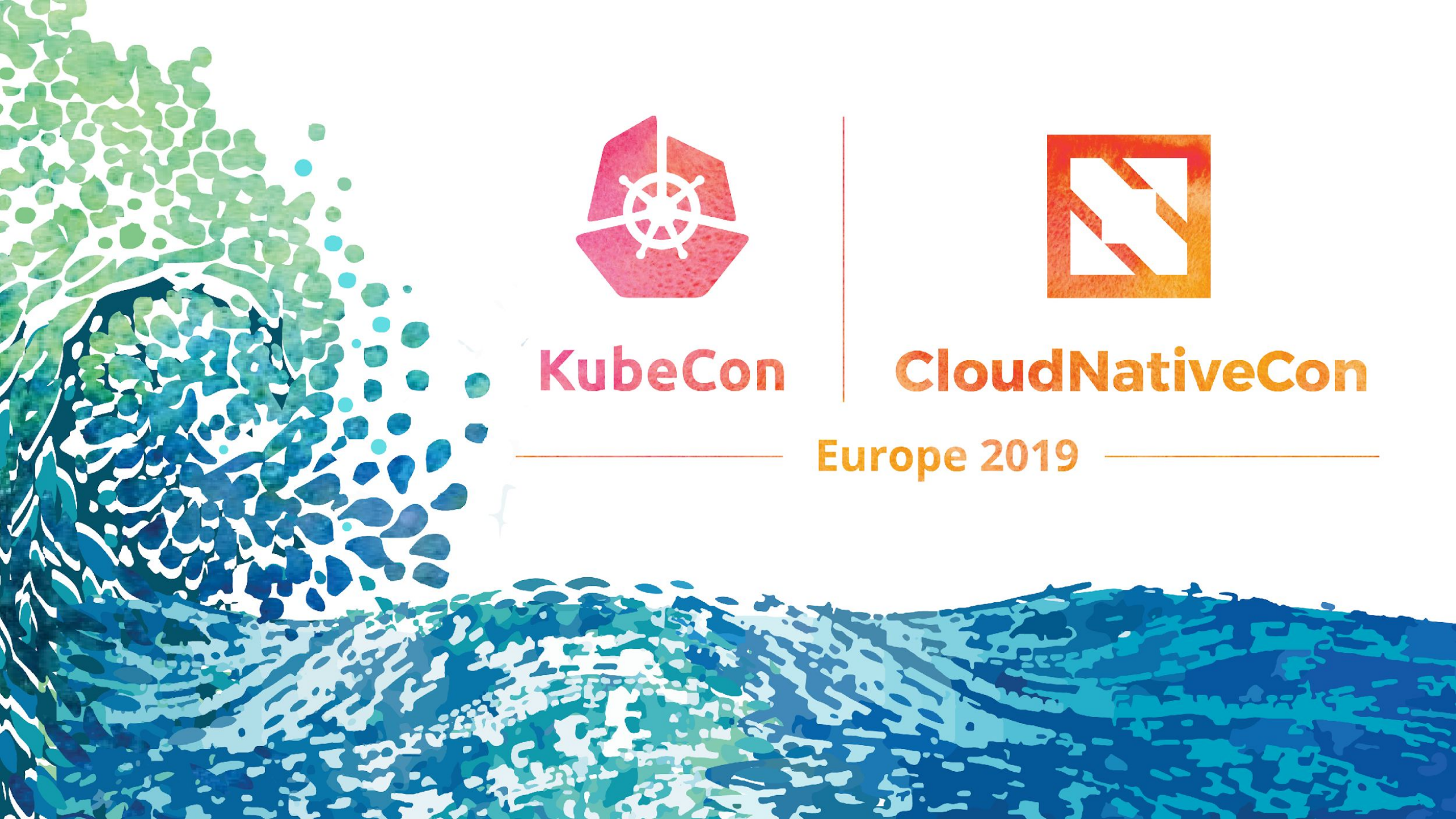

KubeCon
CloudNativeCon
Europe 2019

Zero Trust service mesh with Calico, SPIRE, and Envoy

Evan Gilman (Scytale) and Shaun Crampton (Tigera)

Agenda

KubeCon

CloudNativeCon

Europe 2019

What is Zero Trust?

What is a Service Mesh?

SPIFFE/SPIRE Overview

Calico Overview

Pulling it All Together

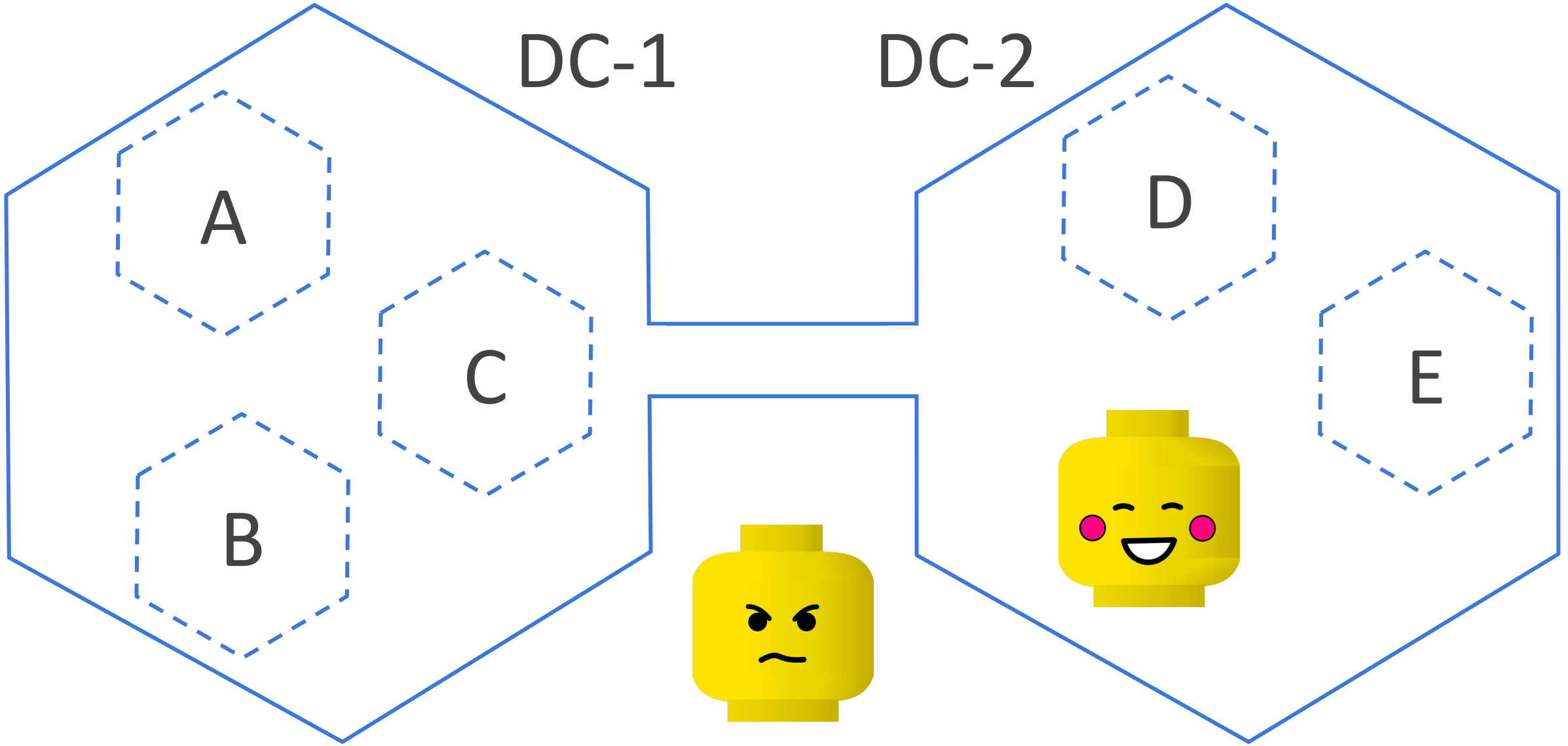
Demo Time!

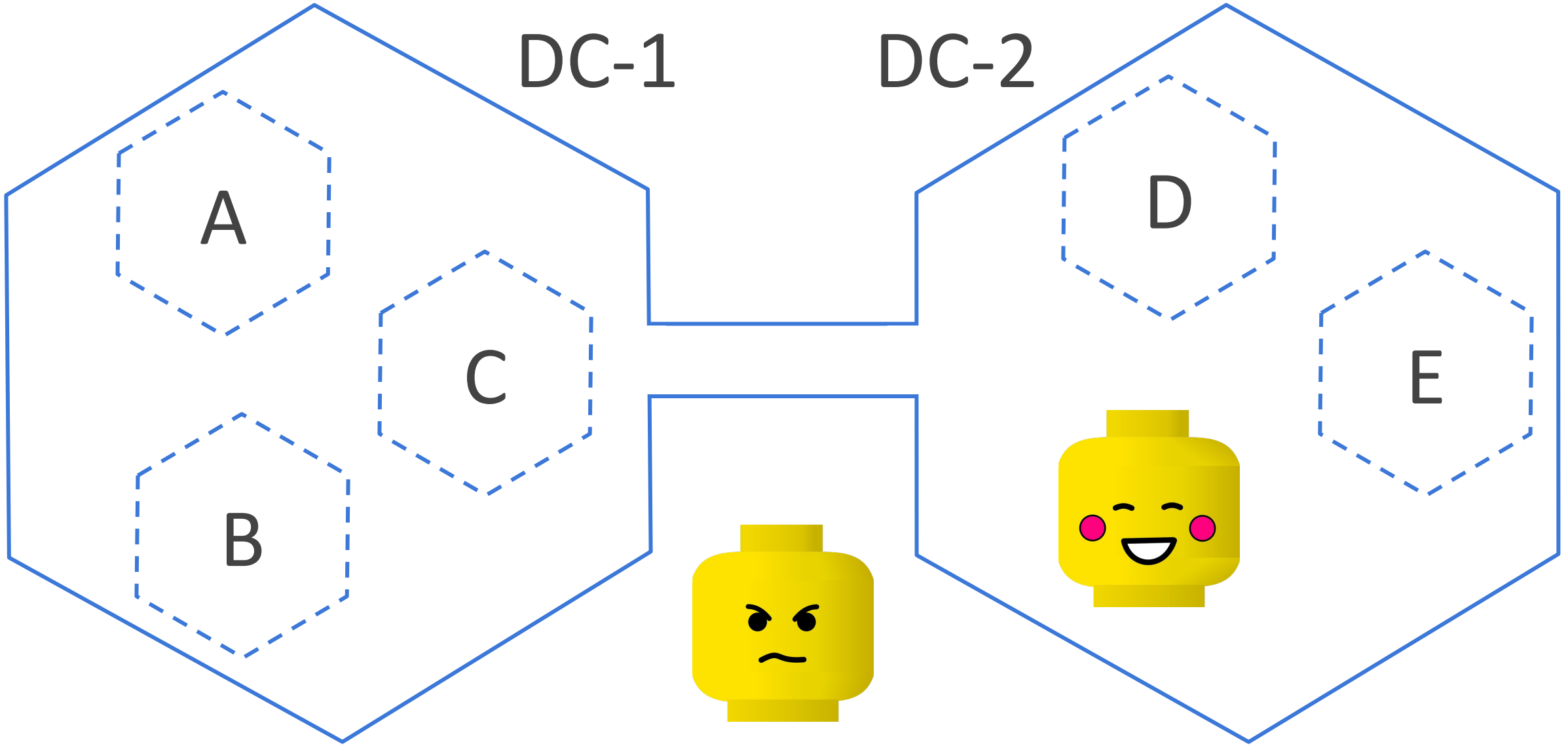
“Zero Trust”

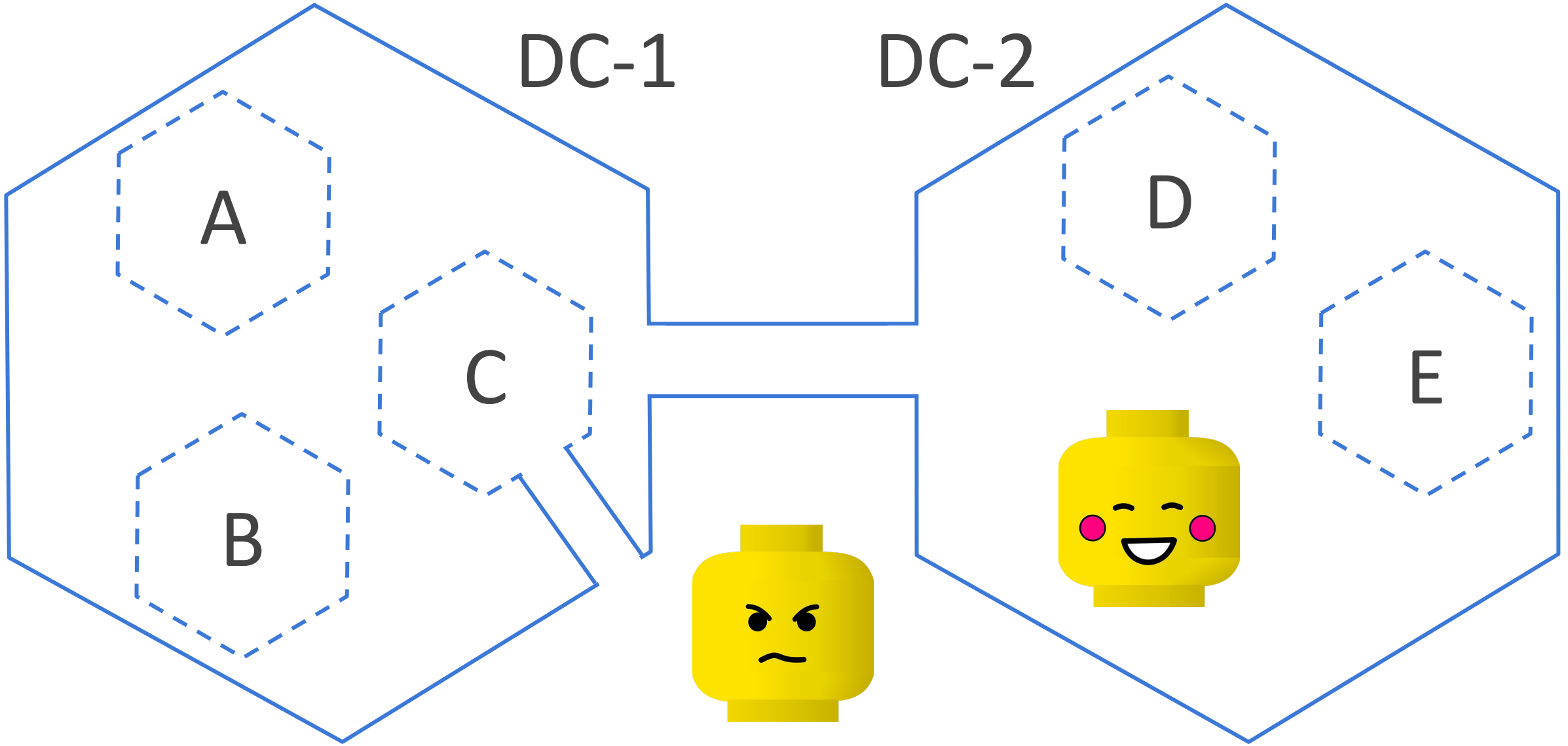
“Zero Trust”

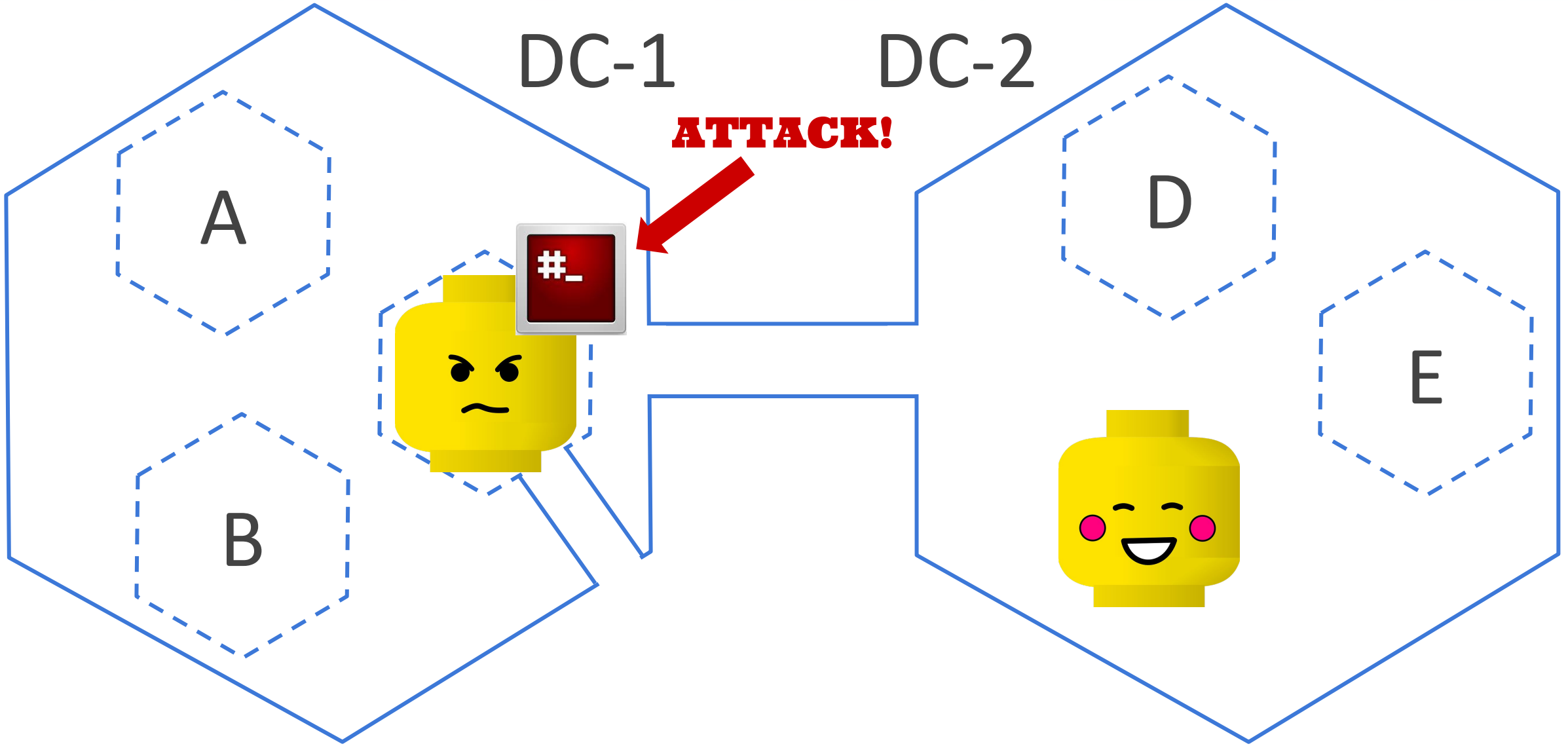
“Zero Trust” (Networks)

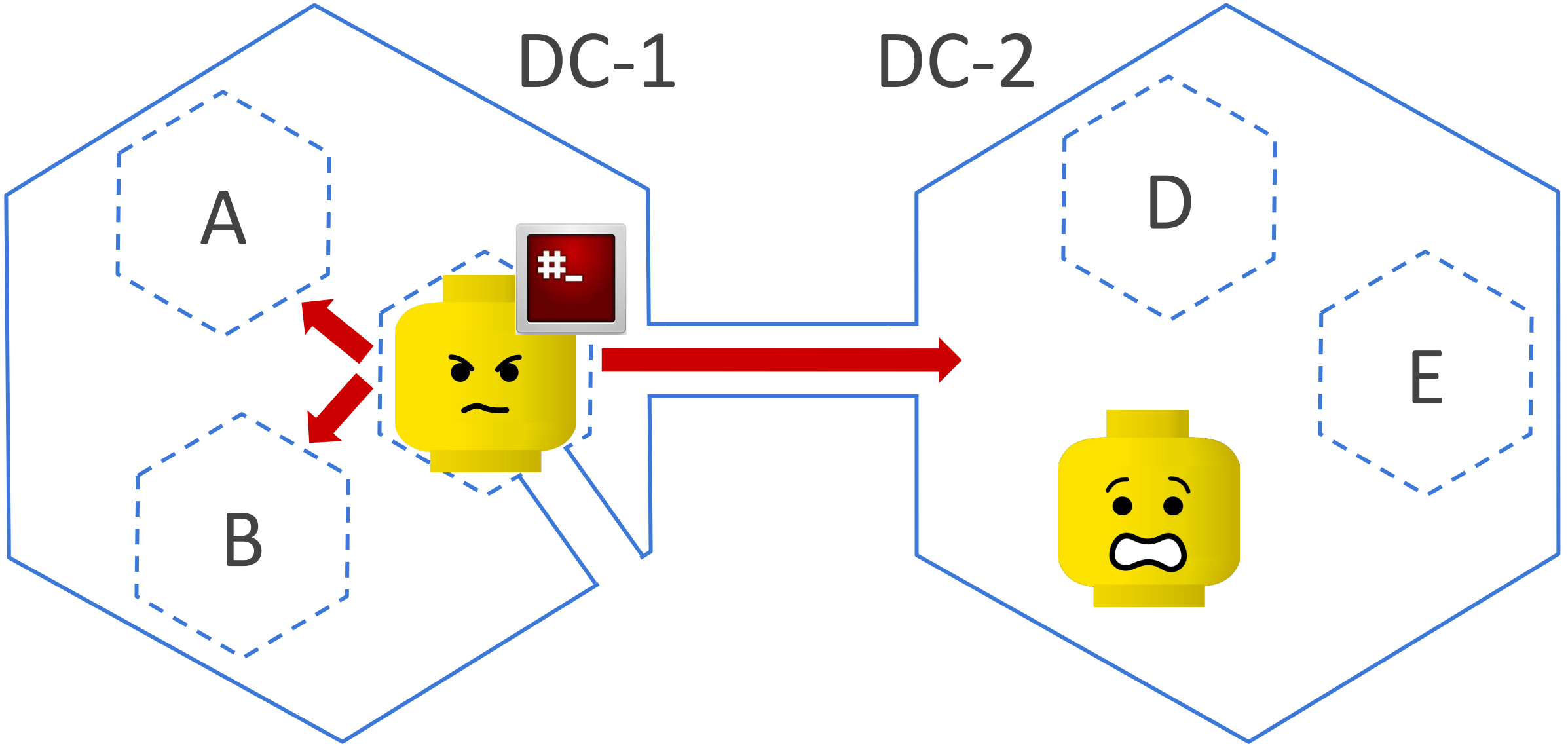
“Zero Trust” (Networks)

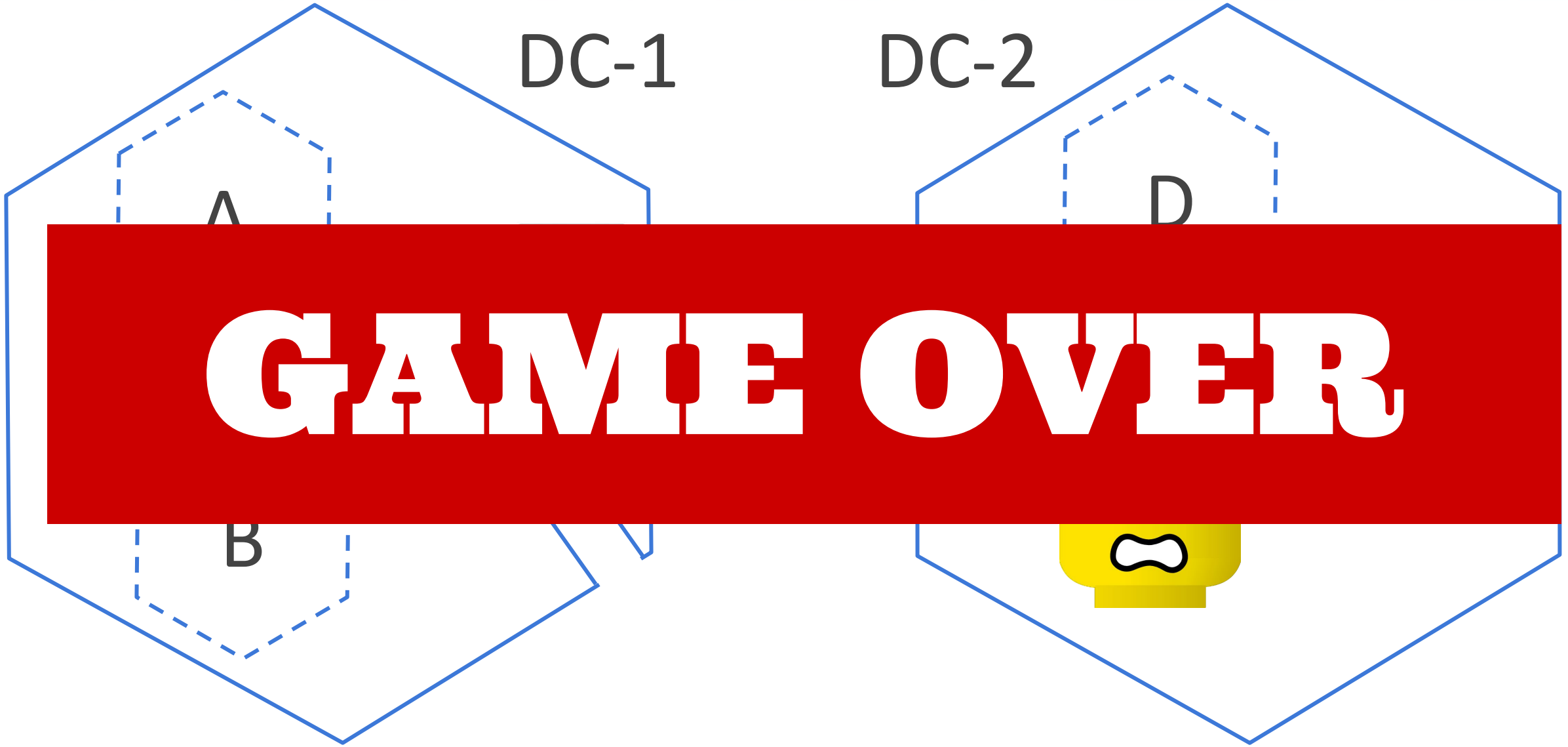

DC-1
DC-2
A
B
C
D
E


DC-1
DC-2
A
B
C
D
E

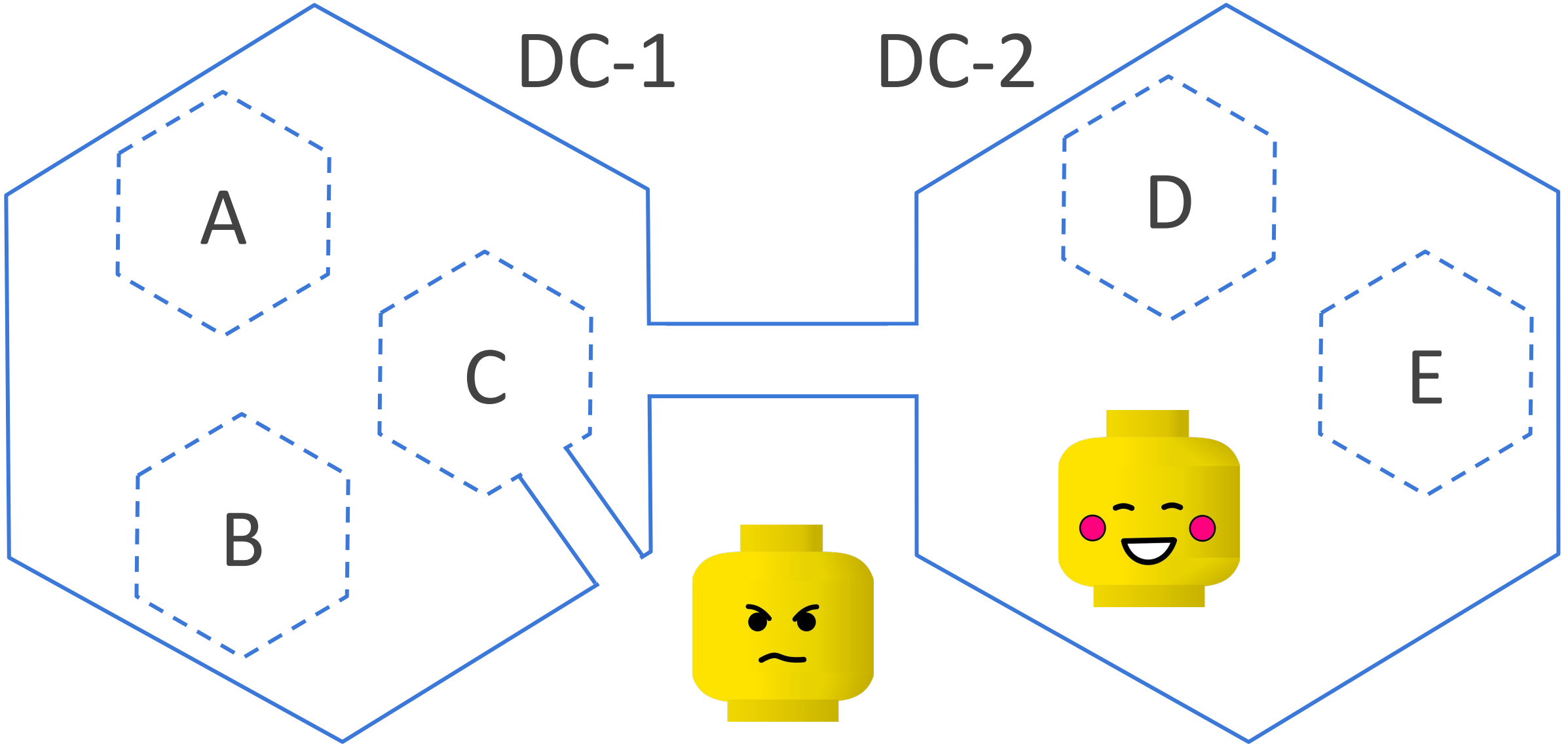

DC-1
DC-2
A
B
C
D
E

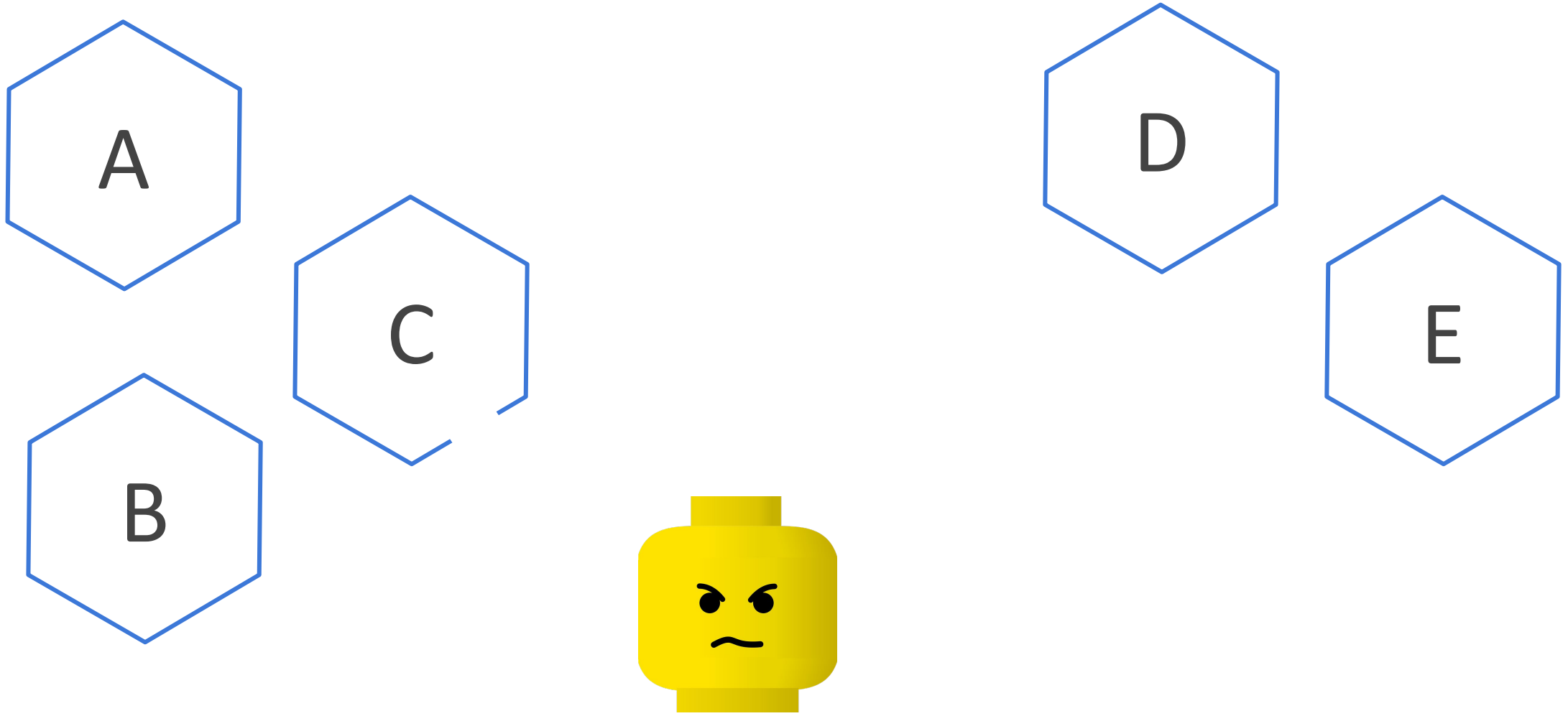

DC-1
DC-2
ATTACK!
A
B
D
E
#_

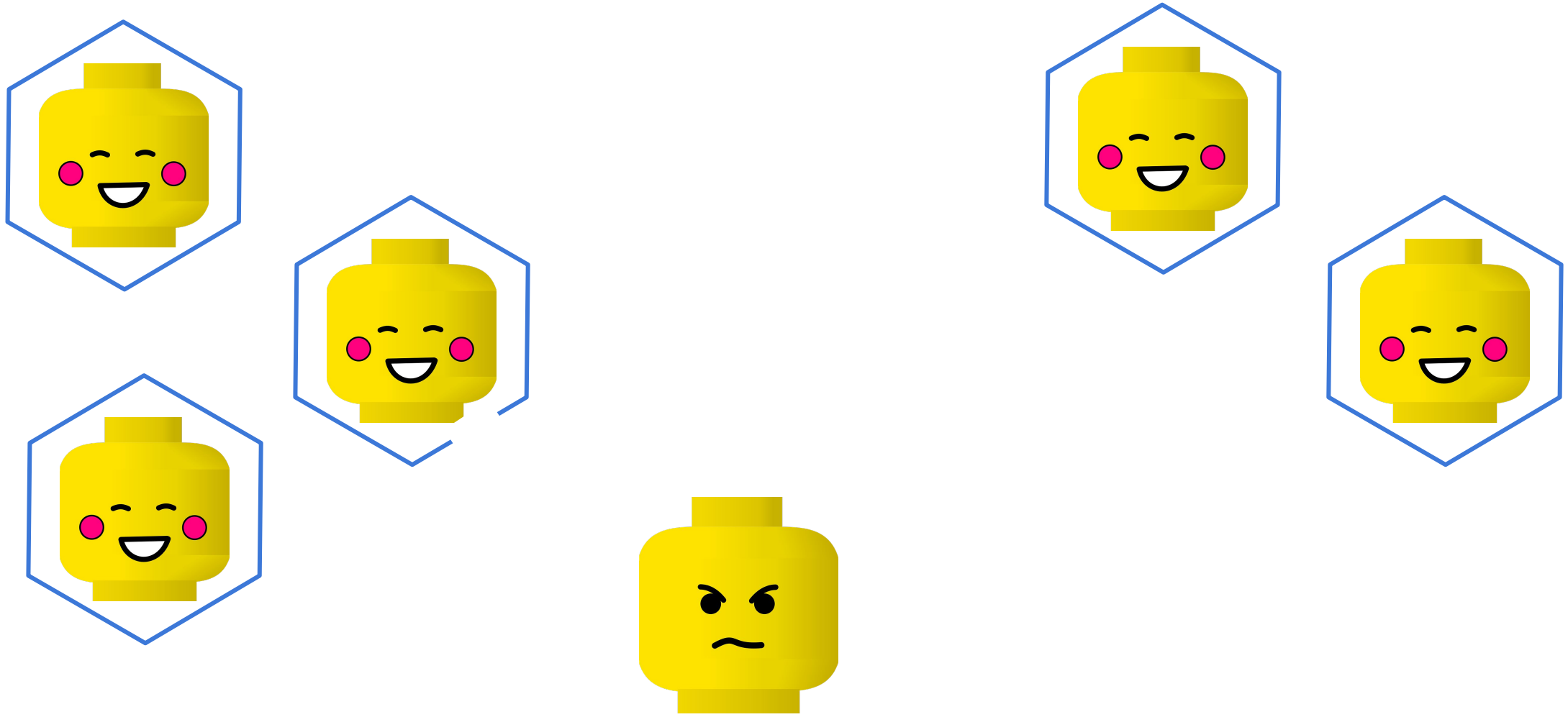

DC-1
DC-2
A
B
D
E
#_

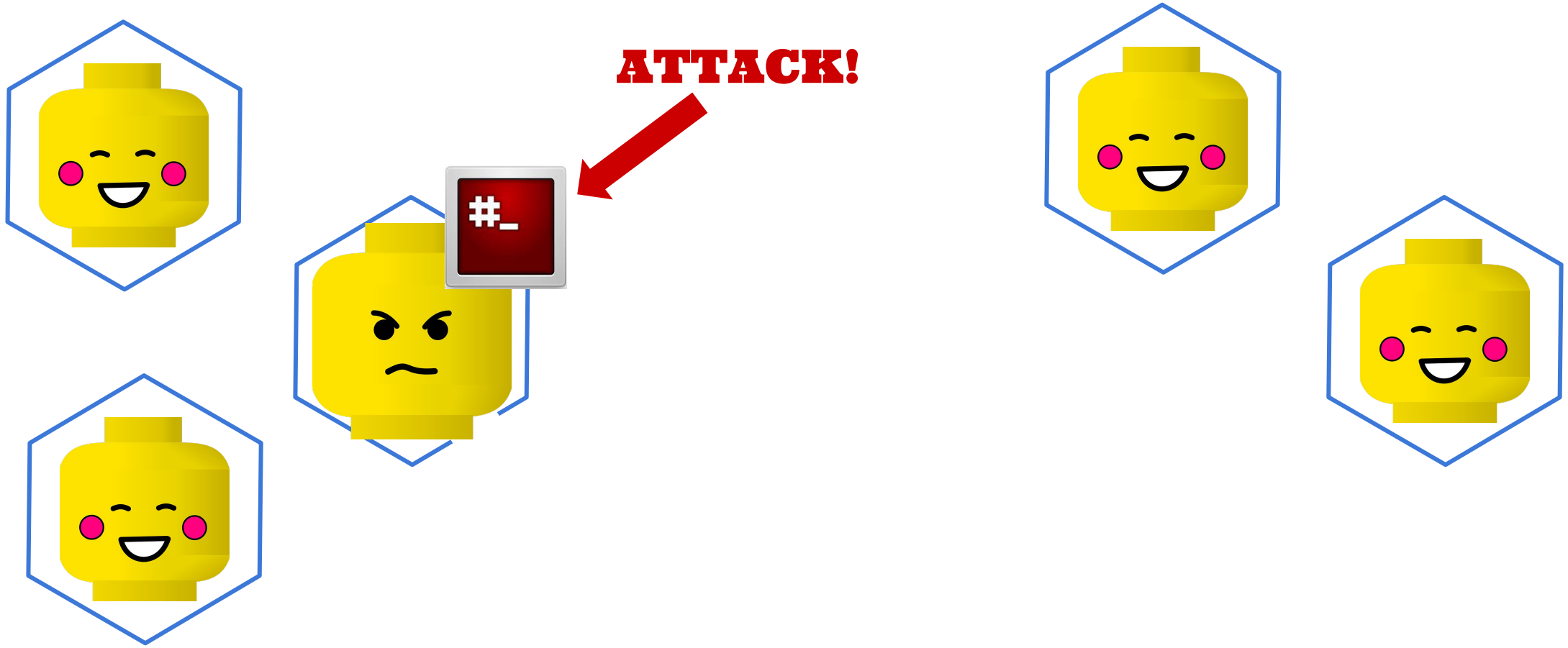


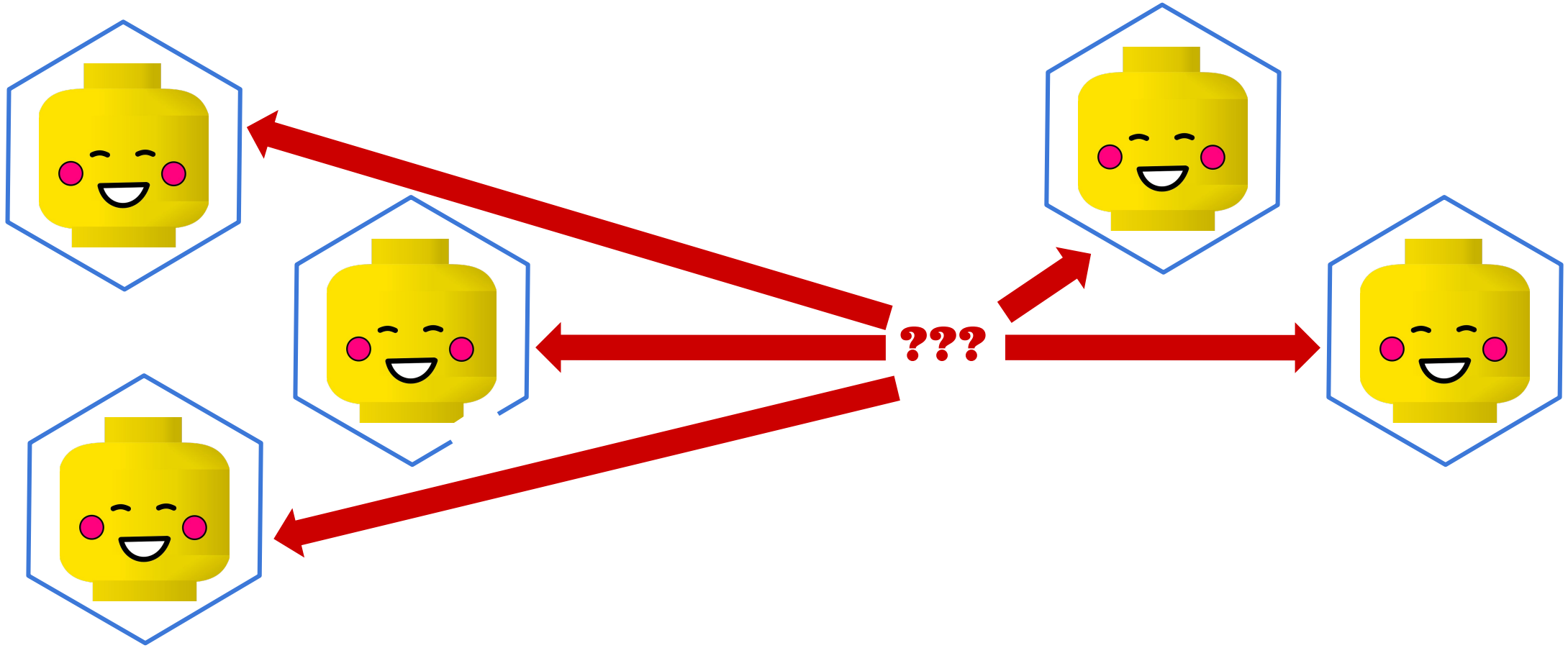
GAME OVER

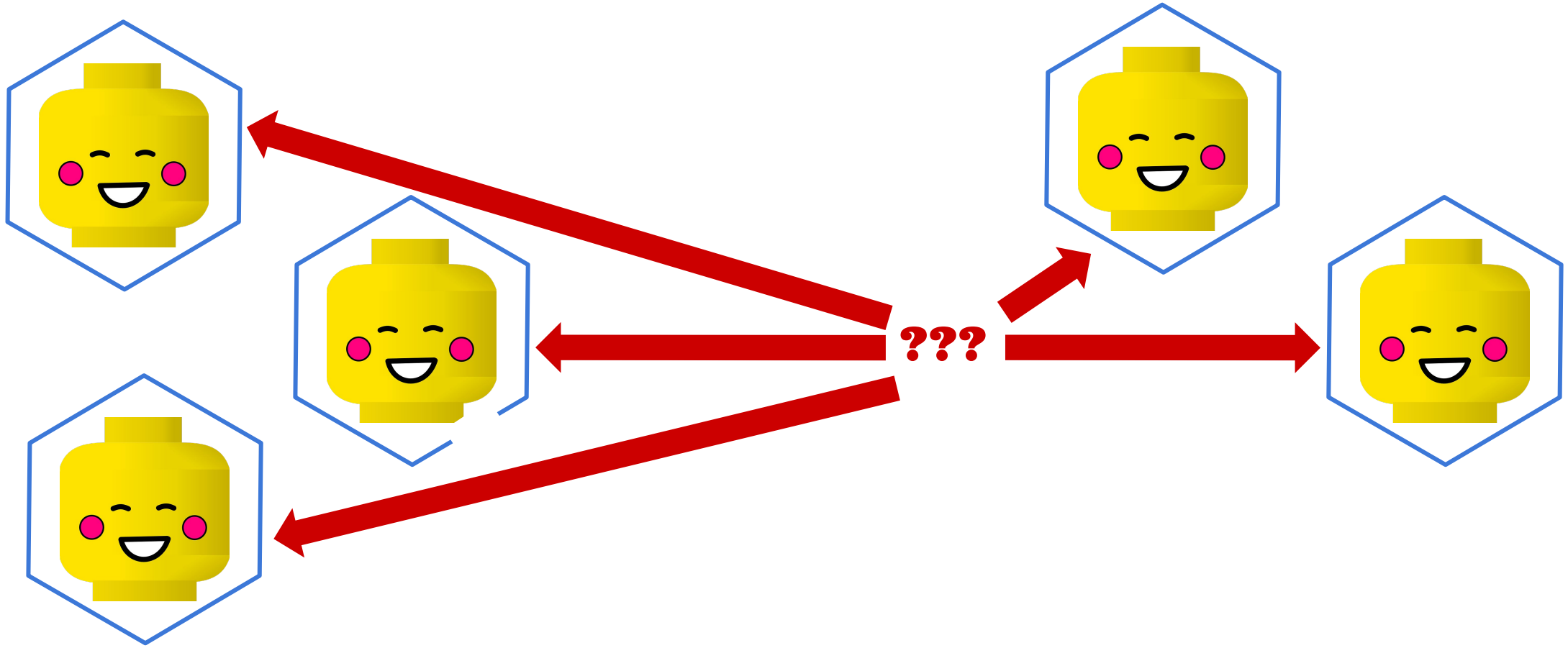

DC-1
DC-2
A
B
C
D
E

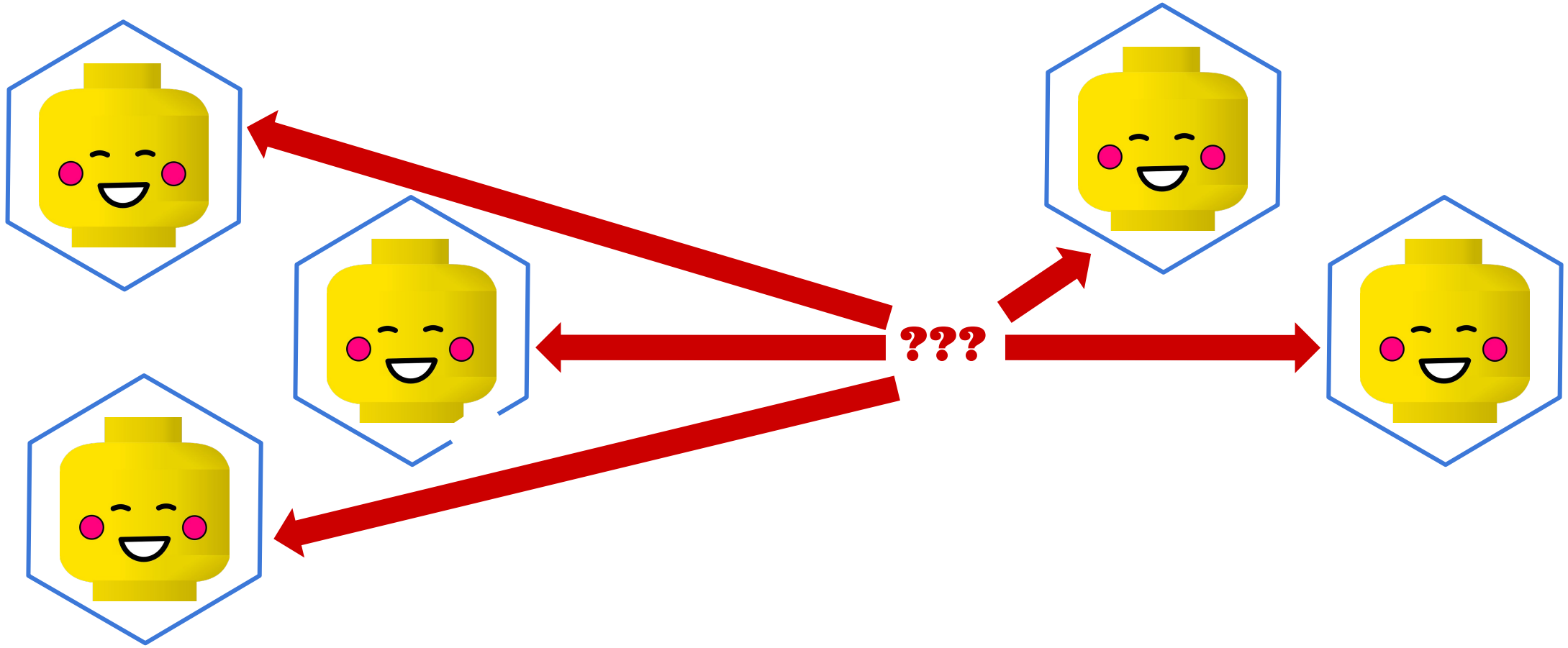

A
B
C
D
E

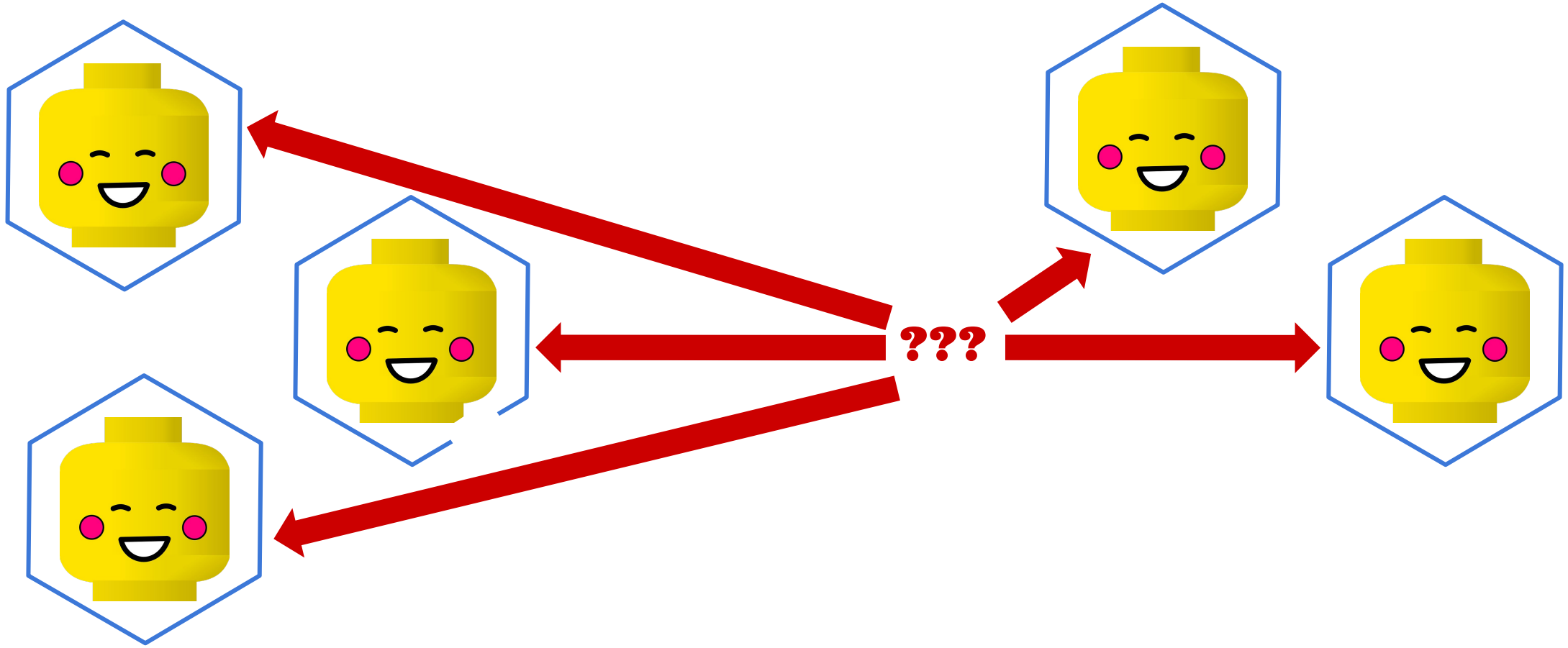


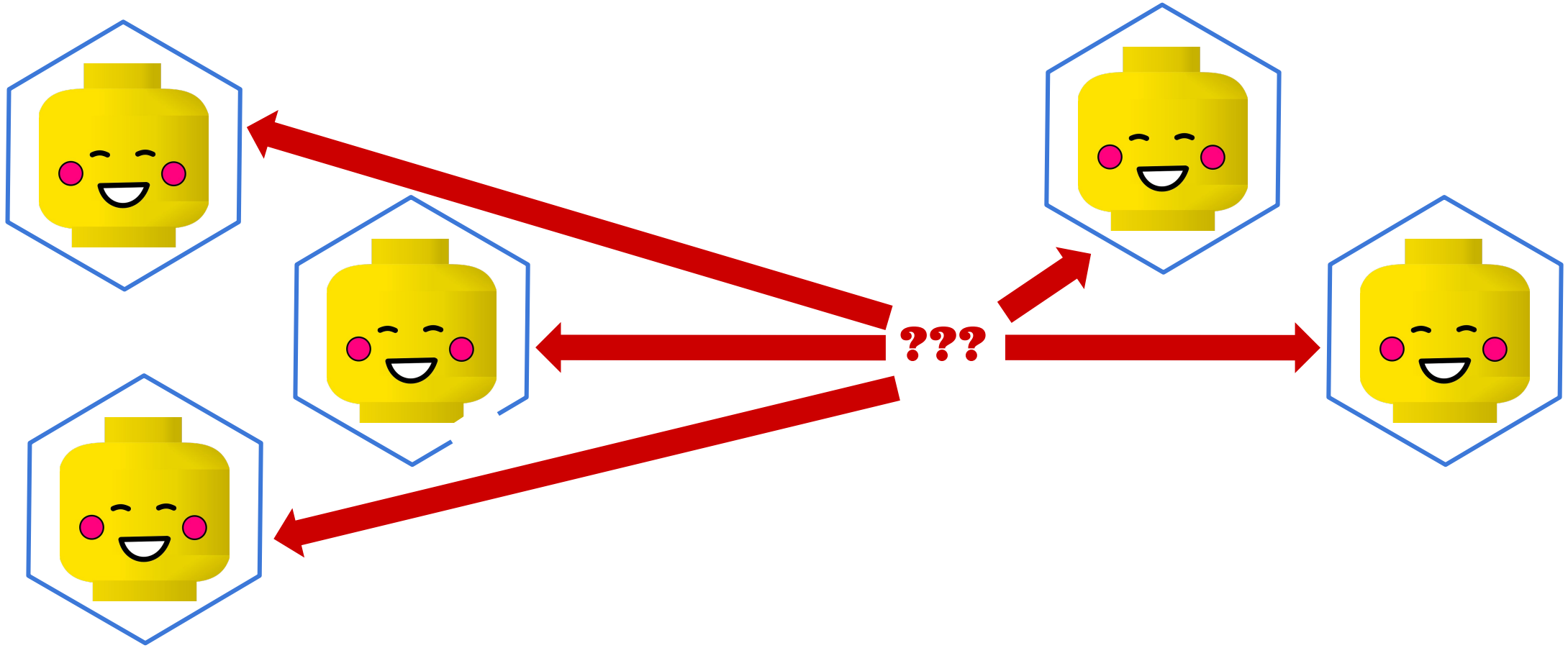

ATTACK!
#_





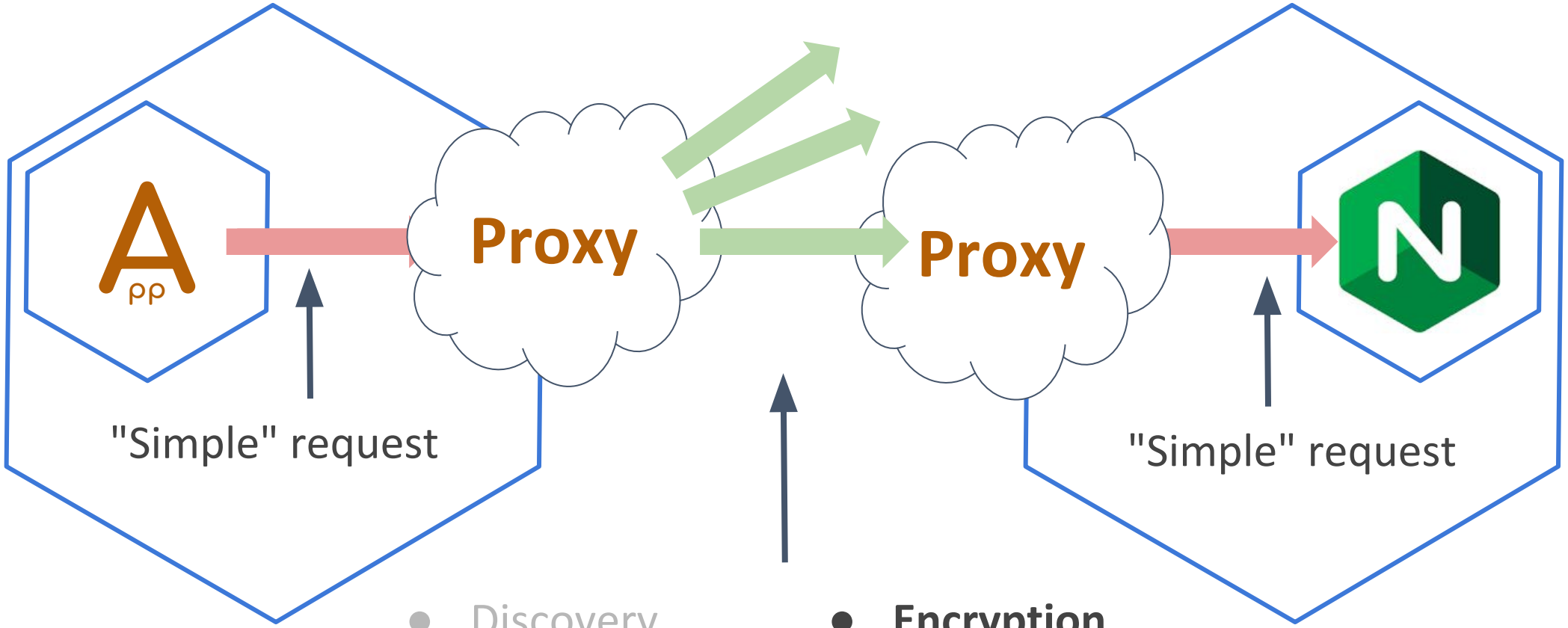






Service mesh

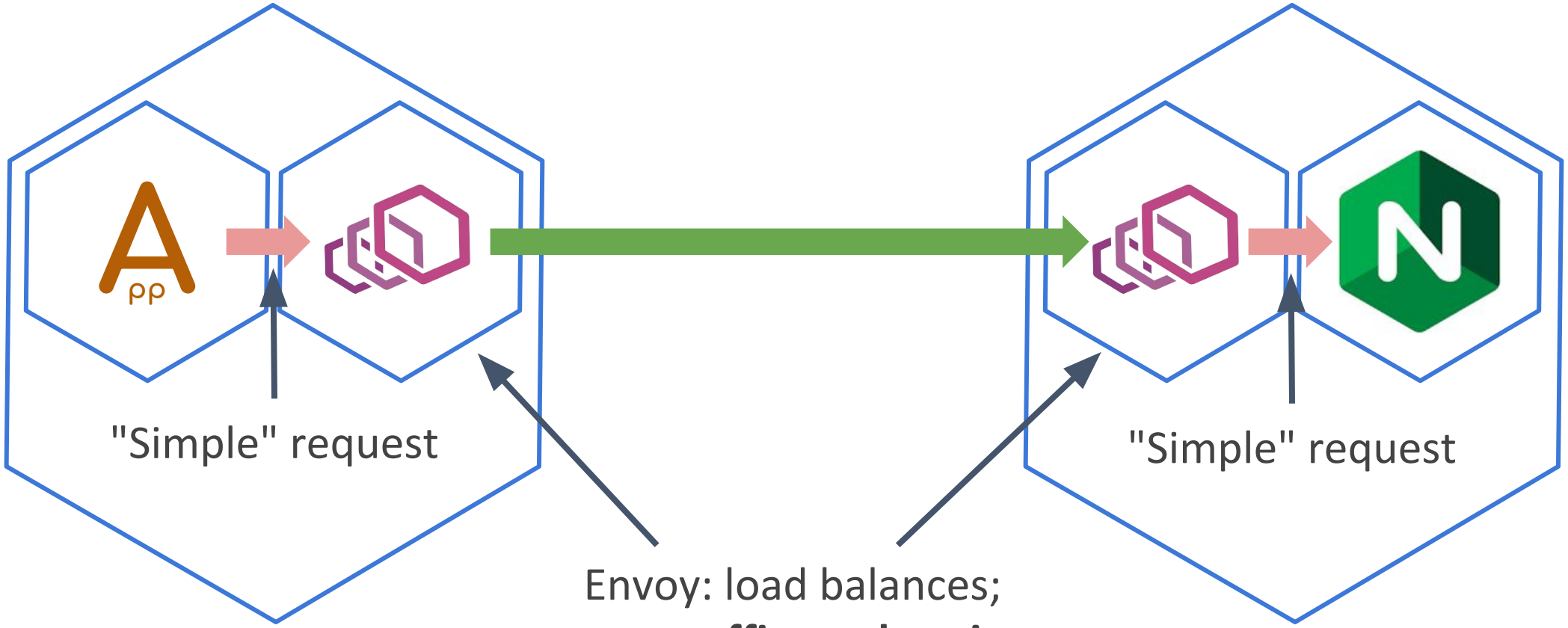
Service mesh



- Discovery
- Load balancing
- Observability

- **Encryption**
- **Authentication**
- **Authorization**

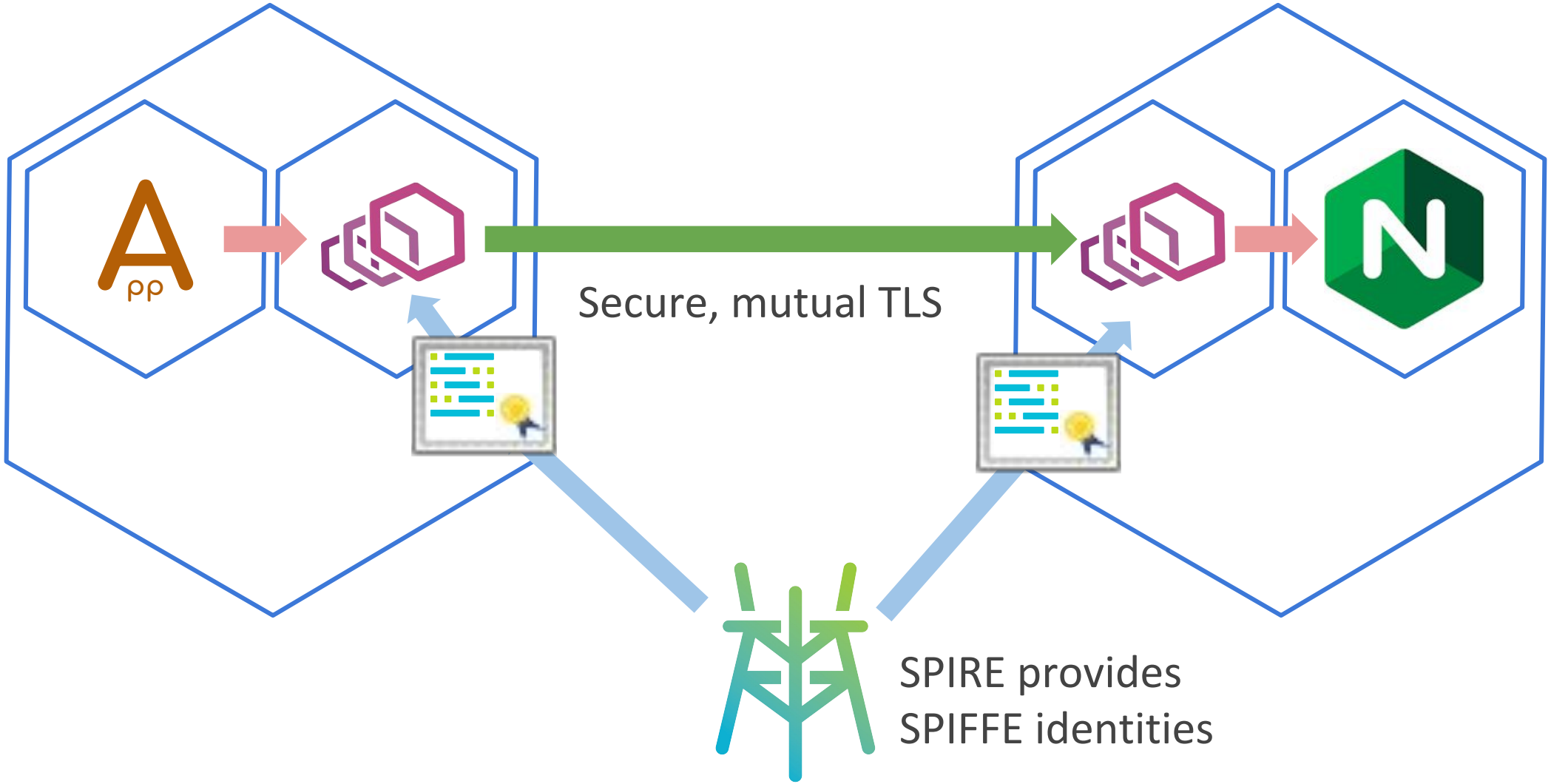
Service proxy: Envoy



Envoy: load balances;
encrypts traffic; **authenticates**;
enforces policy decisions
(and lots more…)

But, it needs help...

Intro to SPIFFE and SPIRE



More about SPIFFE and SPIRE

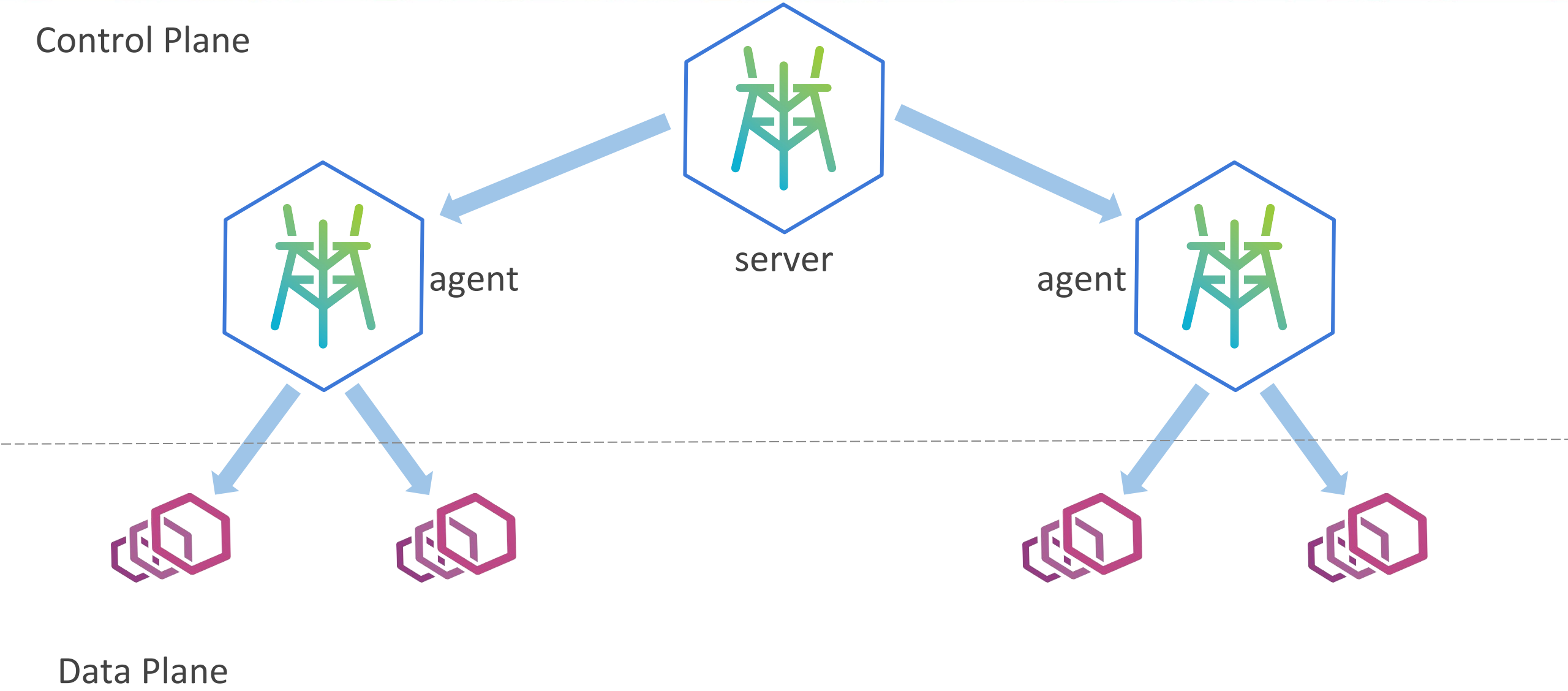
More about SPIFFE and SPIRE


Euroopan unioni
Europeiska unionen
SUOMI : FINLAND
Passi : Pass

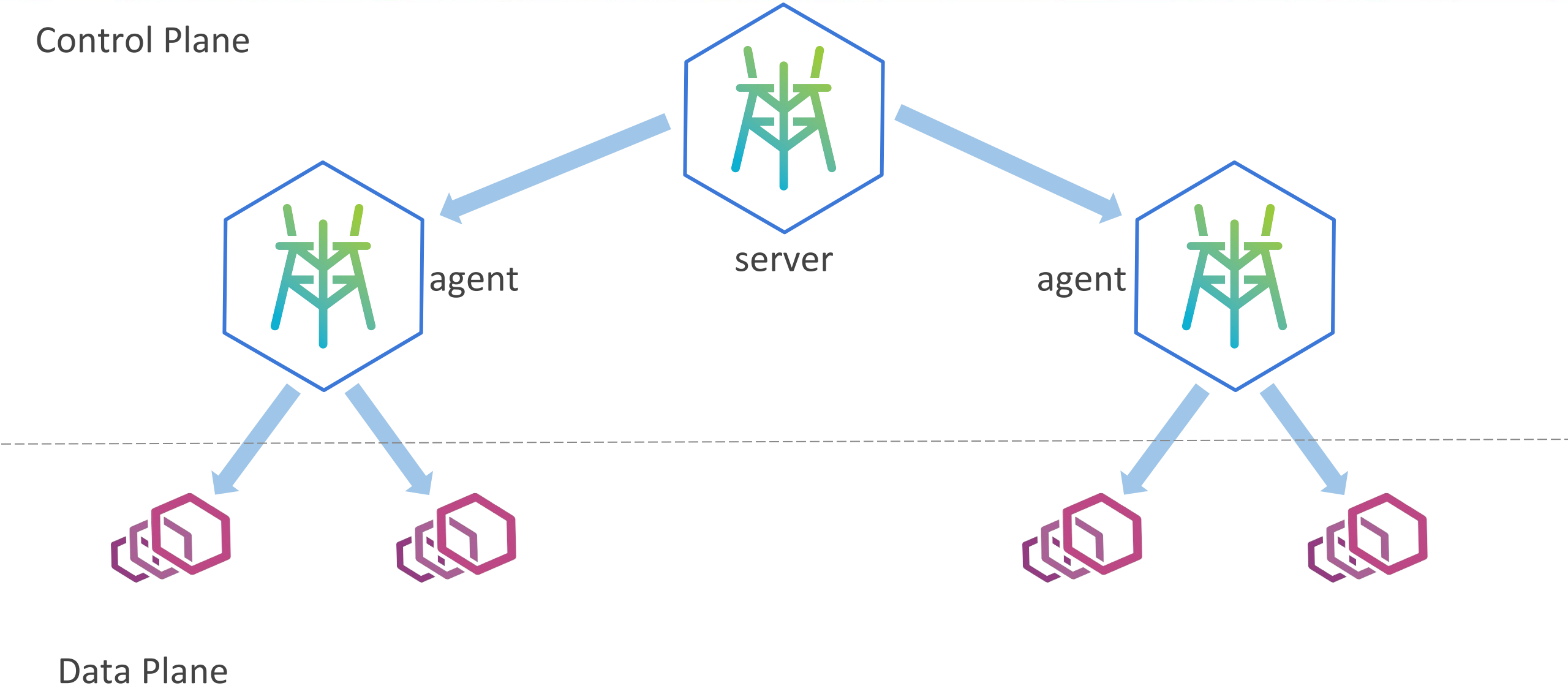

Euroopan unioni
Europeiska unionen
SUOMI : FINLAND
Passi : Pass


Euroopan unioni
Europeiska unionen
SUOMI : FINLAND
Passi : Pass

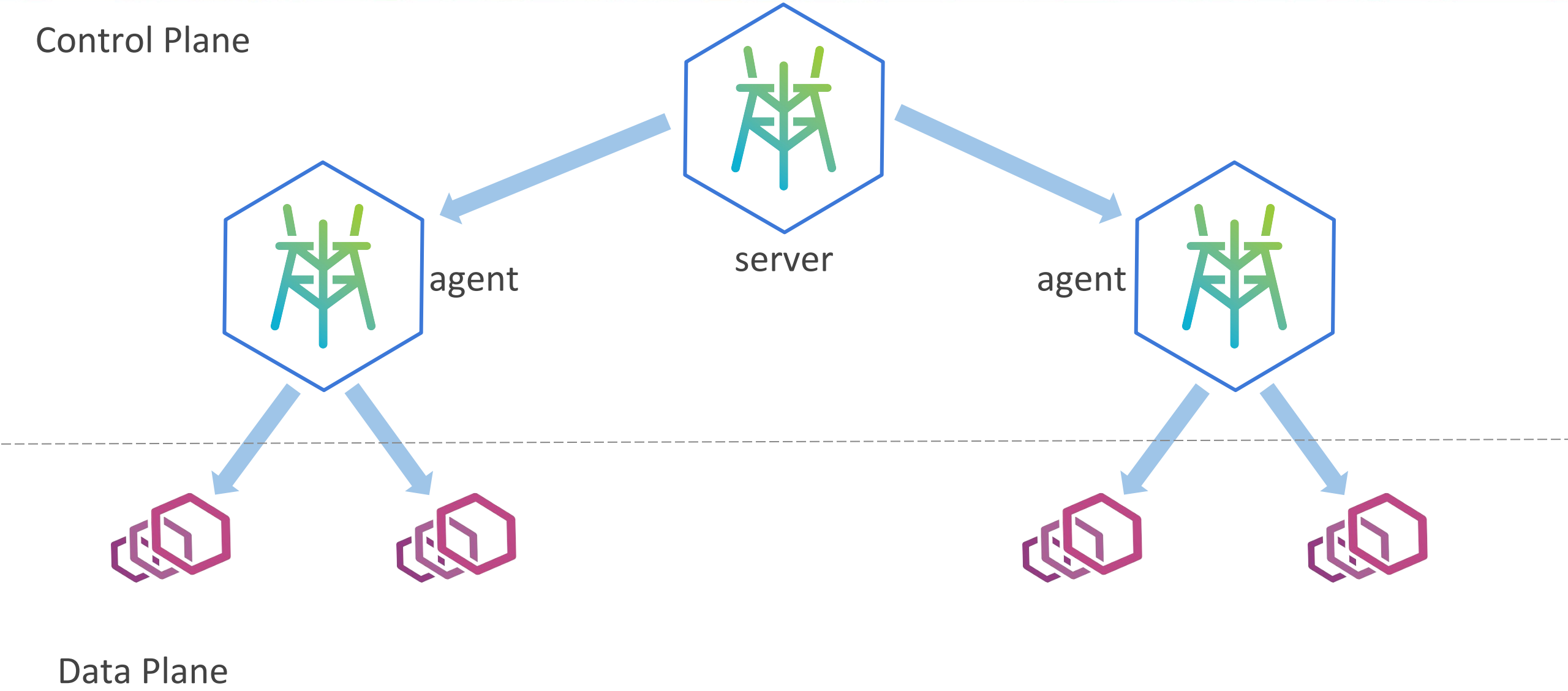
SPIRE Architecture



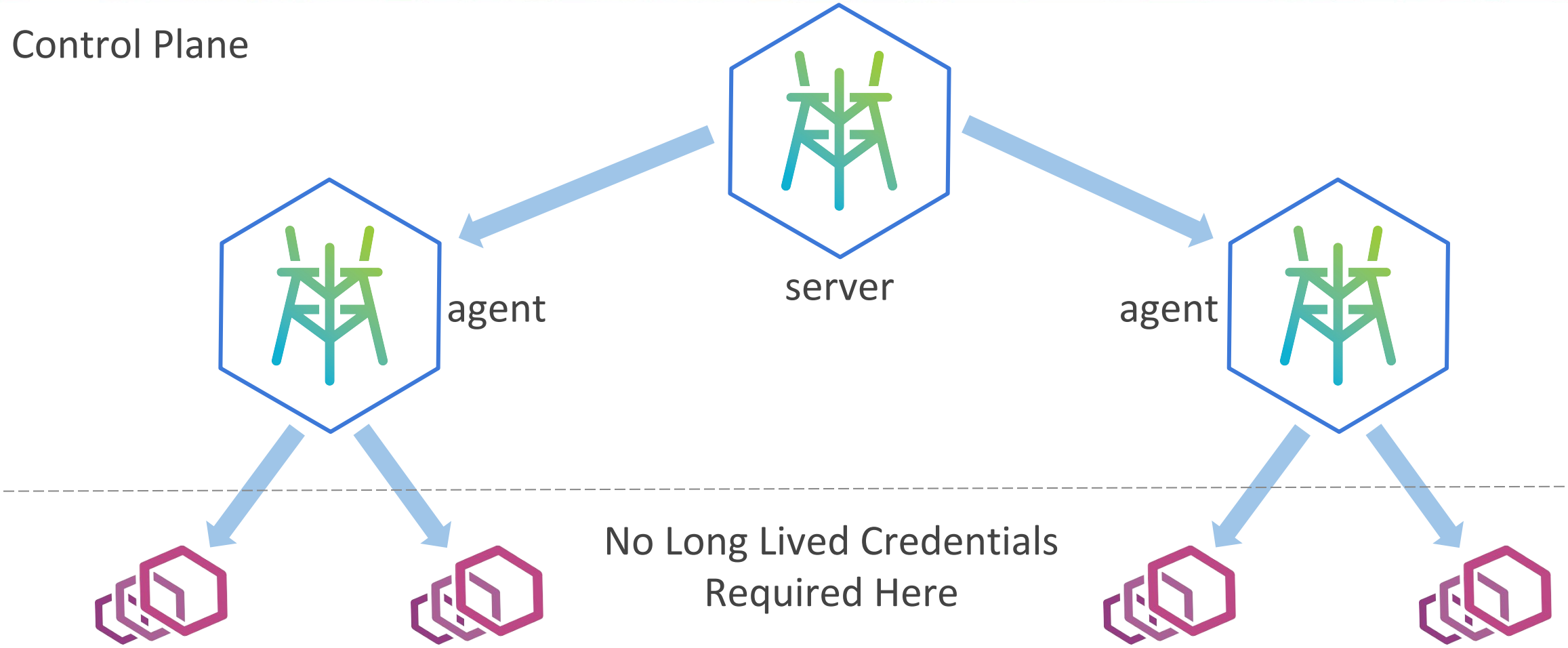
SPIRE Architecture



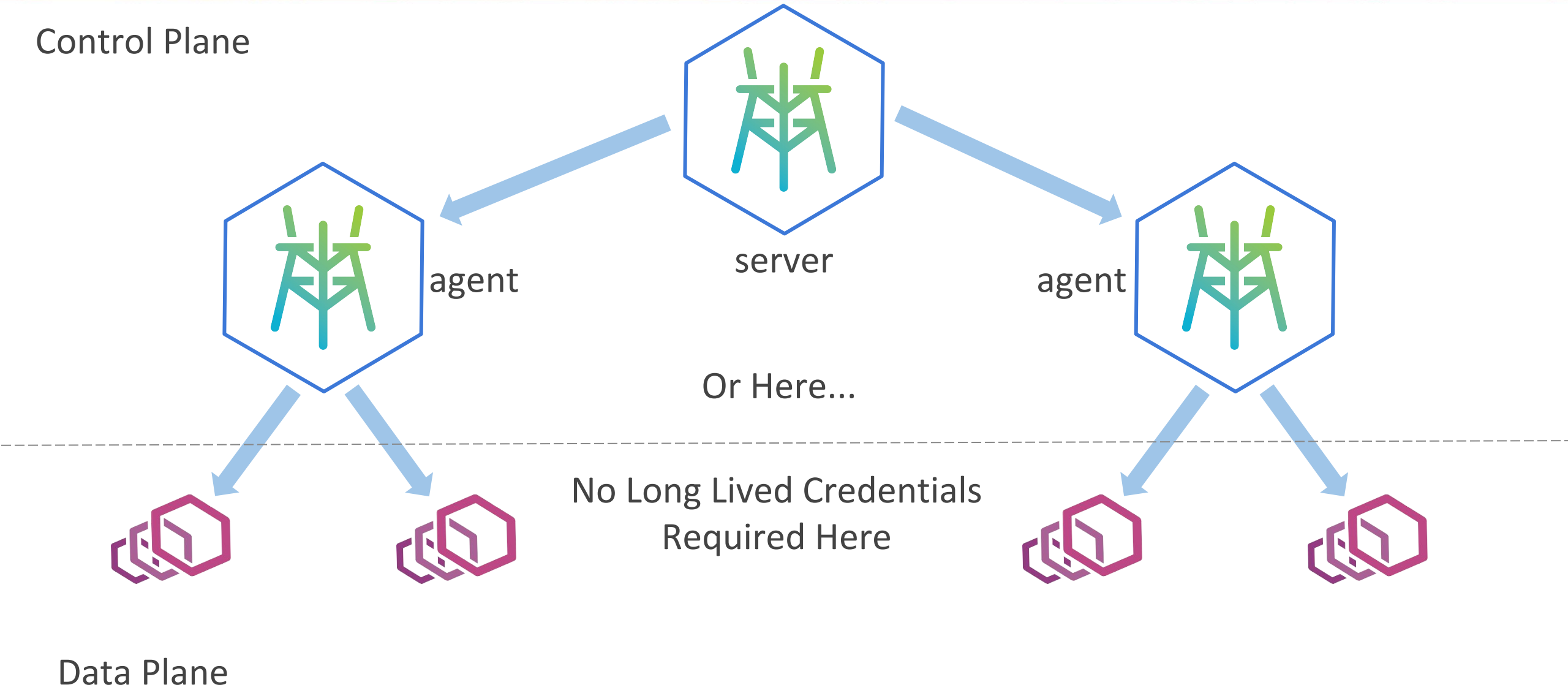
SPIRE Architecture



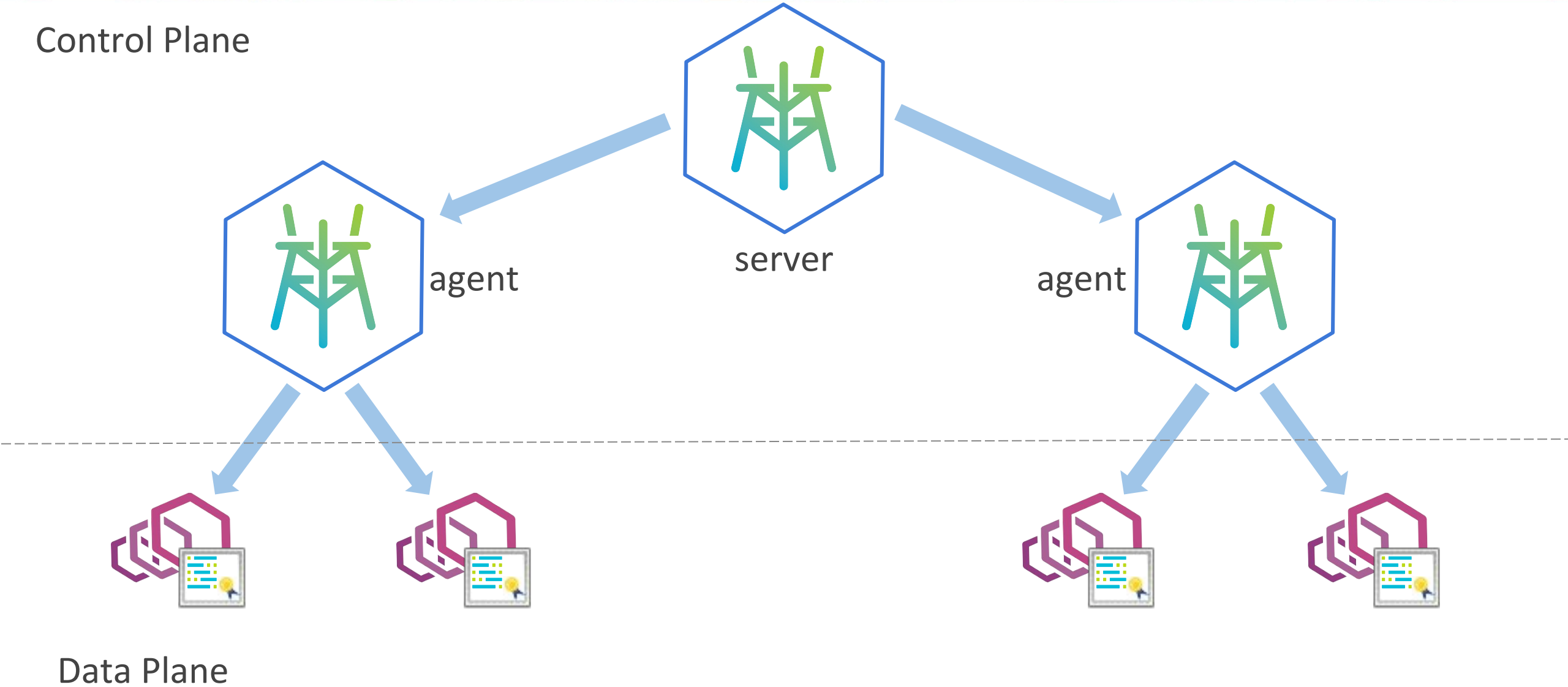
SPIRE Architecture



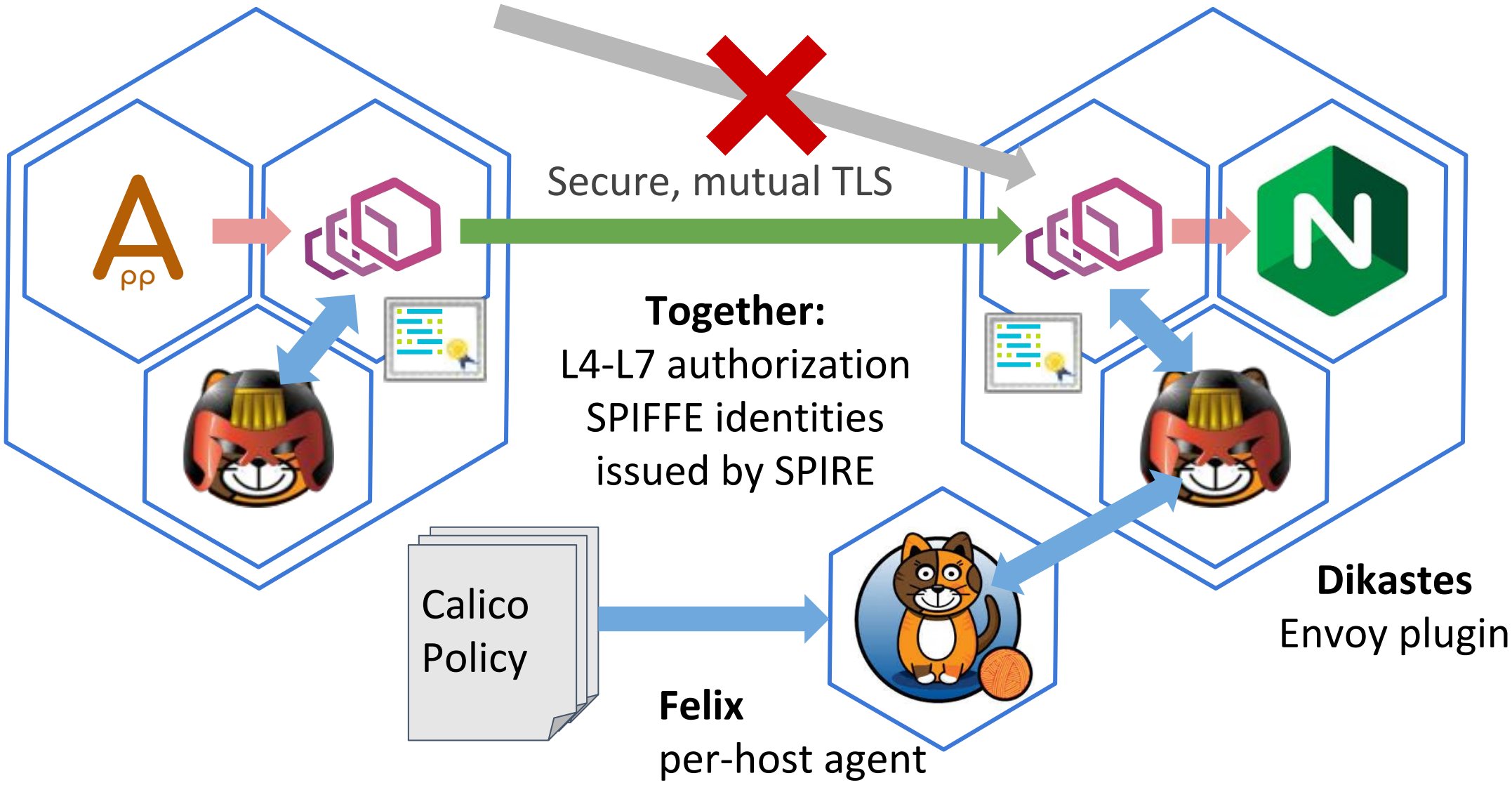
SPIRE Architecture



SPIRE Architecture



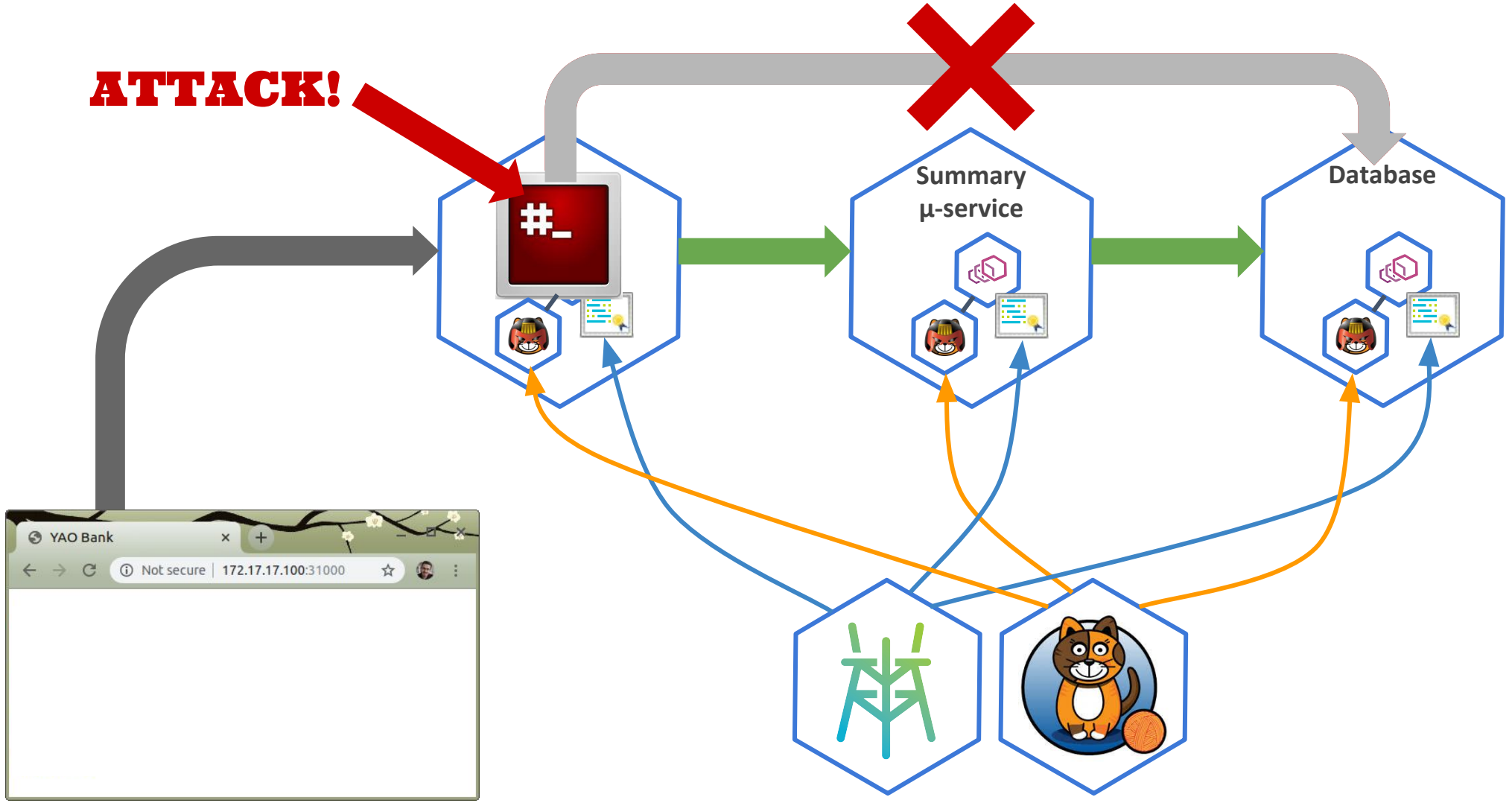
Authorization with Calico



DEMO

- Let's rob a bank...

DEMO


ATTACK!
#_
Summary
µ-service
Database
YAO Bank
Not secure
172.17.17.100:31000

DEMO TIME

Wrap up

- **SPIRE:** https://github.com/spiffe/spire
- **Calico:** https://github.com/projectcalico/calico/
- **Demo YAMLs:** https://github.com/projectcalico/spire-demo