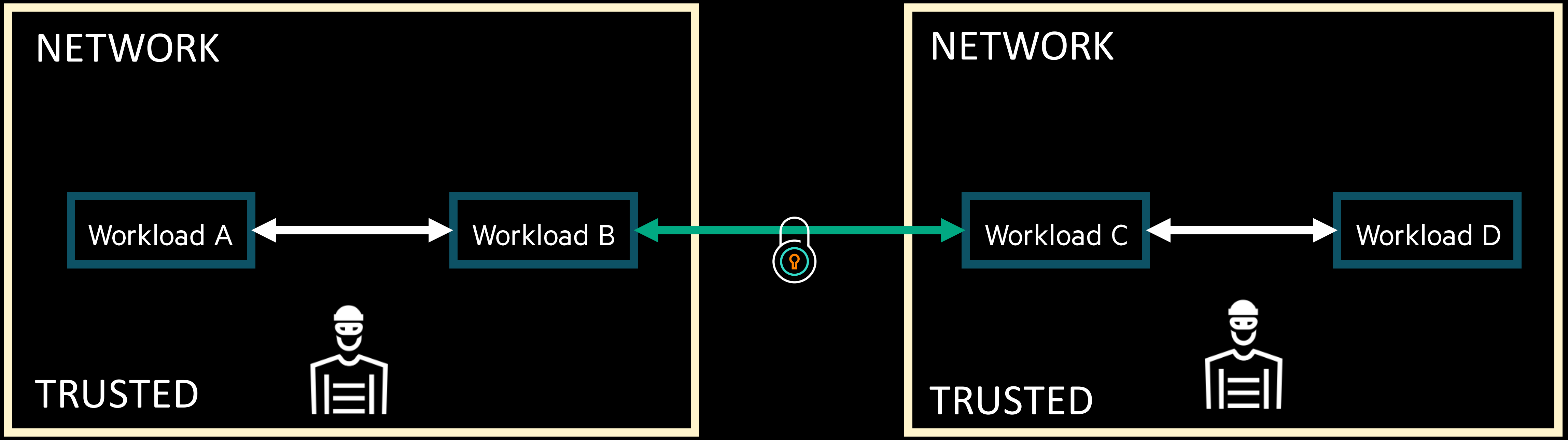
TRUSTED PERIMETER



TRUSTED PERIMETER

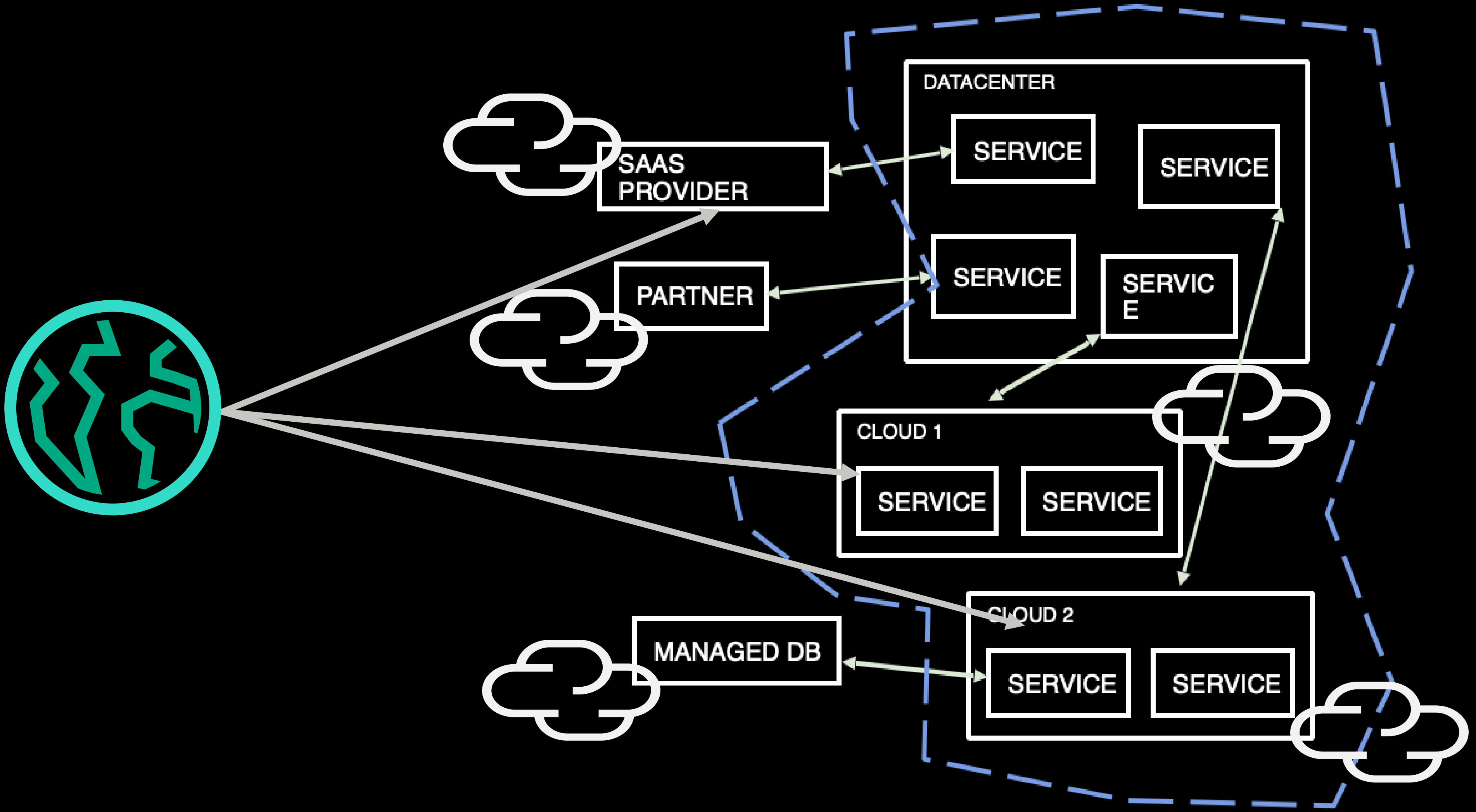


TRUSTED PERIMETER



WHAT IF THE MALICIOUS AGENTS ARE INSIDE THE TRUSTED PERIMETER?

PERIMETER HAS BECOME TOO COMPLEX

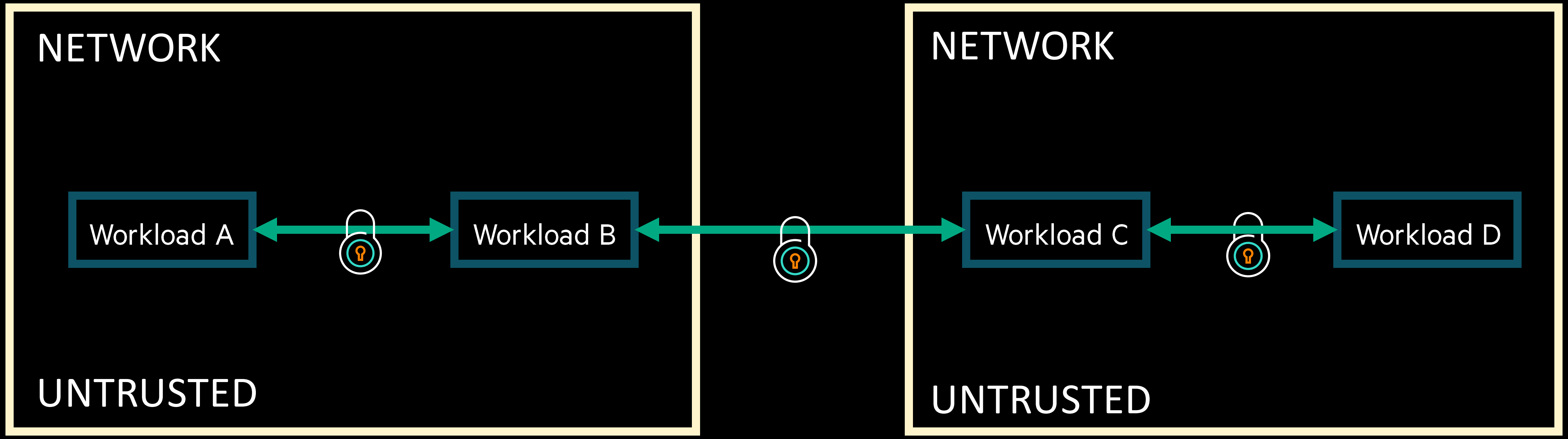


In the era of multi clouds and microservices the perimeter has become untenable.

ZERO (implicit) TRUST

Zero Trust is a security model based on the idea that no one is implicitly trusted, and everything should be verified.

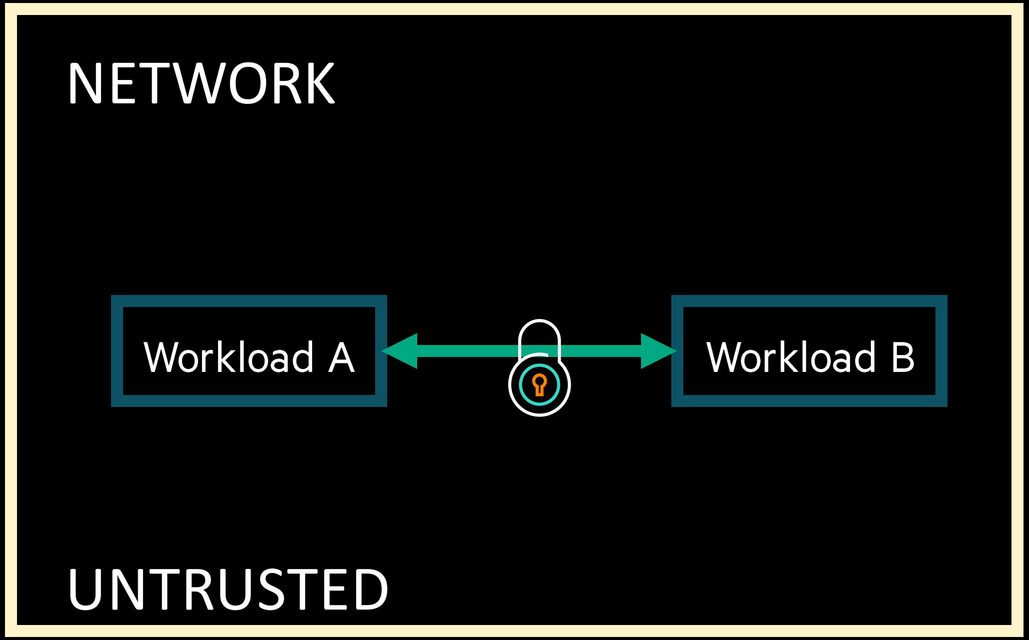
ZERO TRUST: EVERY CONNECTION IS SECURED



SECURE CONNECTION

Identity-centric model

ZERO TRUST: IDENTITY



Workloads A and B should be able to identify who they are talking to, in a secure way.

Hello, SPIFFE

WHAT IS SPIFFE?

SPIFFE is a an open-source standard for software identity.

SPIFFE STANDARD

SPIFFE ID

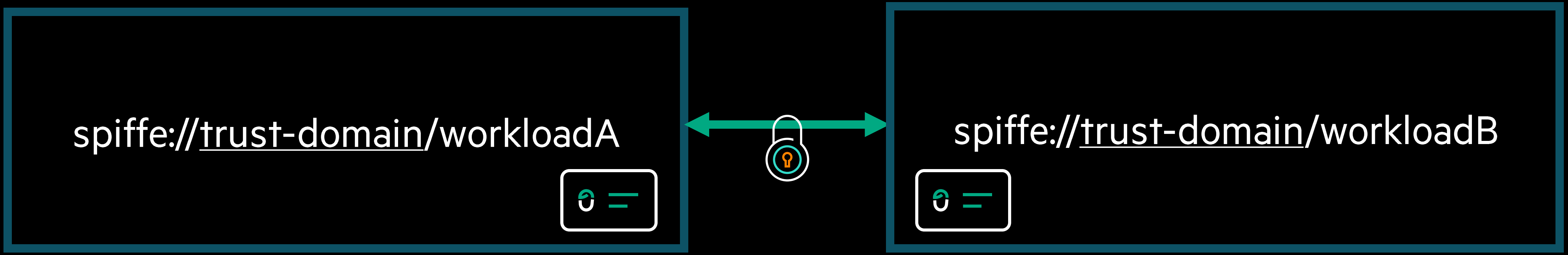
Standard format for a service identifier

spiffe://trust-domain/service

SPIFFE VERIFIABLE IDENTITY DOCUMENT (SVID)

Cryptographically verifiable document asserting a SPIFFE ID

SPIFFE Identities


spiffe://trust-domain/workloadA
spiffe://trust-domain/workloadB

SPIFFE Trust Domain

spiffe://trust-domain/workload

A SPIFFE Trust Domain is an identity namespace with a set of root keys.

All workloads in the same trust domain get identity documents (SVIDs) that can be verified against the root keys of the trust domain.

SPIFFE Trust Bundle

spiffe://trust-domain/workload

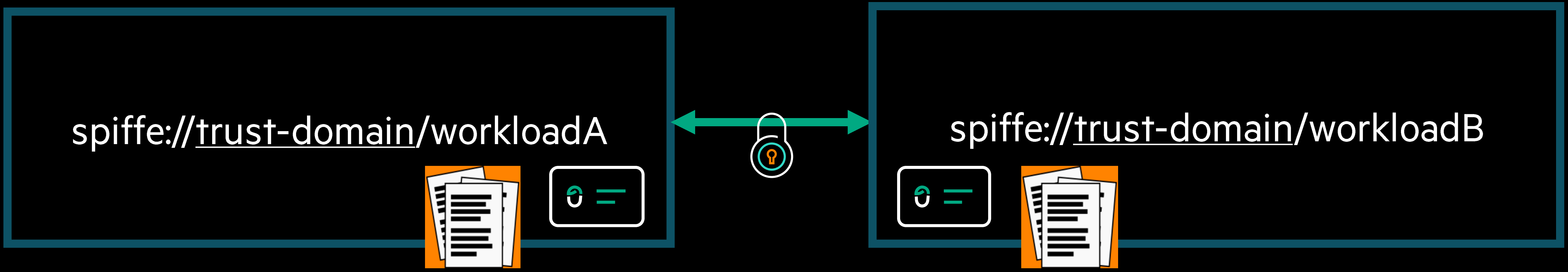
A SPIFFE Trust Domain is an identity namespace.

All workloads in the same trust domain get identity documents (SVIDs) that can be verified against the **root keys of the trust domain**.

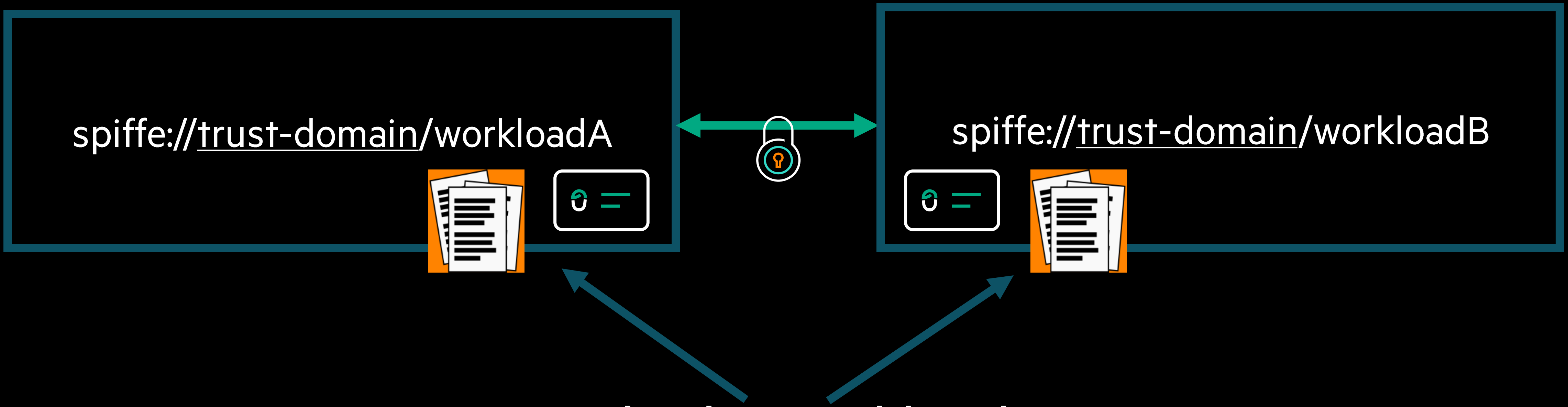
TRUST BUNDLE

Set of public keys used to verify SVIDs

SPIFFE Identity Materials


spiffe://trust-domain/workloadA
spiffe://trust-domain/workloadB

SPIFFE Identity Materials

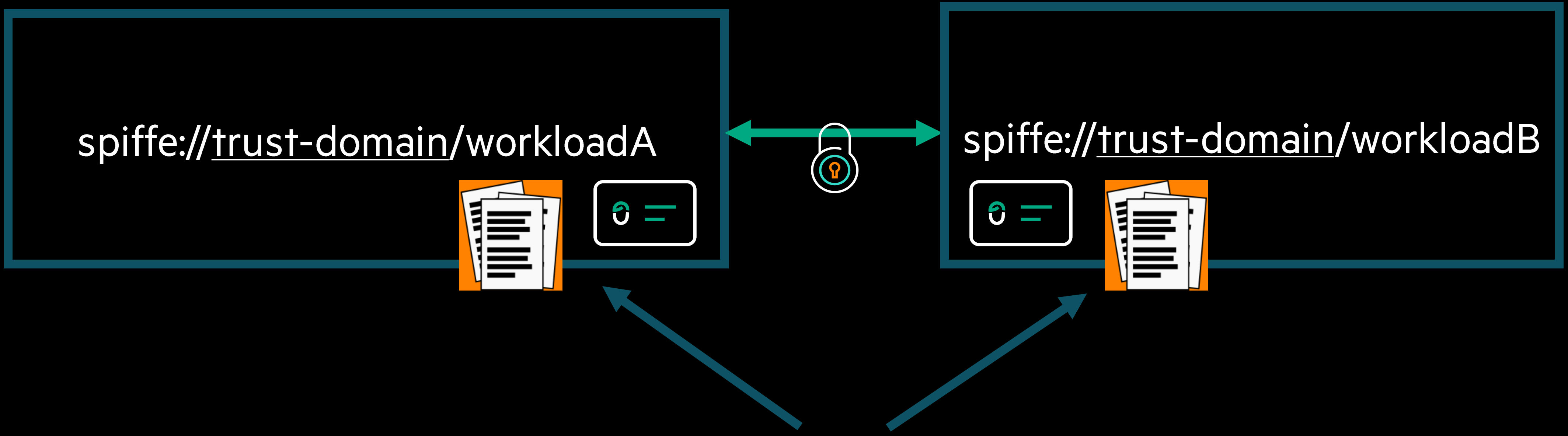


spiffe://trust-domain/workloadA

spiffe://trust-domain/workloadB

How do the workloads get their SVIDs and Trust Bundles?

SPIFFE Workload API



spiffe://trust-domain/workloadA

spiffe://trust-domain/workloadB

How do the workloads get their IDs and Trust Bundles?

SPIFFE WORKLOAD API

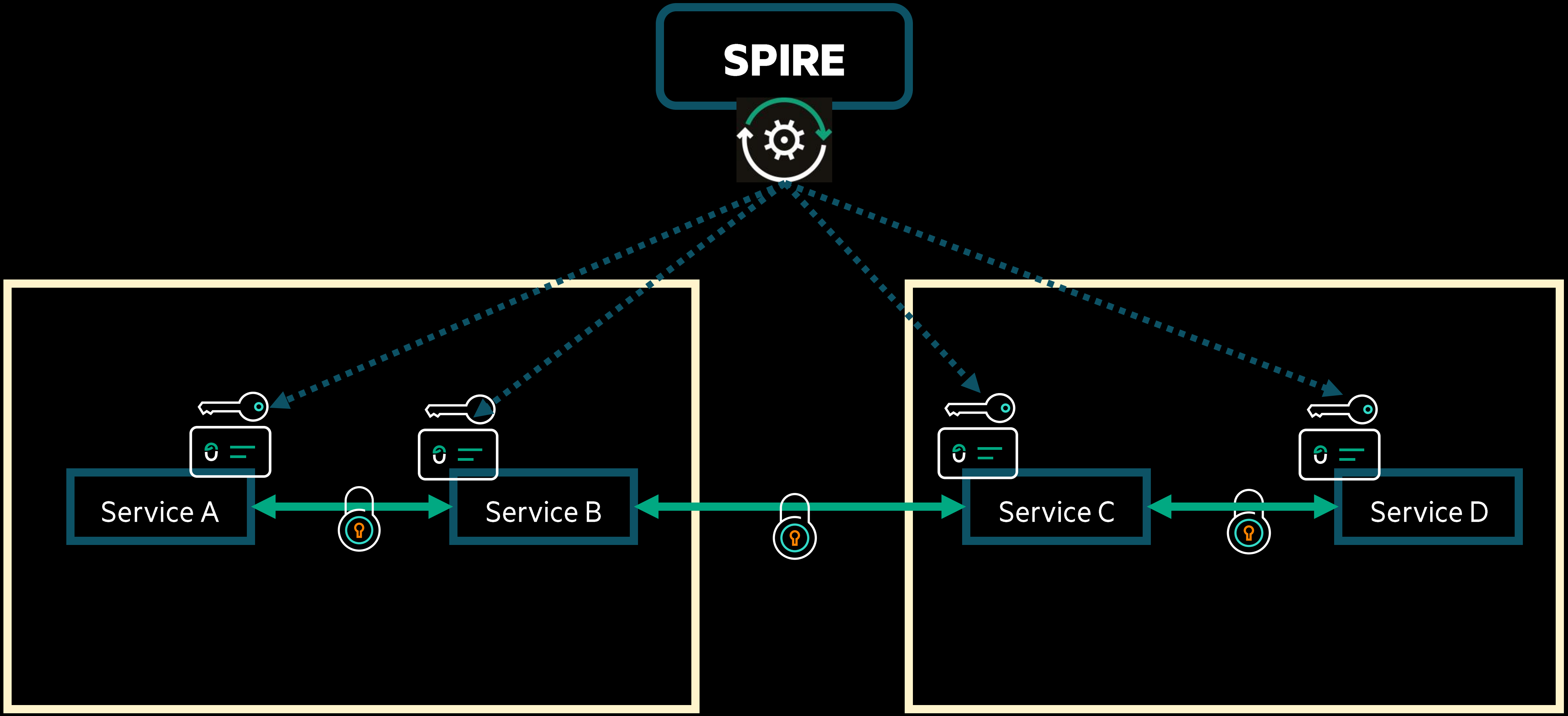
Local API for workloads to retrieve their identities (SVIDs and Trust Bundles)

SPIFFE RUNTIME ENVIRONMENT

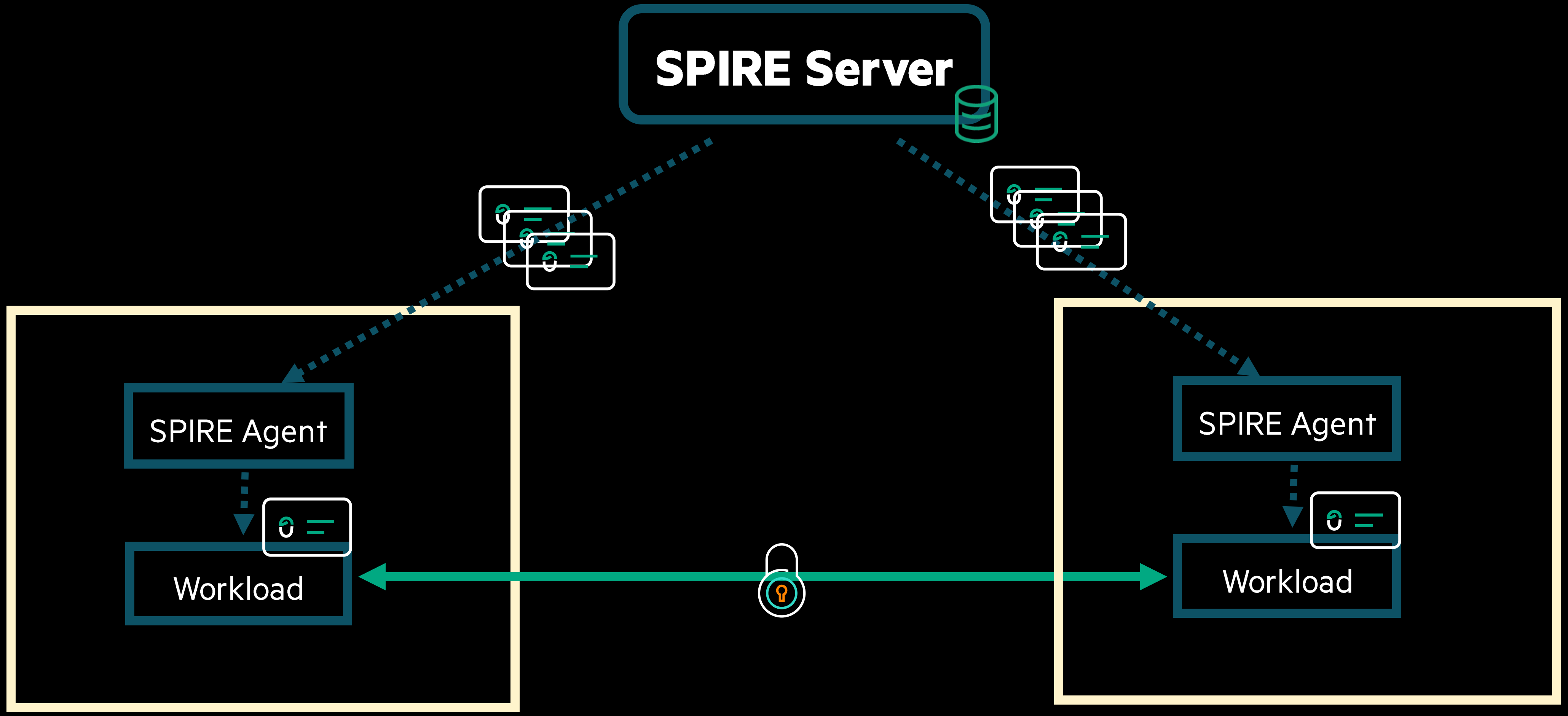
SPIRE

An Identity Control Plane based on SPIFFE.

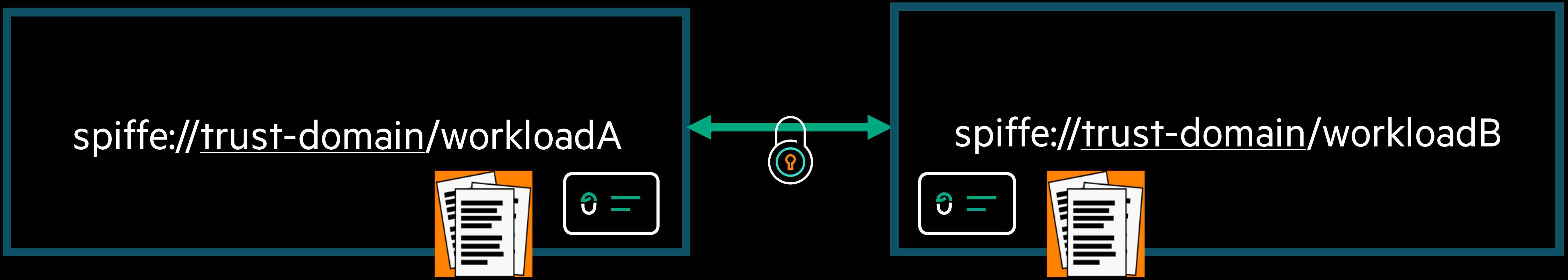
SPIRE AS THE IDENTITY CONTROL PLANE



SPIRE AS THE IDENTITY CONTROL PLANE

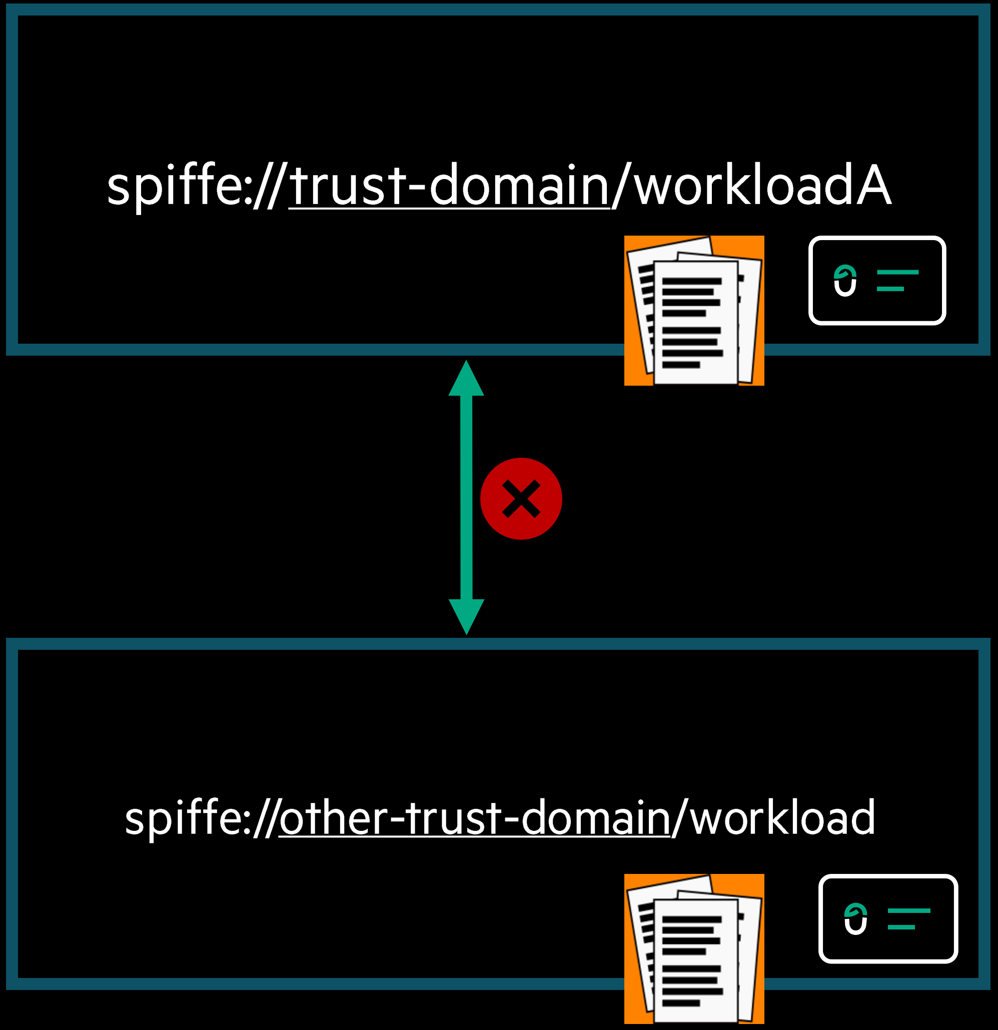


SPIFFE


spiffe://trust-domain/workloadA
spiffe://trust-domain/workloadB

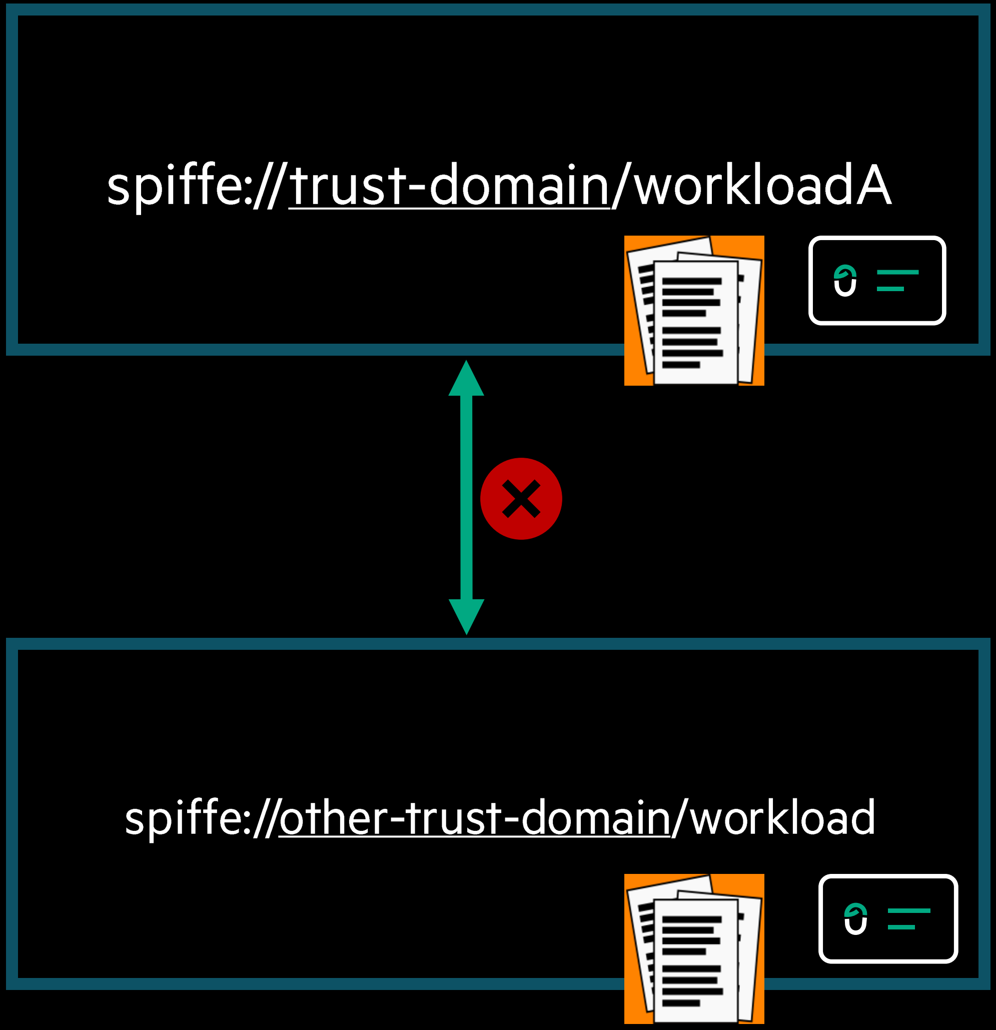
So far, we can deliver and validate identities in one Trust Domain

SPIFFE


spiffe://trust-domain/workloadA
spiffe://other-trust-domain/workload

What if we need to securely connect workloads across **multiple trust domains**?

SPIFFE Federation



spiffe://trust-domain/workloadA

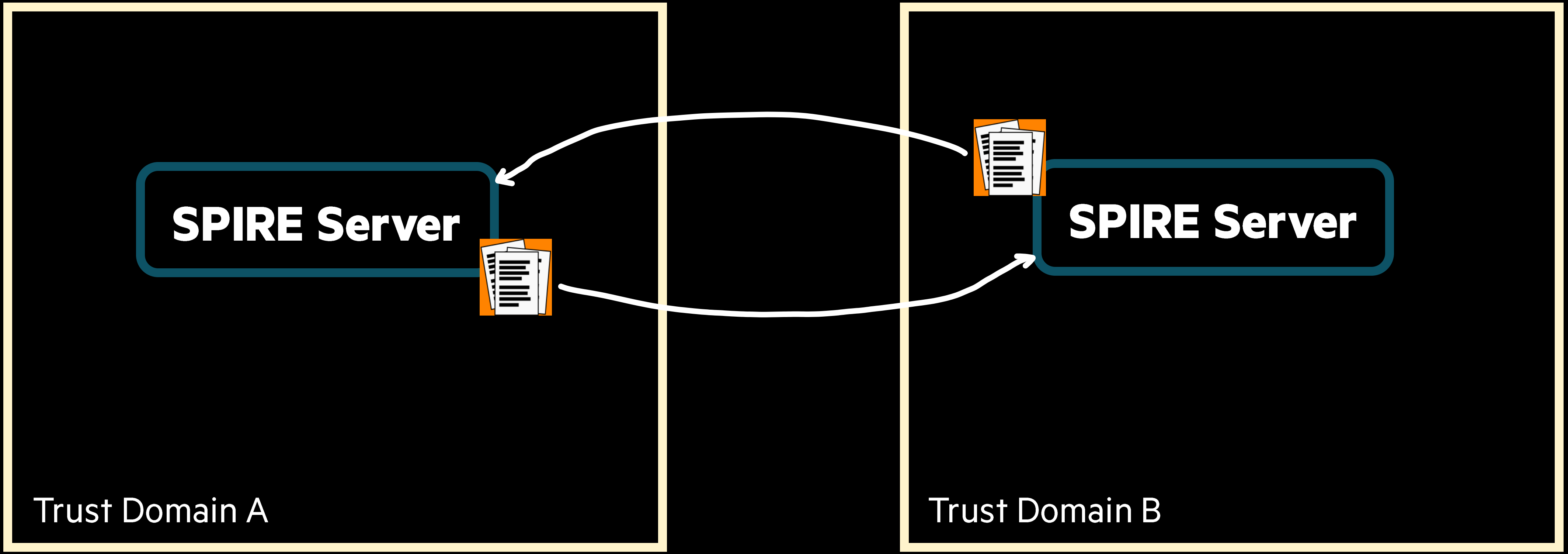
spiffe://other-trust-domain/workload

What if we need to securely connect across multiple Trust Domains?

SPIFFE Federation

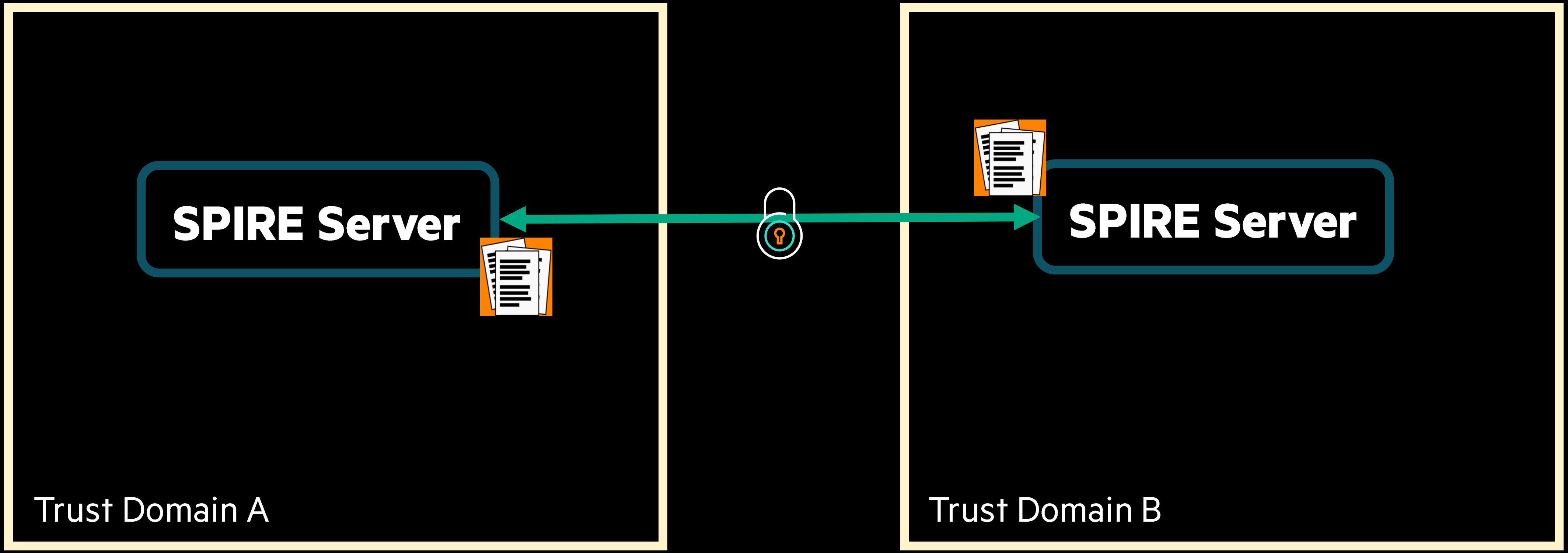
A mechanism to share SPIFFE Trust Bundles across Trust Domains.

SPIRE FEDERATION

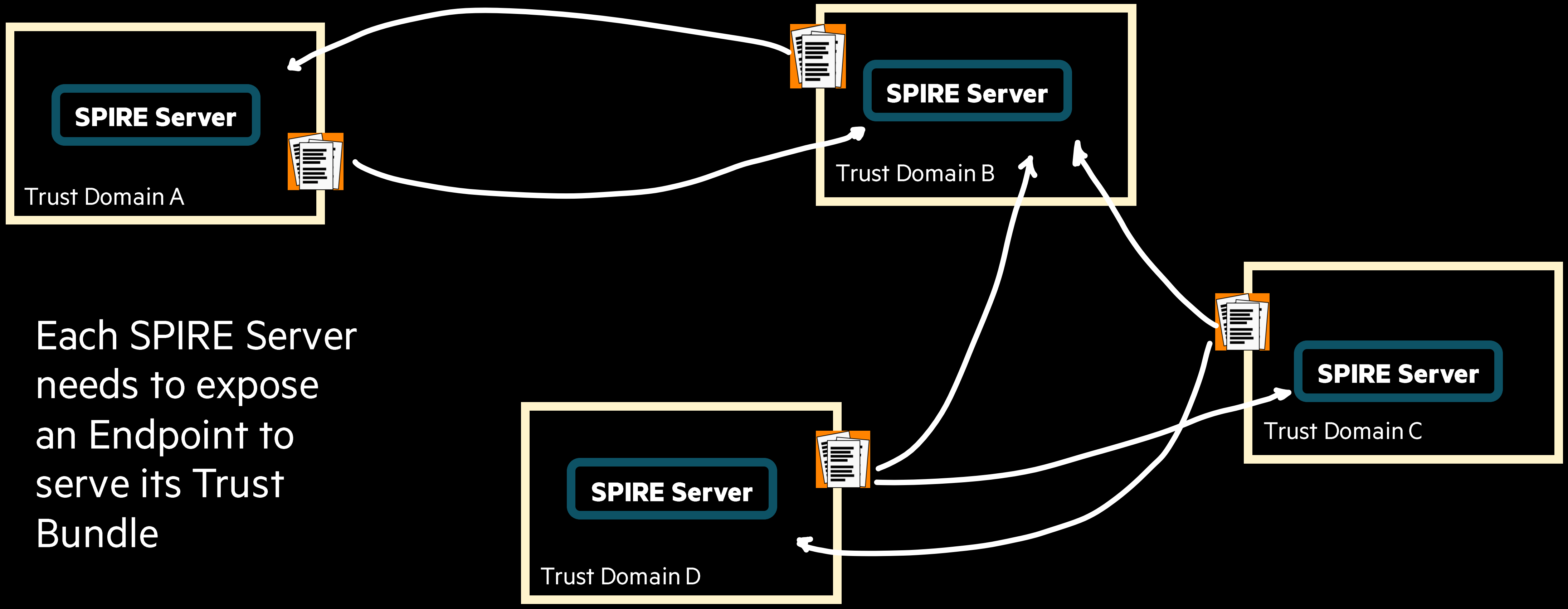


SPIRE FEDERATION

SPIRE Servers need to serve an HTTPS Bundle Endpoint to securely make their Trust Bundles available to be consumed by other SPIRE Servers.

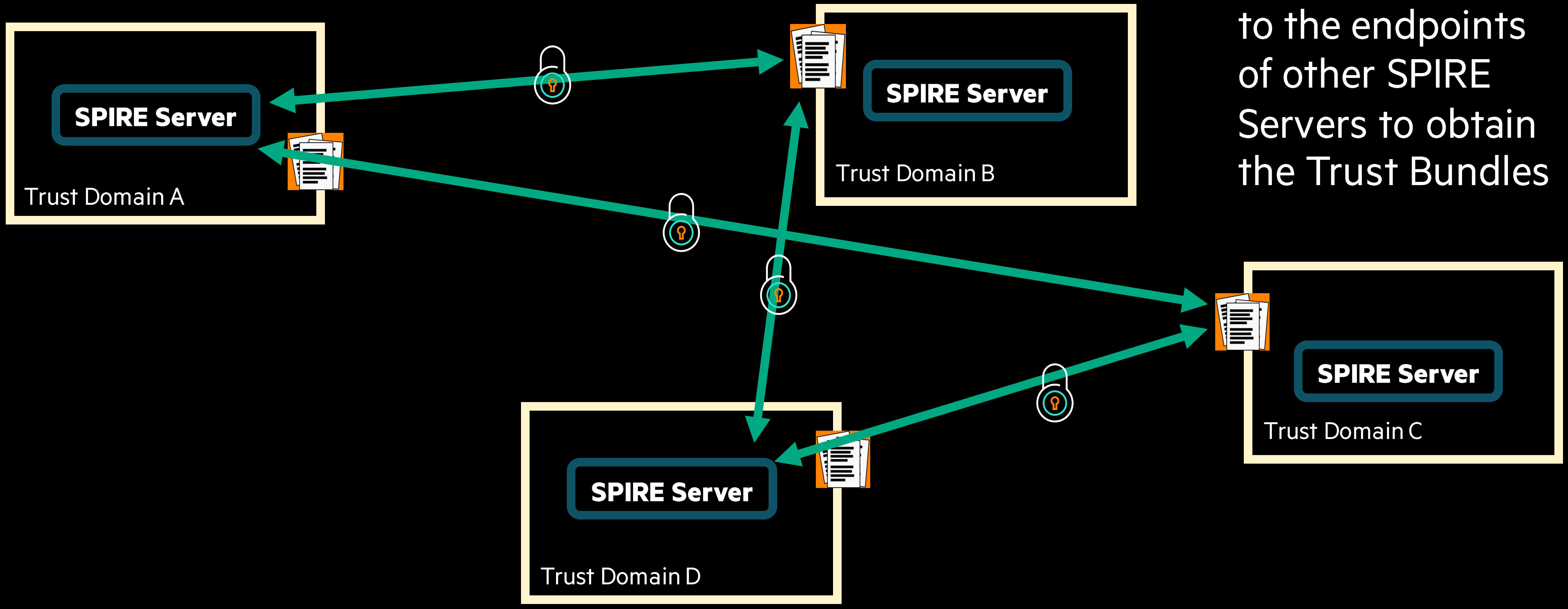


SPIRE FEDERATION: DIFFICULTIES



Each SPIRE Server needs to expose an Endpoint to serve its Trust Bundle

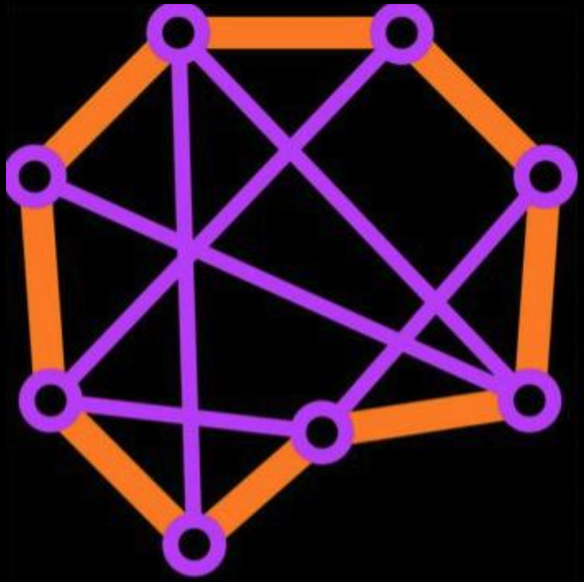
SPIRE FEDERATION: DIFFICULTIES



Each SPIRE Server needs to be configured to connect securely to the endpoints of other SPIRE Servers to obtain the Trust Bundles

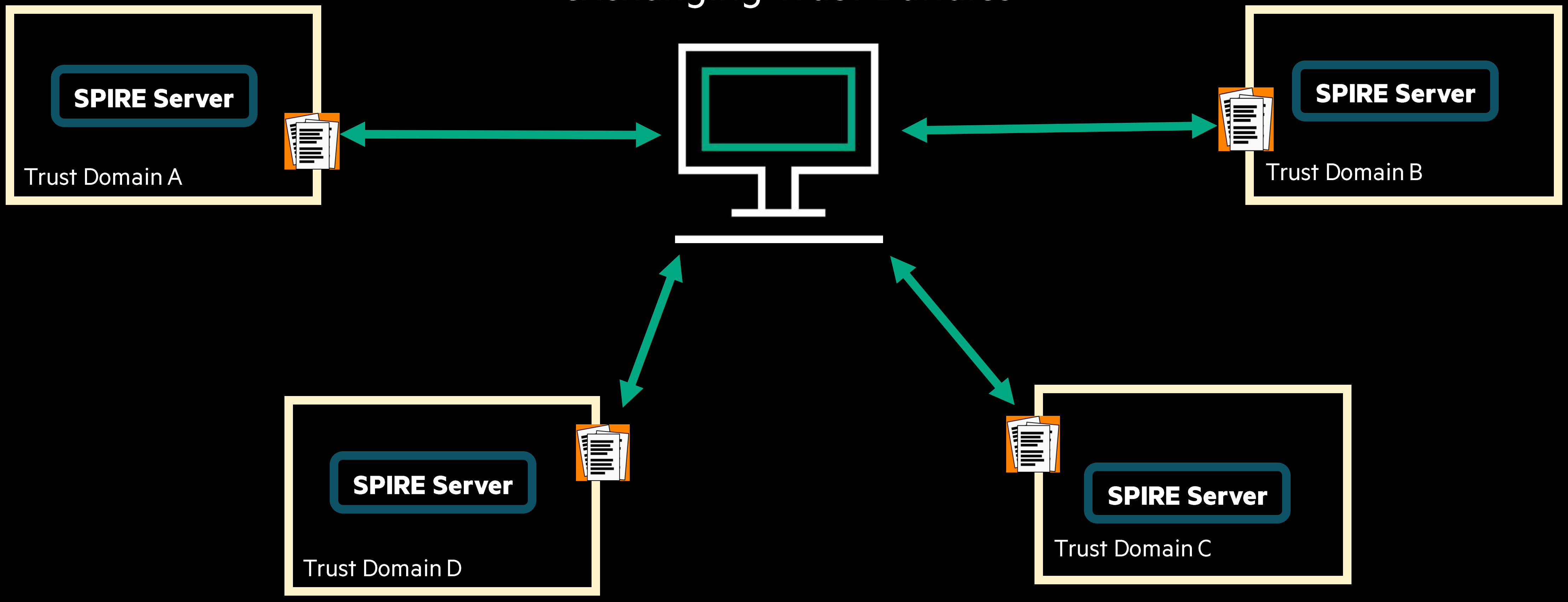
What if we could federate Trust Domains in an easier and scalable way?

Project Galadriel

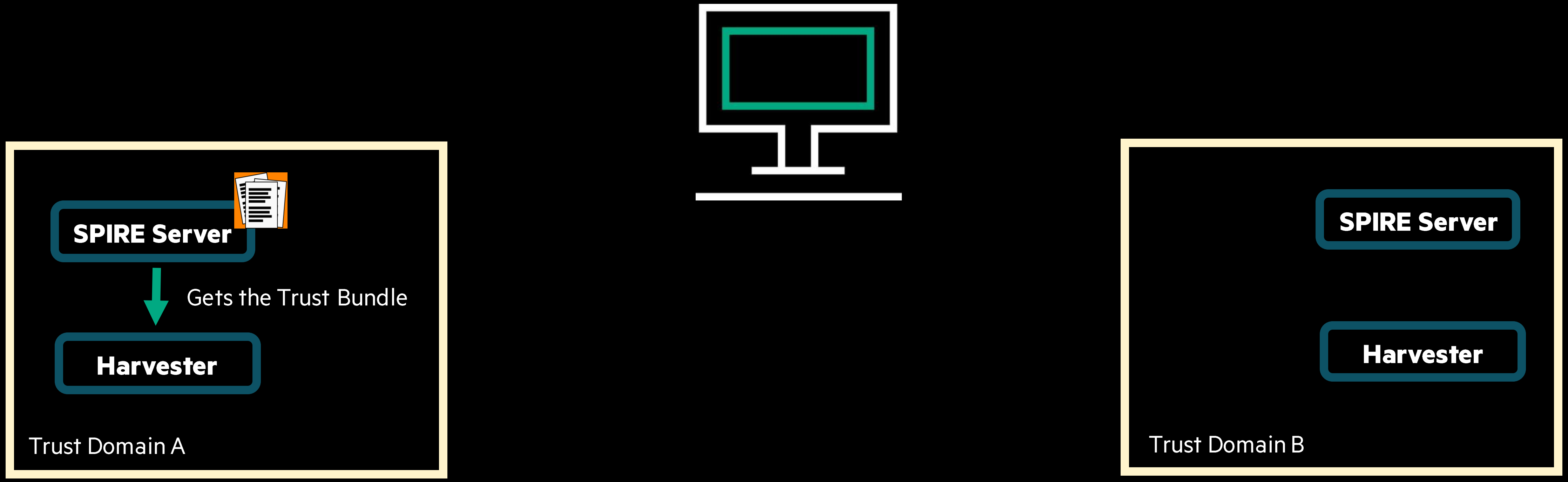


GALADRIEL: FEDERATION AT SCALE

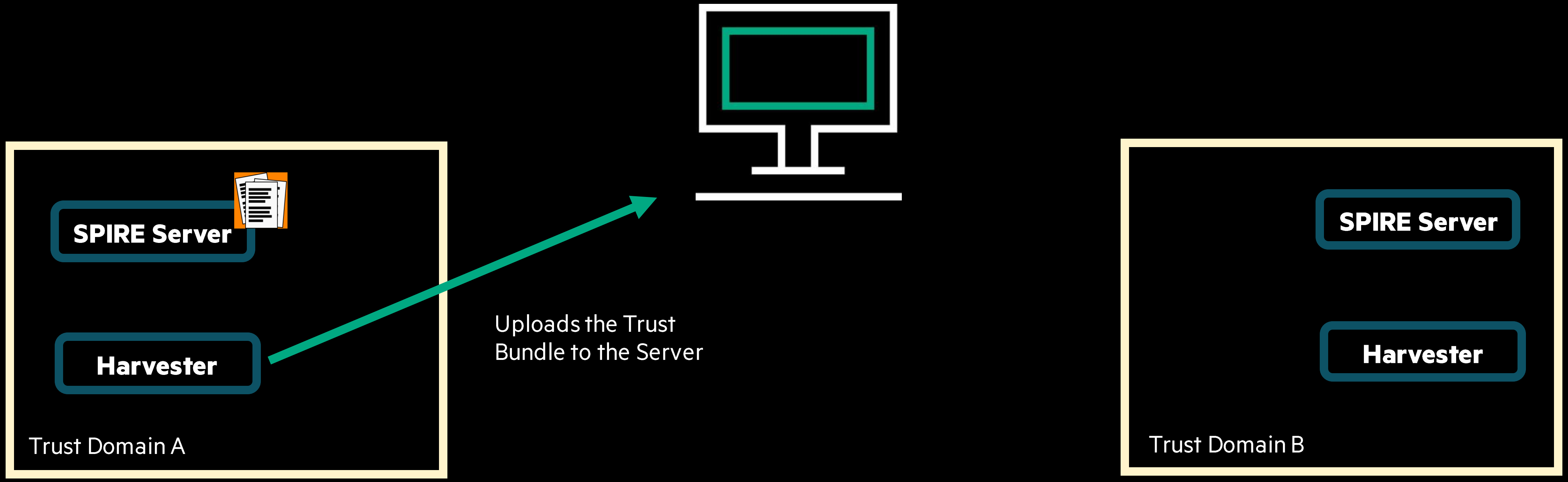
Central Hub for configuring Federation Relationships and exchanging Trust Bundles



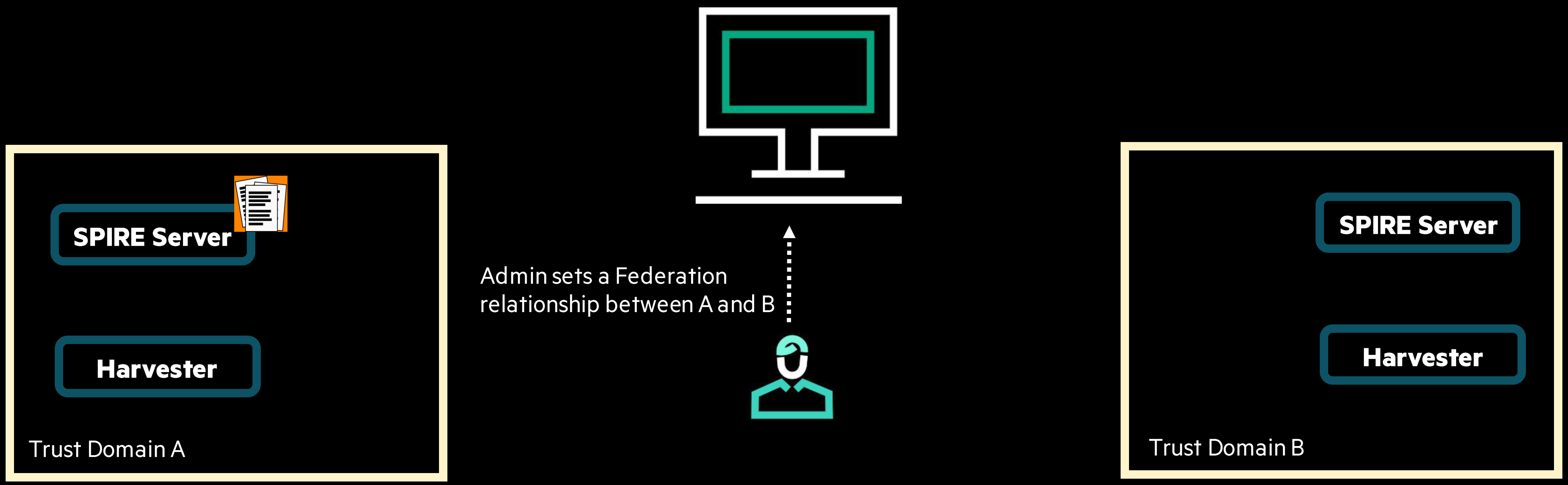
GALADRIEL: HOW IT WORKS



GALADRIEL: HOW IT WORKS



GALADRIEL: HOW IT WORKS



SPIRE Server

Harvester

Trust Domain A

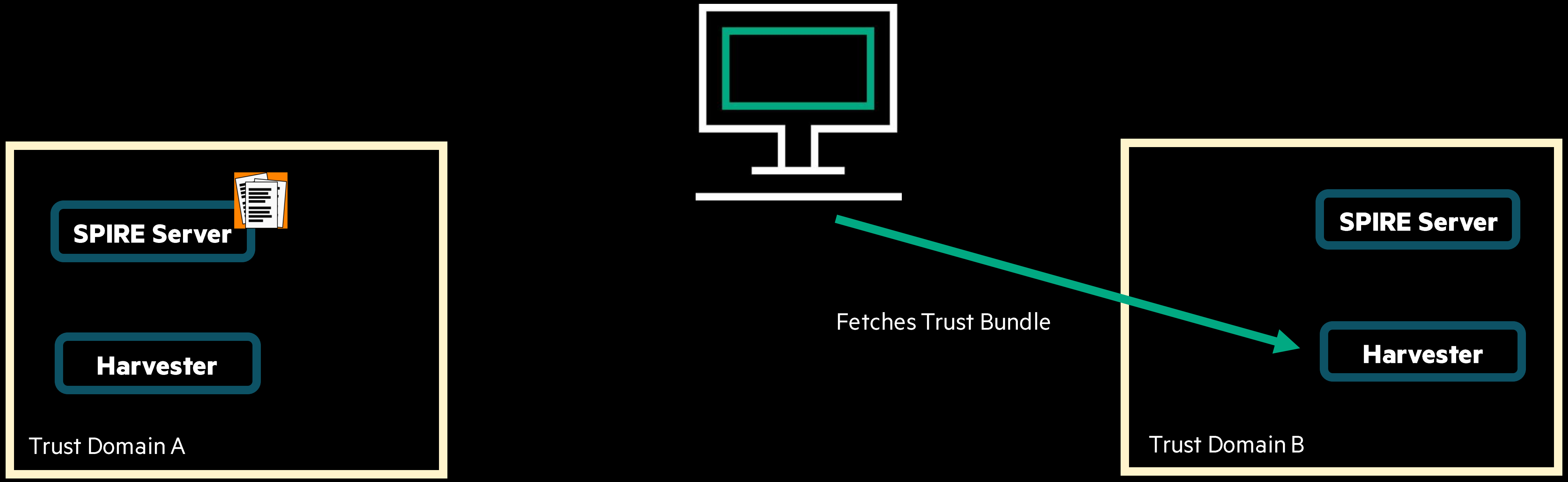
Admin sets a Federation relationship between A and B

SPIRE Server

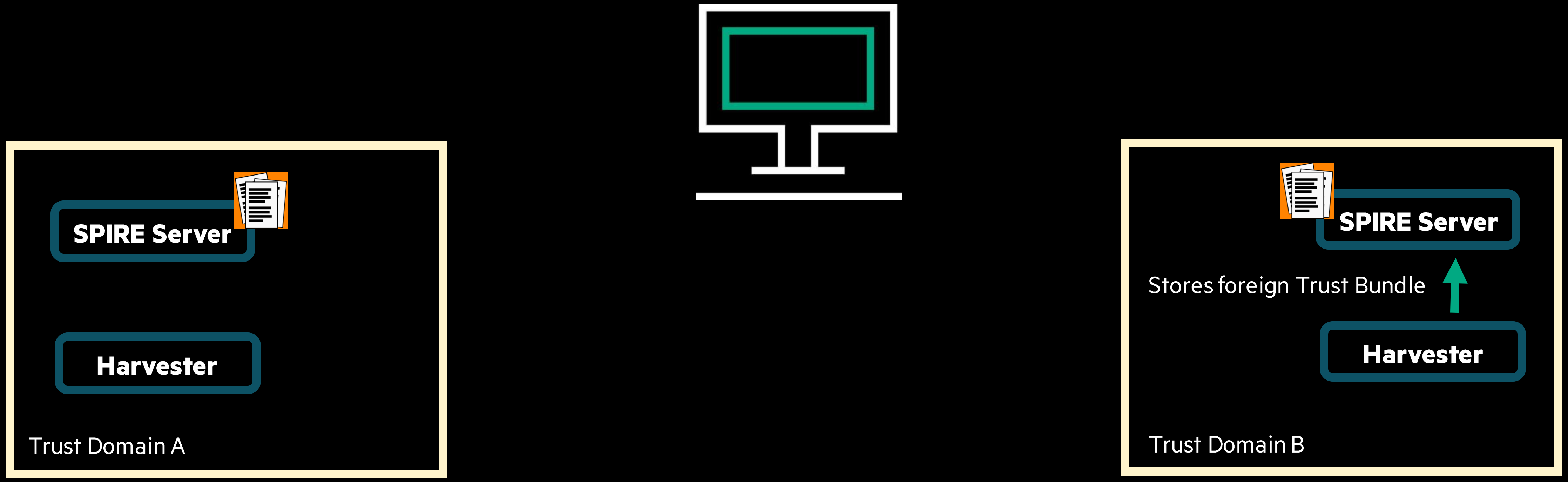
Harvester

Trust Domain B

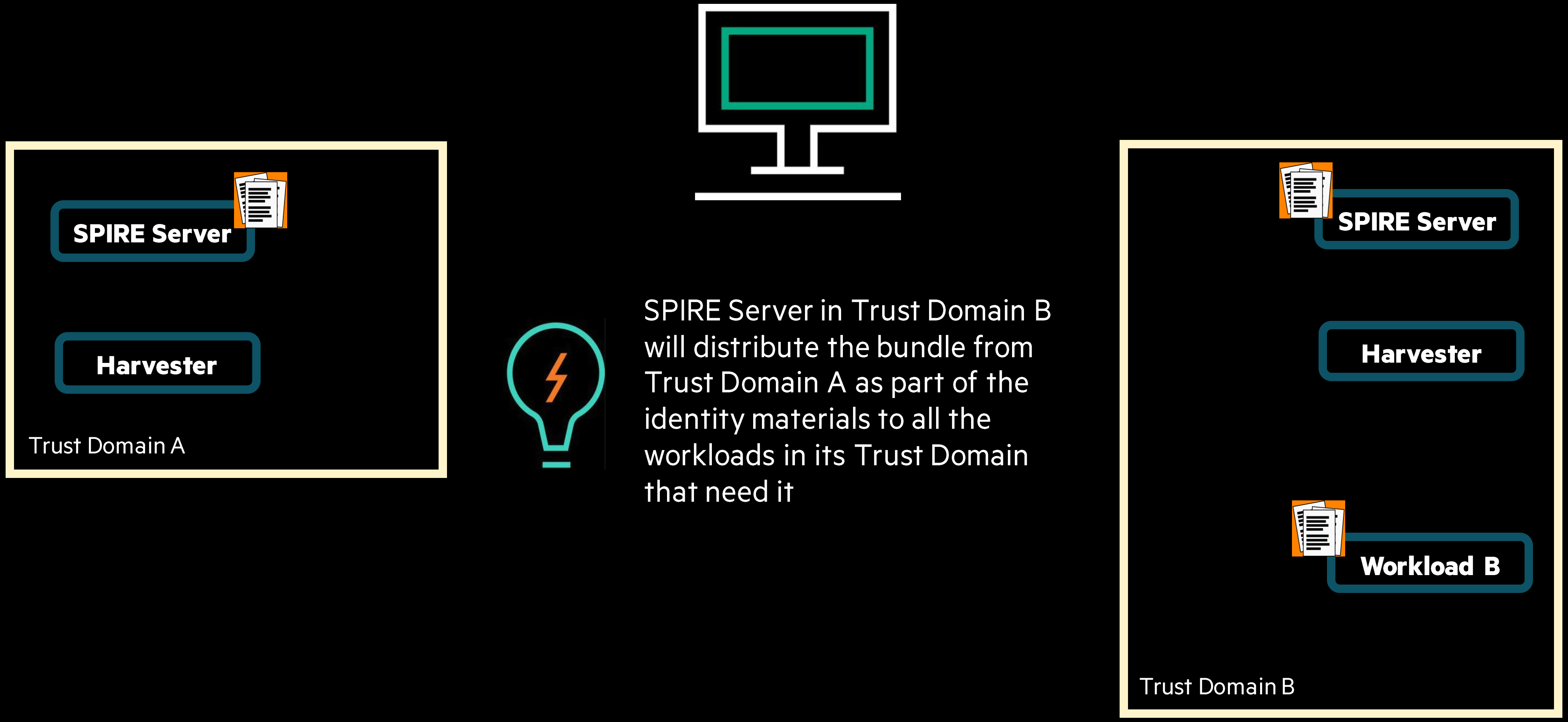
GALADRIEL: HOW IT WORKS



GALADRIEL: HOW IT WORKS

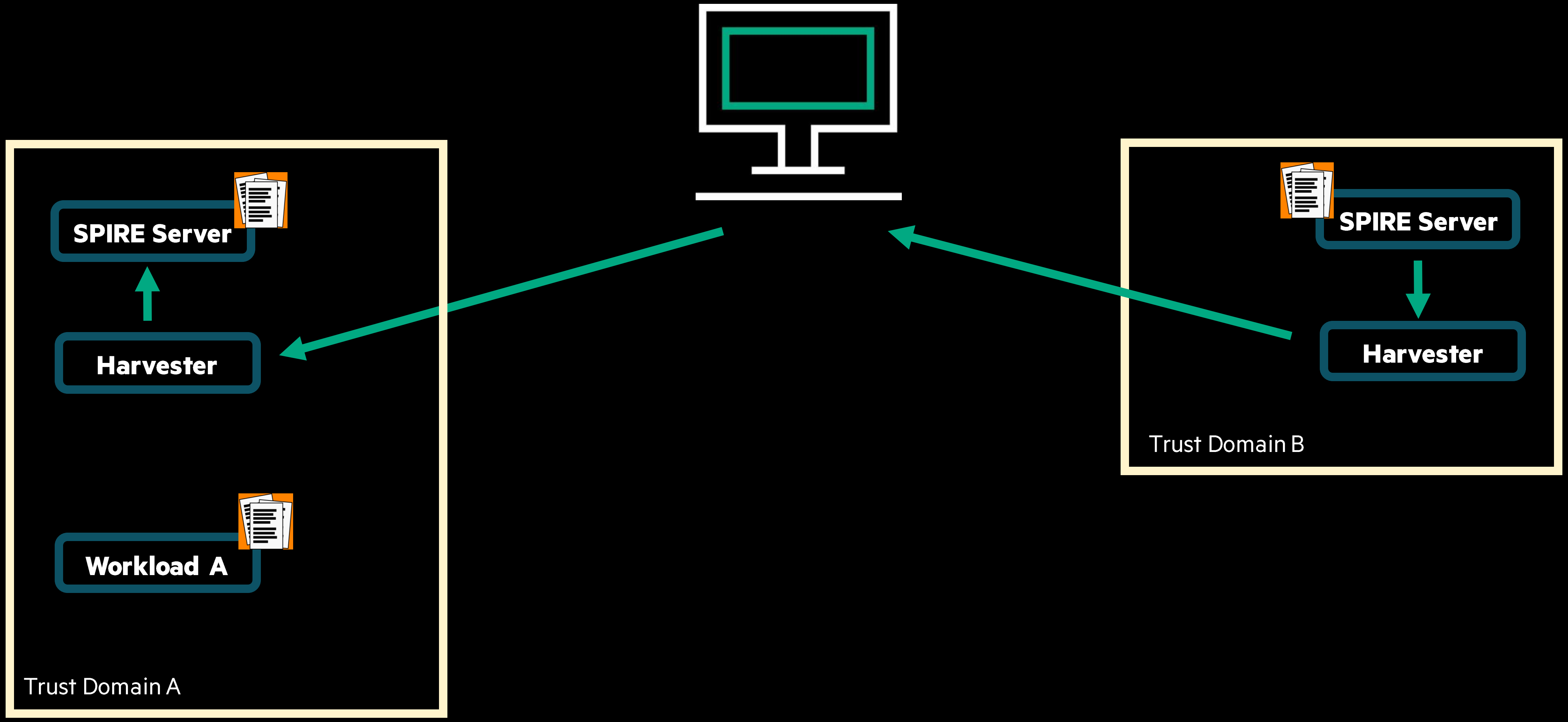


GALADRIEL: HOW IT WORKS

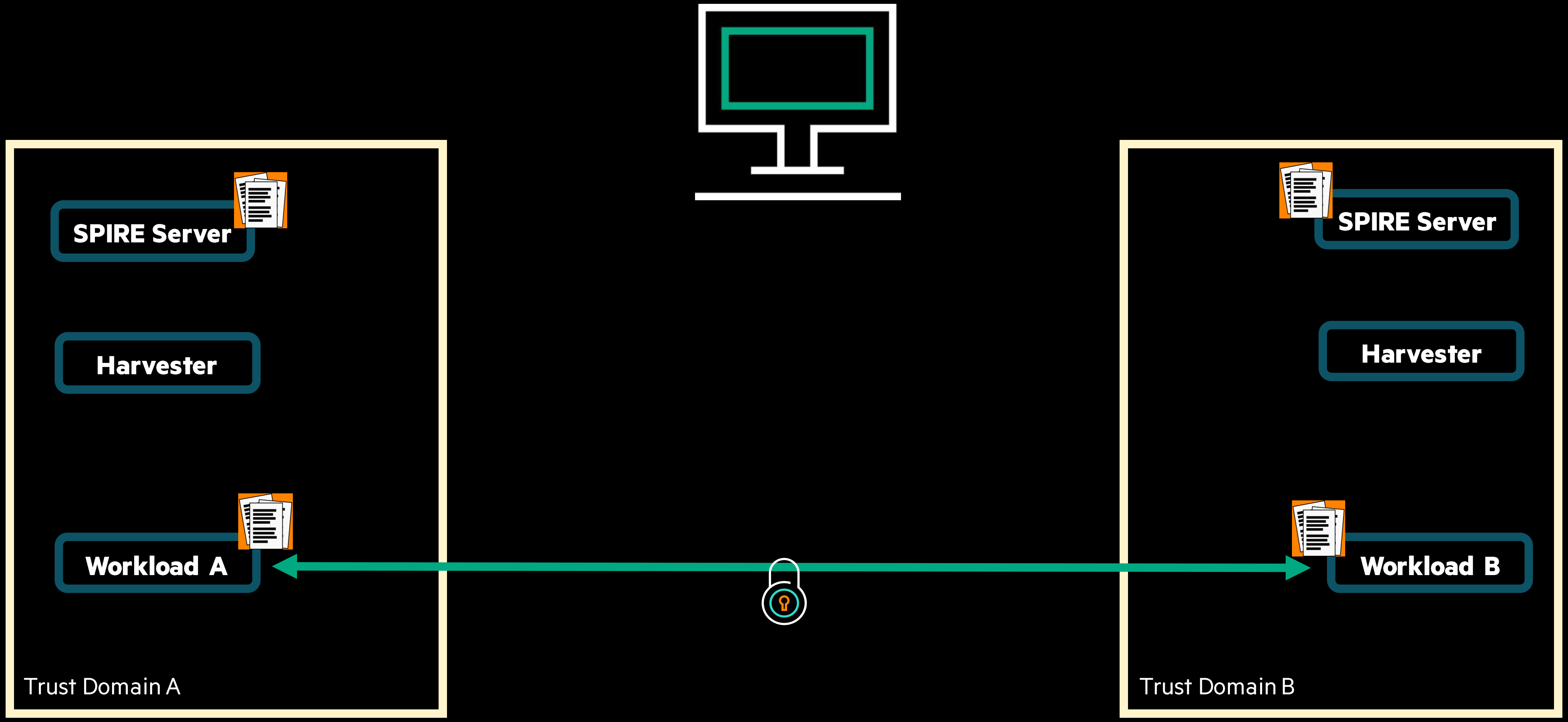


SPIRE Server in Trust Domain B will distribute the bundle from Trust Domain A as part of the identity materials to all the workloads in its Trust Domain that need it

GALADRIEL: HOW IT WORKS



GALADRIEL: HOW IT WORKS



GALADRIEL: WHAT IS

- Alternative approach to SPIRE Federation
- Federation at scale – ease management and audit
- Central hub – federation control plane
- Open source ♥

GALADRIEL: WHAT IS NOT

○ Replacement for SPIRE/SPIFFE Federation

○ SPIRE plugin (not yet)

GALADRIEL: THE FOUNDATIONS

- Explicit mutual consent for Federation Relationships
- Integrity verification end-to-end (Bundle Integrity)
- Auditable

GALADRIEL: ARCHITECTURE

Galadriel Server

- Exchange hub for Trust domains and their Trust Bundles
- Federation relationships and consents

GALADRIEL: ARCHITECTURE

Galadriel Certificate Authority (CA)

- Root of Trust for all Harvesters
- Sign certificates to enable trust bundle signing (Bundle integrity)

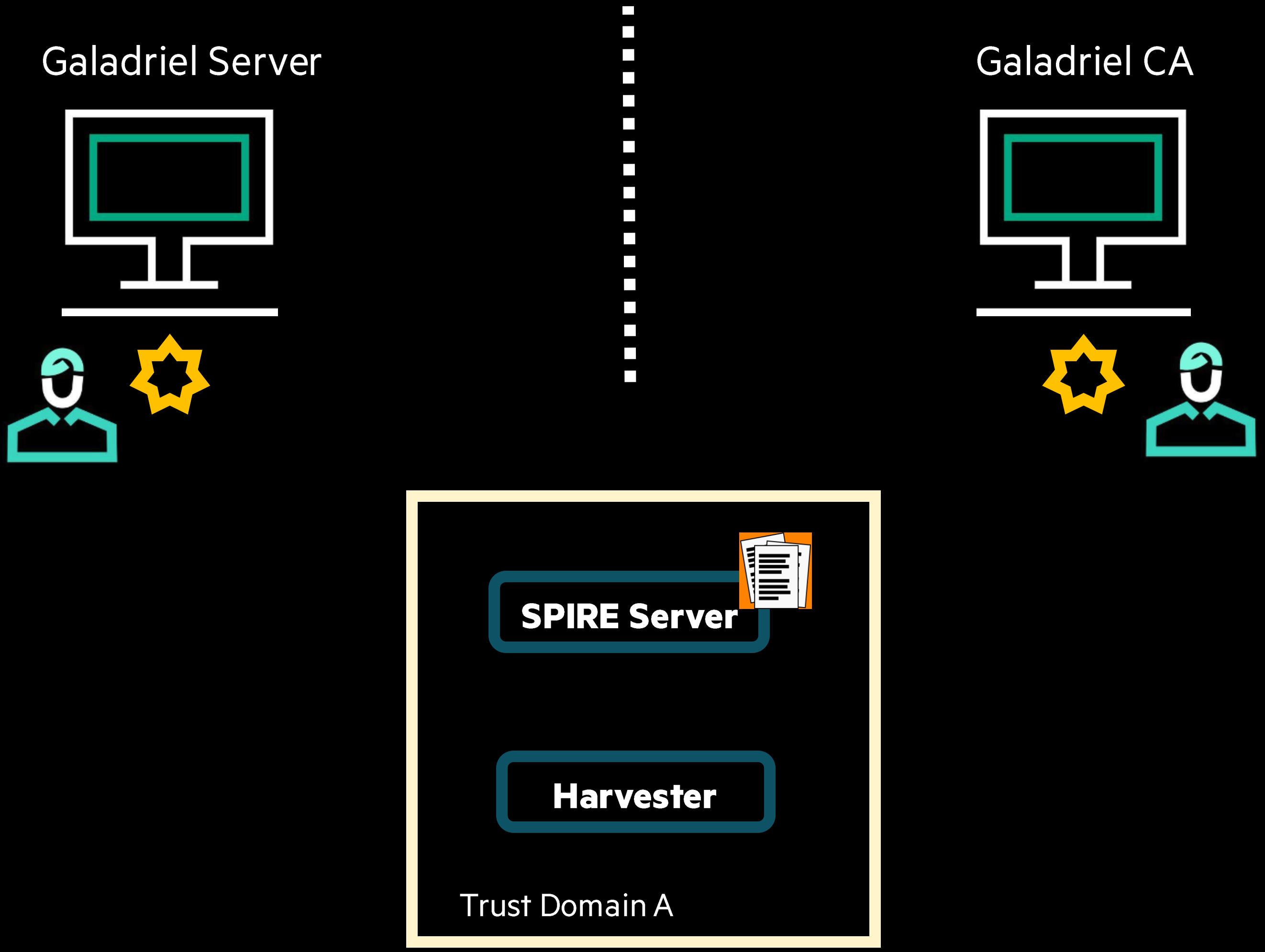
GALADRIEL: ARCHITECTURE

Galadriel Harvester

- Run alongside each SPIRE Server
- Steers Trust Bundles distribution between SPIRE Server and Galadriel Server
- Sign and verify Trust Bundles
- Accept and verify federation relationships

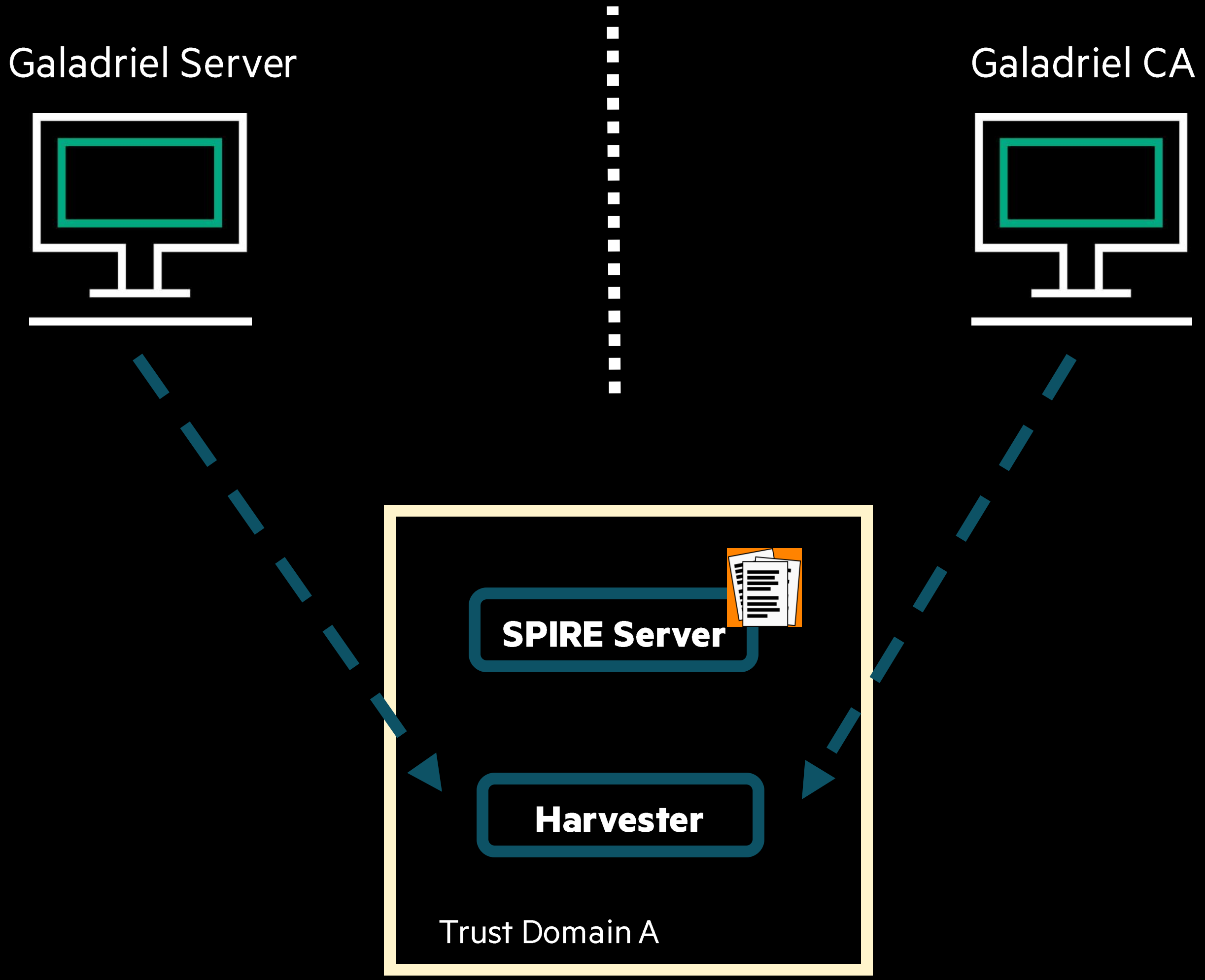
GALADRIEL: TRUST BUNDLE INTEGRITY

Harvester onboarding



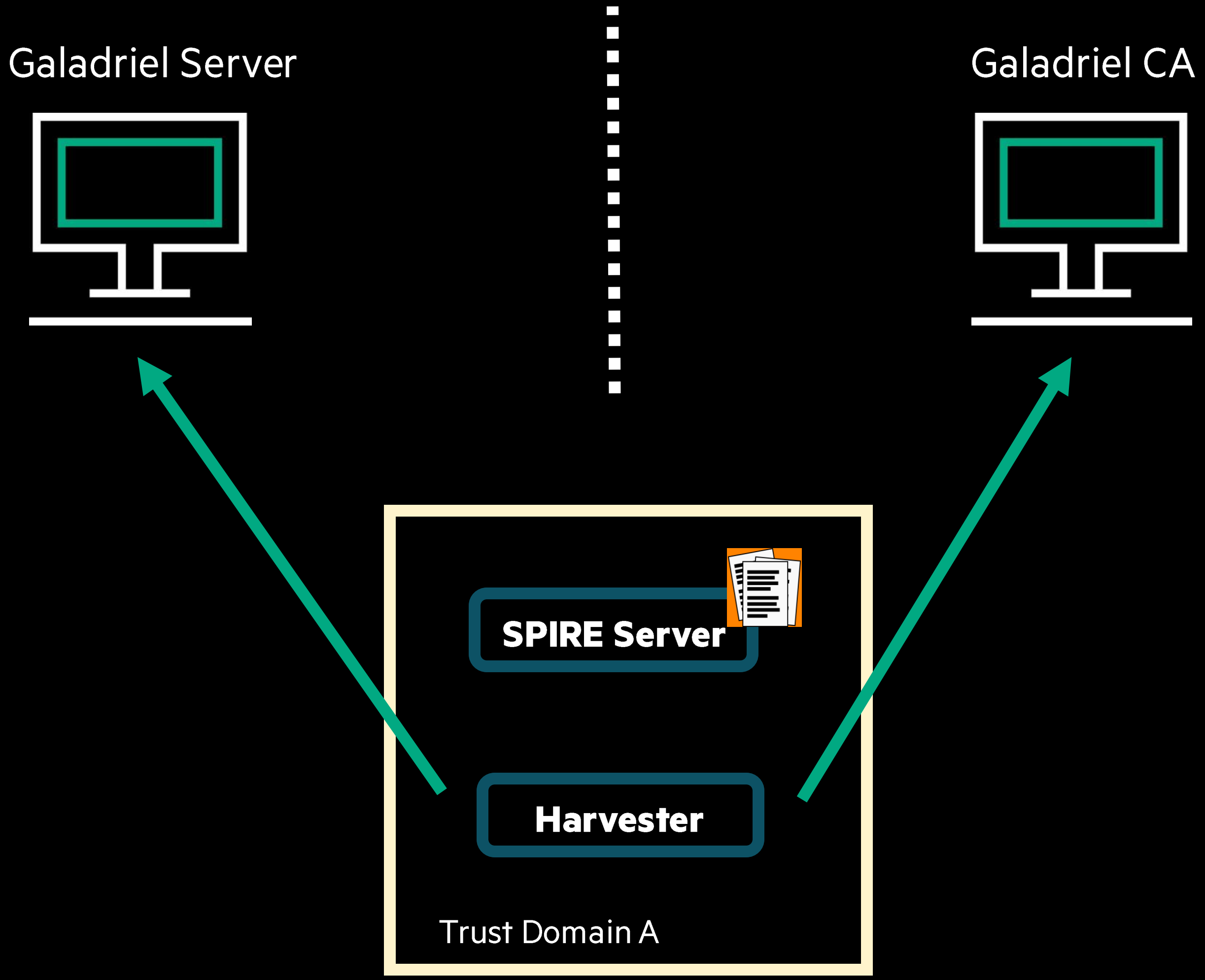
GALADRIEL: TRUST BUNDLE INTEGRITY

Harvester onboarding

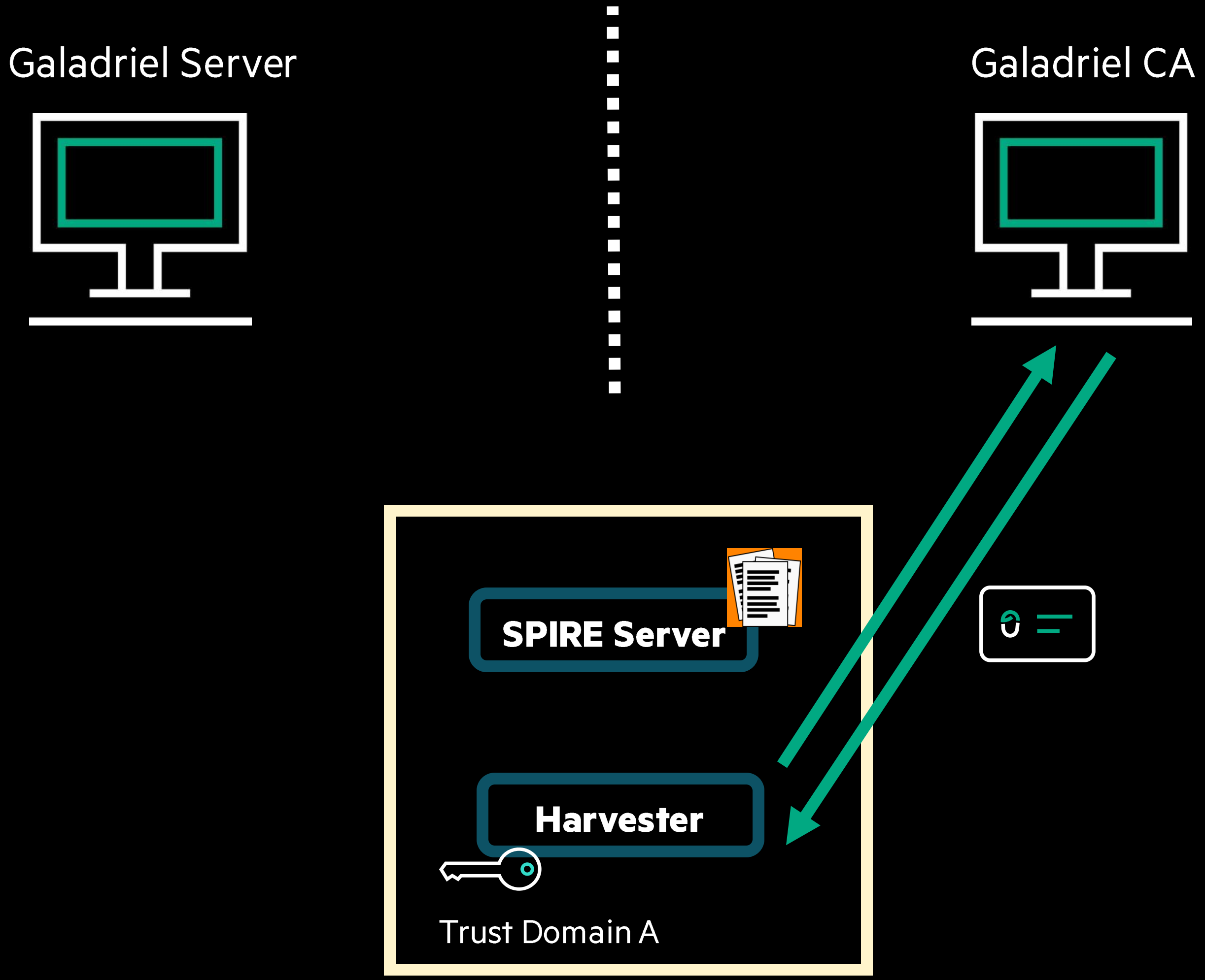


GALADRIEL: TRUST BUNDLE INTEGRITY

Secure introduction



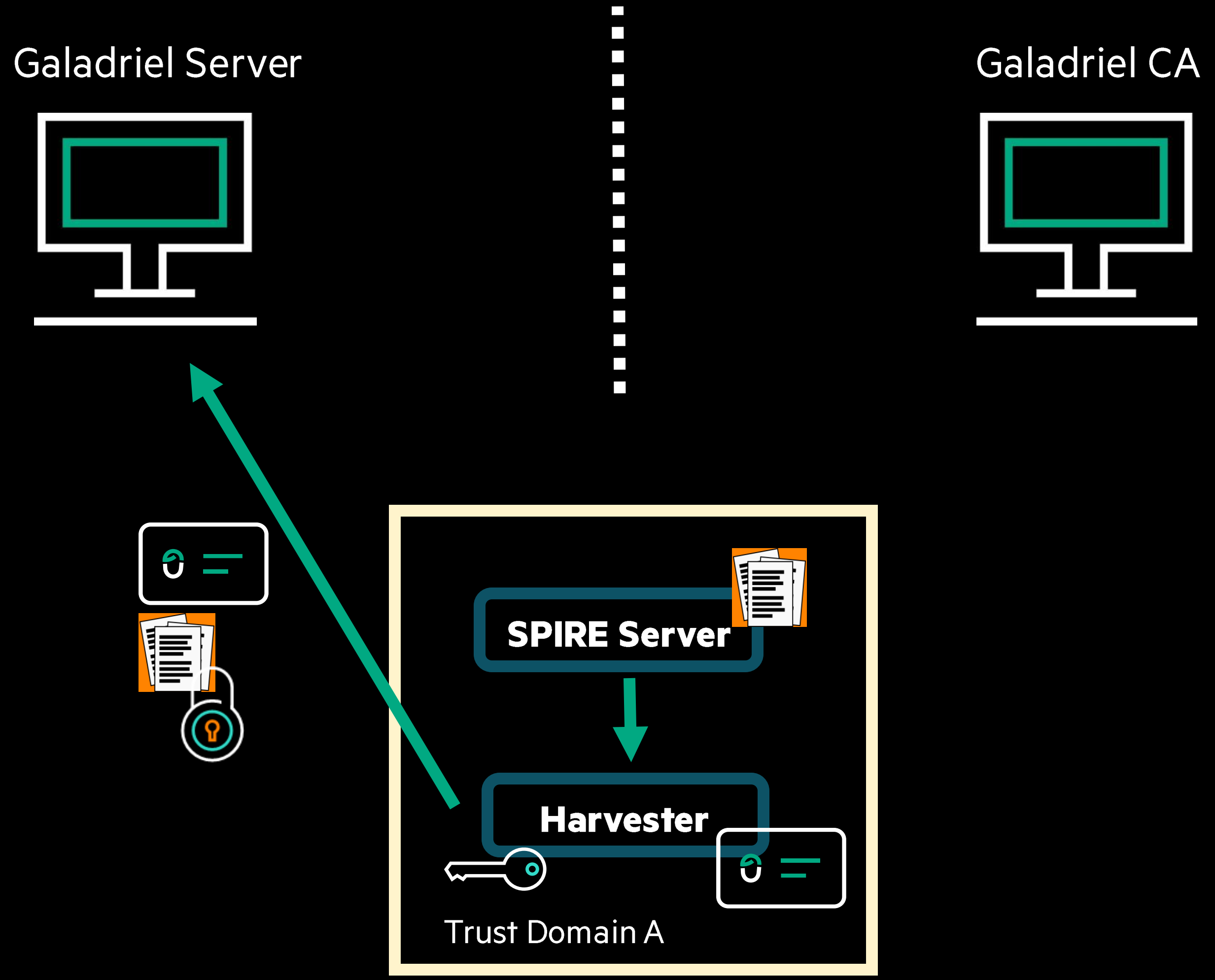
GALADRIEL: TRUST BUNDLE INTEGRITY



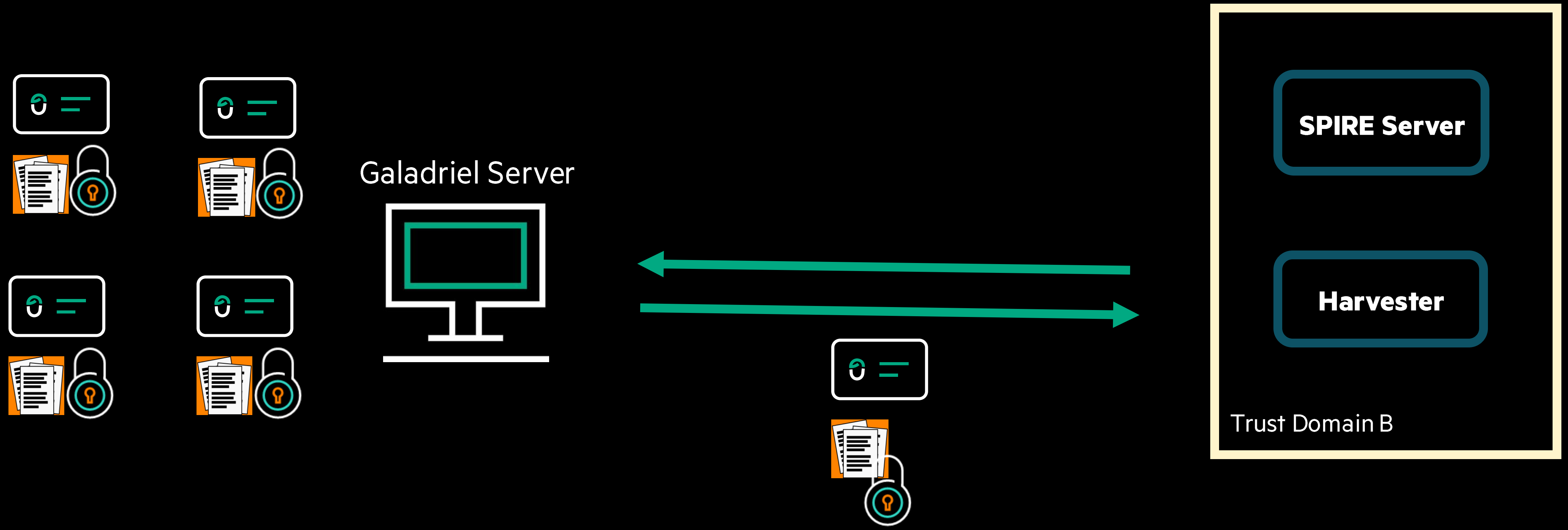
Signing material

GALADRIEL: TRUST BUNDLE INTEGRITY

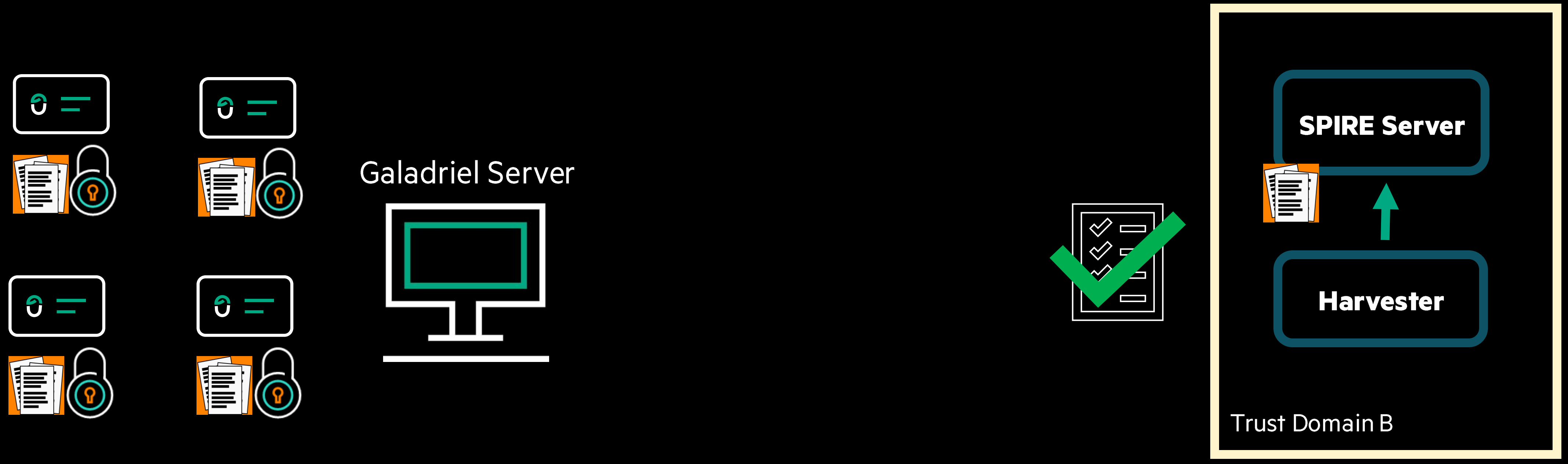
Trust bundle uploading



GALADRIEL: TRUST BUNDLE INTEGRITY

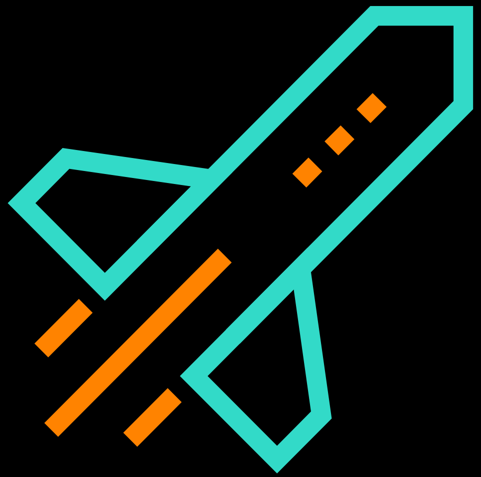


GALADRIEL: TRUST BUNDLE INTEGRITY

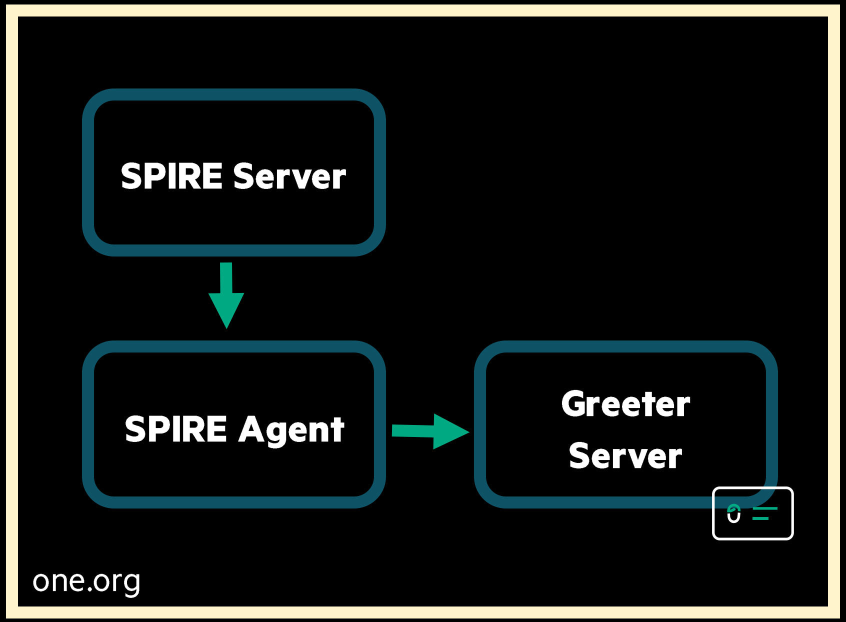


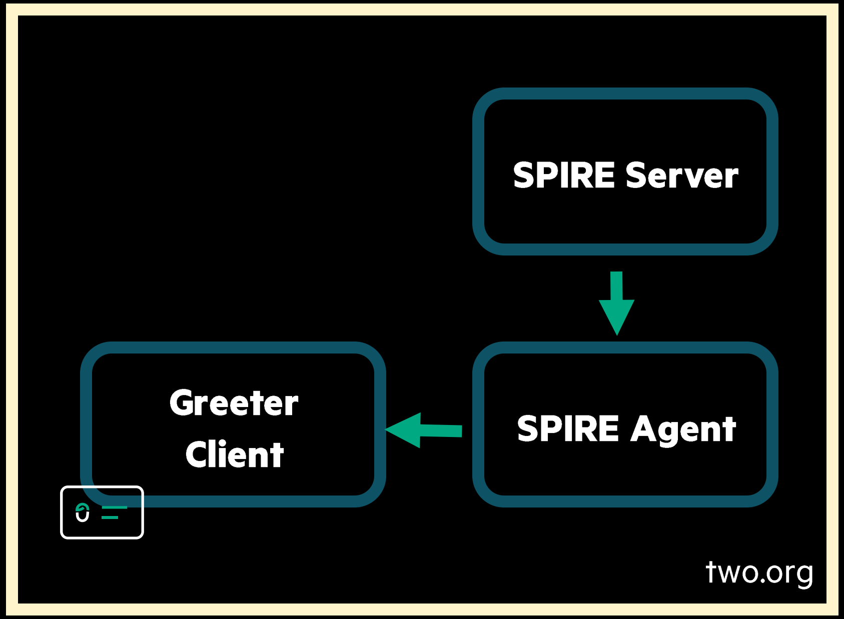
✓ Harvester A identity issued by Galadriel CA
✓ Trust Bundle signed by Harvester A
✓ Trust Bundle belongs to consented Trust Domain

Demo time

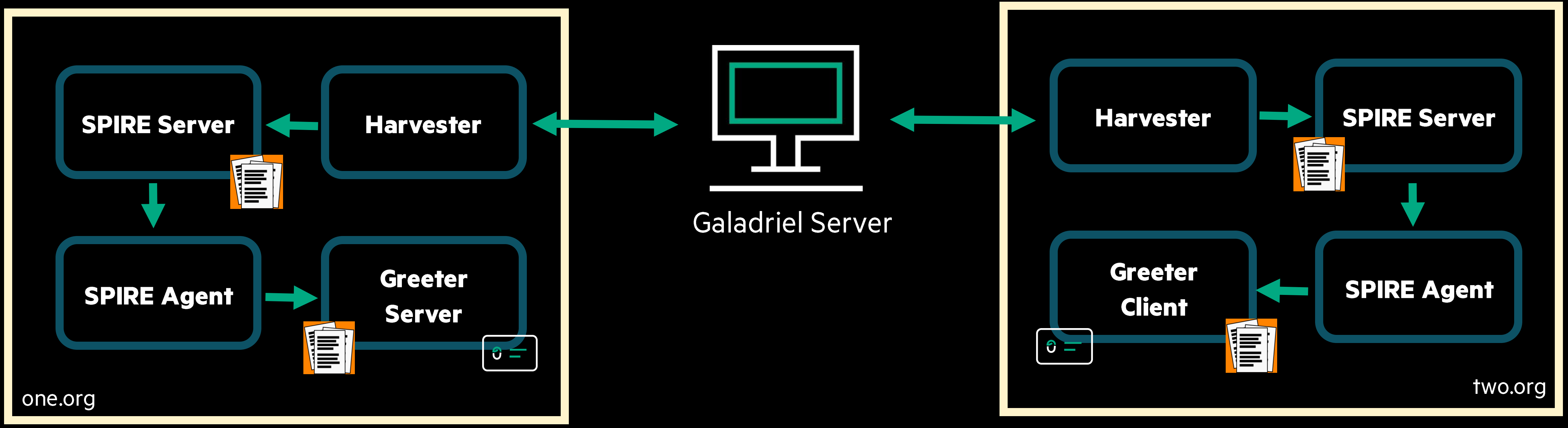


DEMO

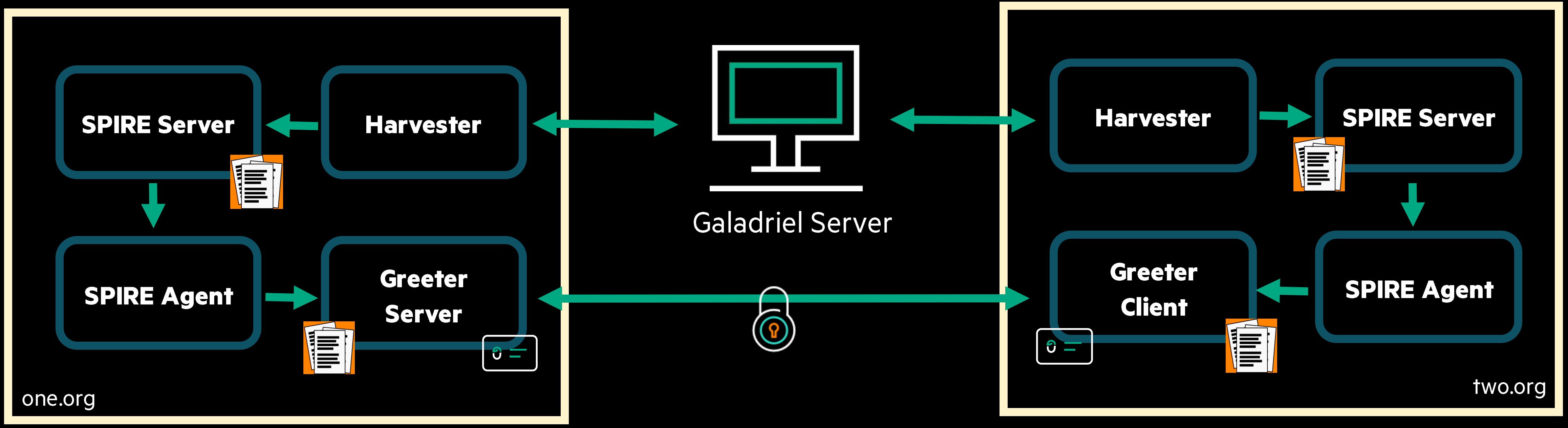

SPIRE Server
SPIRE Agent
Greeter Server
one.org


SPIRE Server
Greeter Client
SPIRE Agent
two.org

DEMO


SPIRE Server
Harvester
SPIRE Agent
Greeter
Server
one.org
Galadriel Server
Harvester
SPIRE Server
Greeter
Client
SPIRE Agent
two.org

DEMO


SPIRE Server
Harvester
SPIRE Agent
Greeter
Server
one.org
Galadriel Server
Harvester
SPIRE Server
Greeter
Client
SPIRE Agent
two.org

THANK YOU

Max Lambrecht
max.lambrecht@hpe.com
Slack.spiffe.io

Maximiliano Churichi
maximiliano.churichi@hpe.com
Slack.spiffe.io