An Interoperable Zero Trust Federated Architecture for Tactical Systems

Alexandre Poirrier (DGA & Ecole polytechnique)
Laurent Cailleux (DGA-MI)
Thomas Heide Clausen (Ecole polytechnique)

A Need for Interoperability

Federated Mission Networking

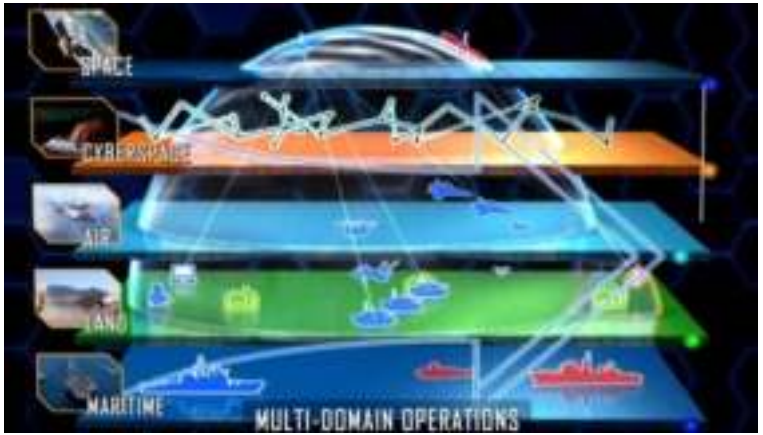
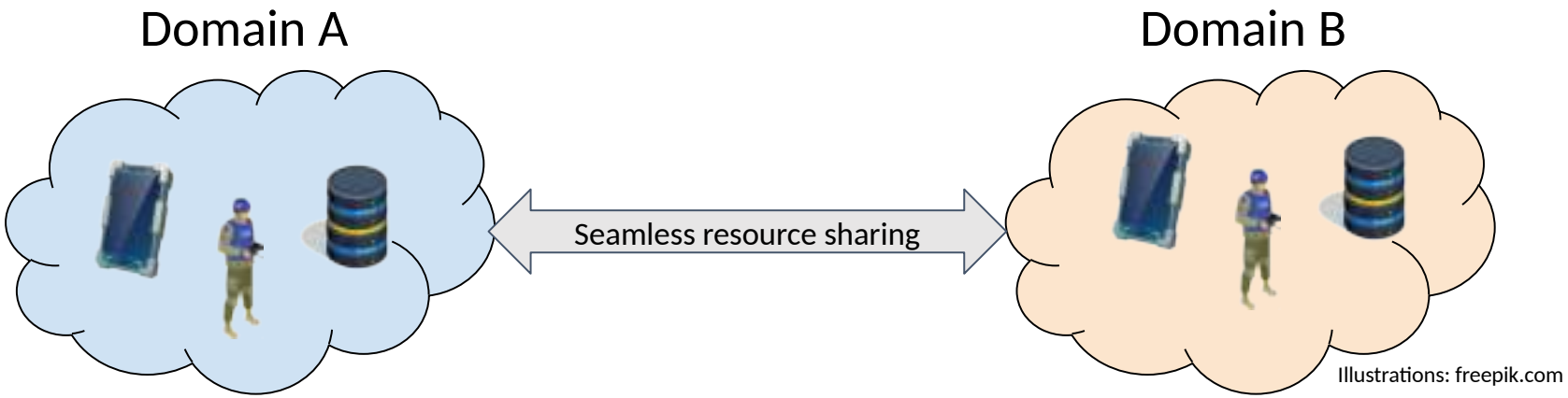


Illustration: acquisitiontalk.com

"Interoperability is the ability to act together coherently, effectively and efficiently to achieve Allied objectives"

A Need for Interoperability



Illustrations: freepik.com

A Need for Security

A Need for Security

Zero Trust

A Need for Security

Do

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

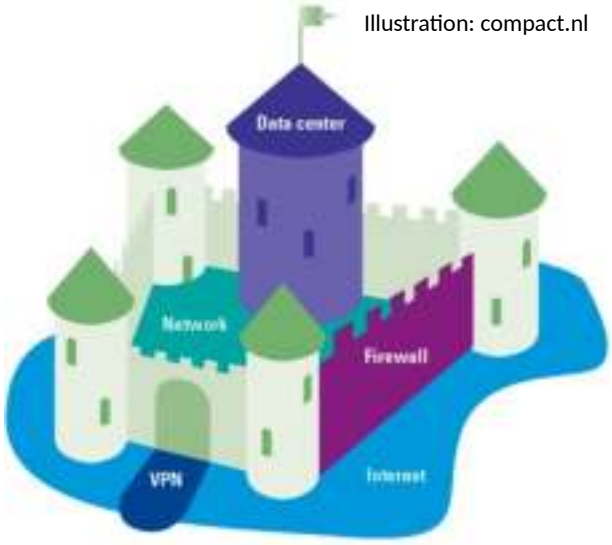
This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

ain B

Illustrations: freepik.com

Going Beyond Perimeter Security

Illustration: compact.nl



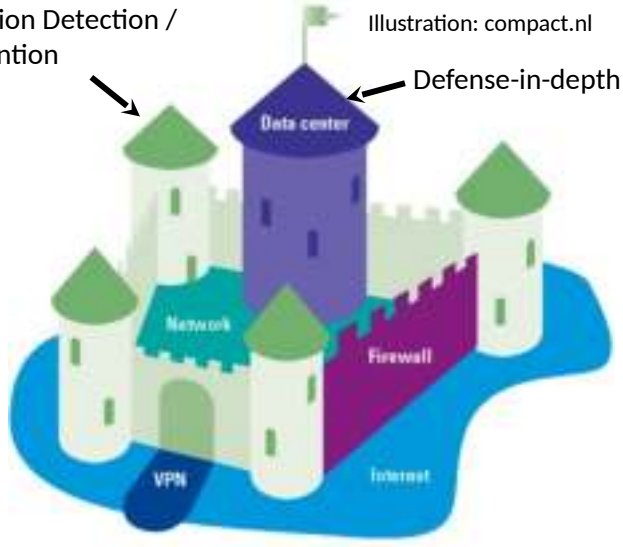
Traditional Perimeter Security

Going Beyond Perimeter Security

Intrusion Detection / Prevention

Illustration: compact.nl

Defense-in-depth



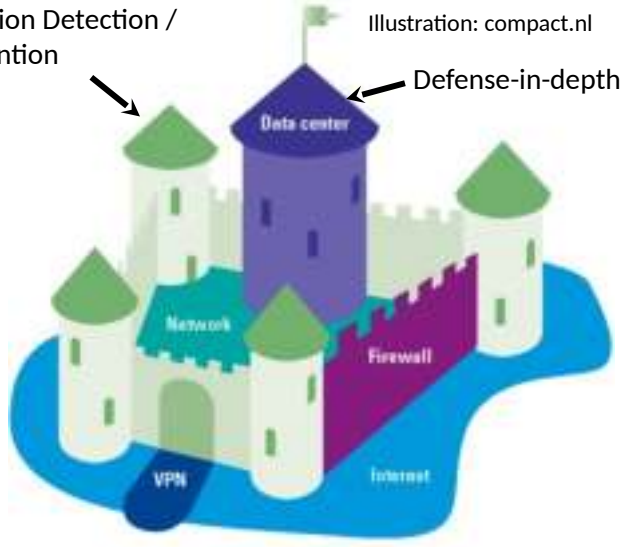
Traditional Perimeter Security

Going Beyond Perimeter Security

Intrusion Detection / Prevention

Illustration: compact.nl

Defense-in-depth



Traditional Perimeter Security

Perimeter Security Flaws

Insider Threats

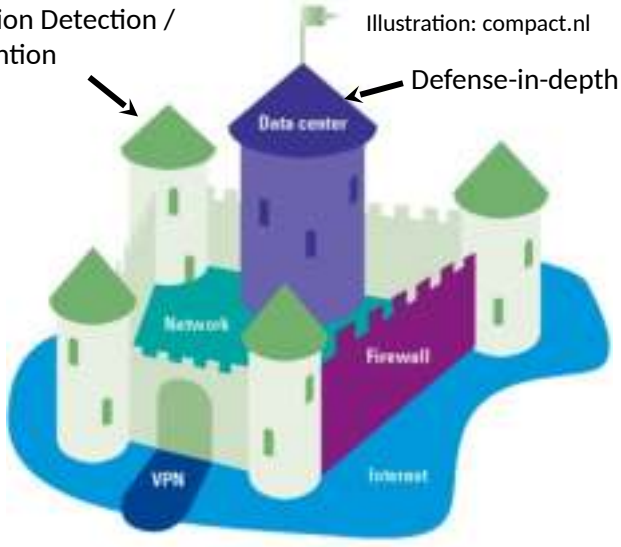
Source: Verizon

Going Beyond Perimeter Security

Intrusion Detection / Prevention

Illustration: compact.nl

Defense-in-depth



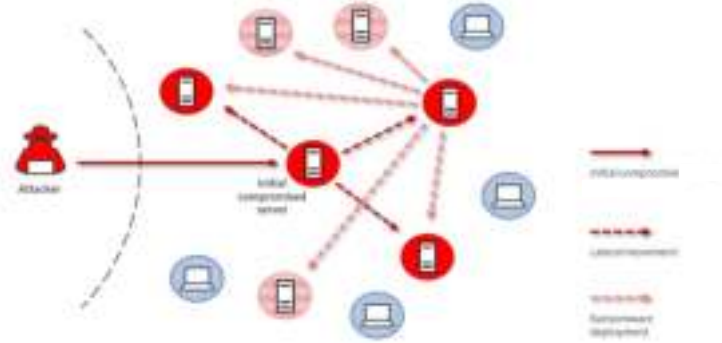
Traditional Perimeter Security

Perimeter Security Flaws

Insider Threats

Source: Verizon

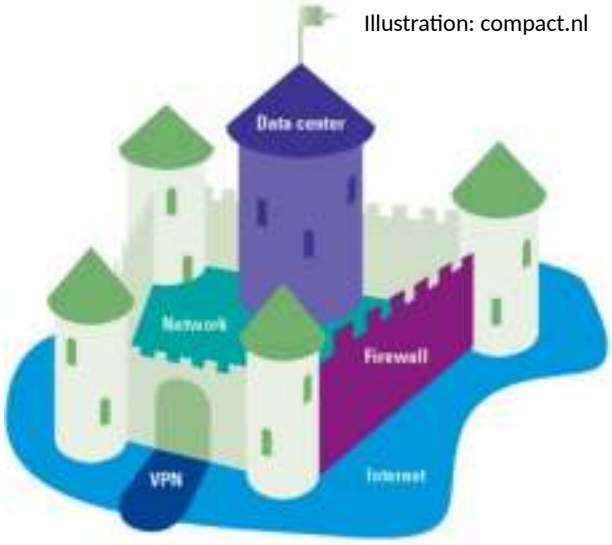
Lateral Movement



Source: Microsoft

A (short) Dive into Zero Trust

Illustration: compact.nl



Traditional Perimeter Security

Zero Trust

“Never trust, always verify”

A (short) Dive into Zero Trust

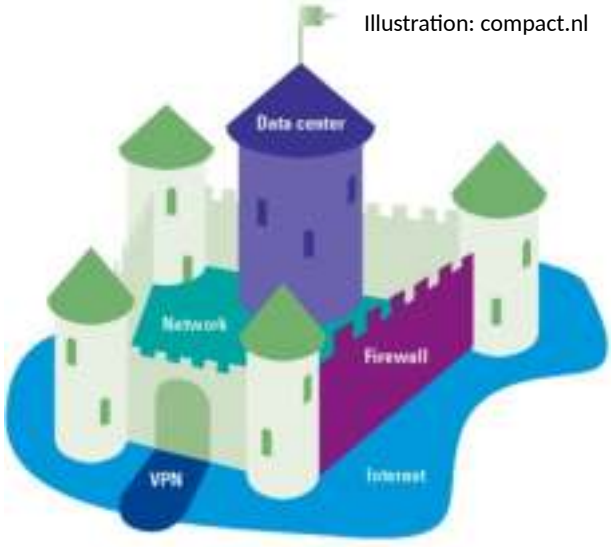


Illustration: compact.nl

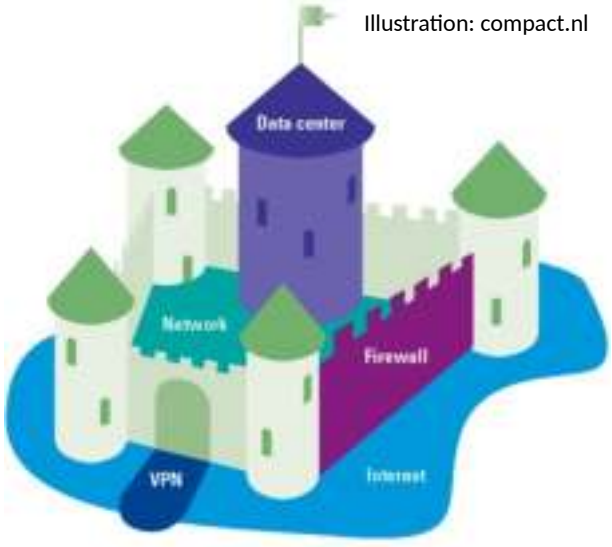
Traditional Perimeter Security

Zero Trust

“Never trust, always verify”

NIST Special Publication 800-207 “Zero Trust Architecture”

A (short) Dive into Zero Trust



Traditional Perimeter Security

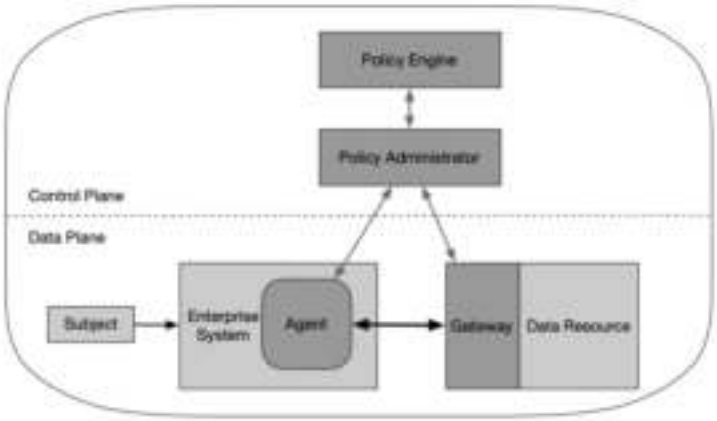
Zero Trust

"Never trust, always verify"

NIST Special Publication 800-207 "Zero Trust Architecture"

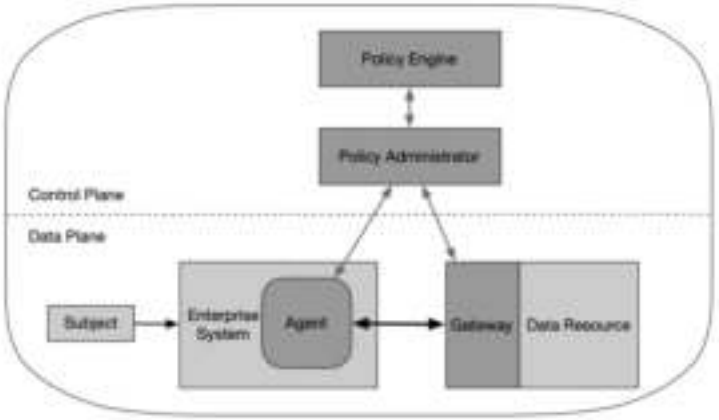
Cybersecurity & Infrastructure Security Agency

Software-Defined Perimeters

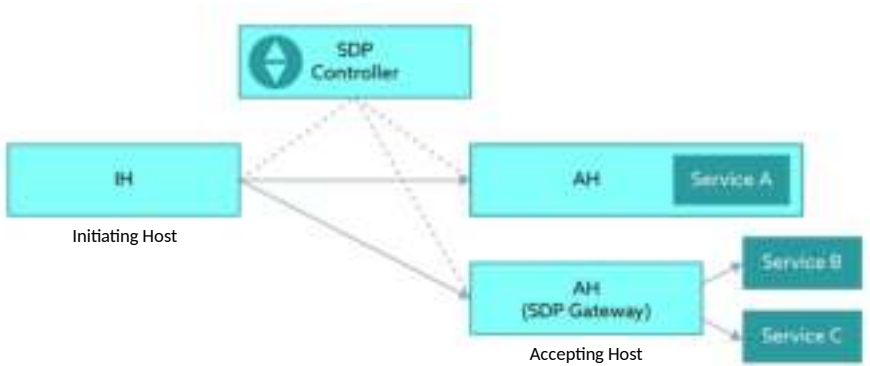


NIST SP 800-207: Device Agent/Gateway Model

Software-Defined Perimeters

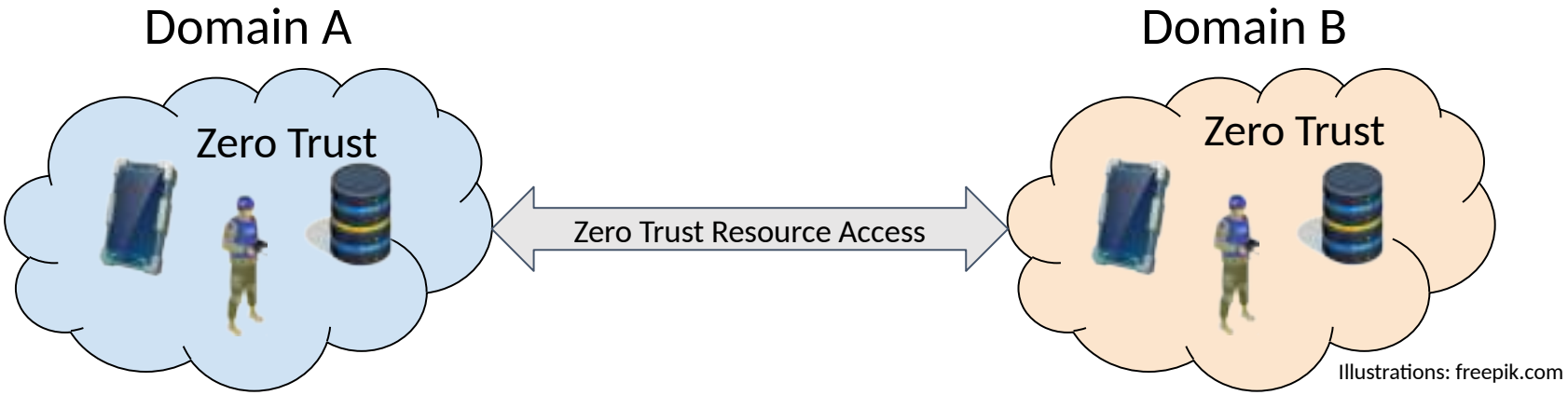


NIST SP 800-207: Device Agent/Gateway Model



Cloud Security Alliance - Software-Defined Perimeter (SDP) Specification v2.0

Problem Statement

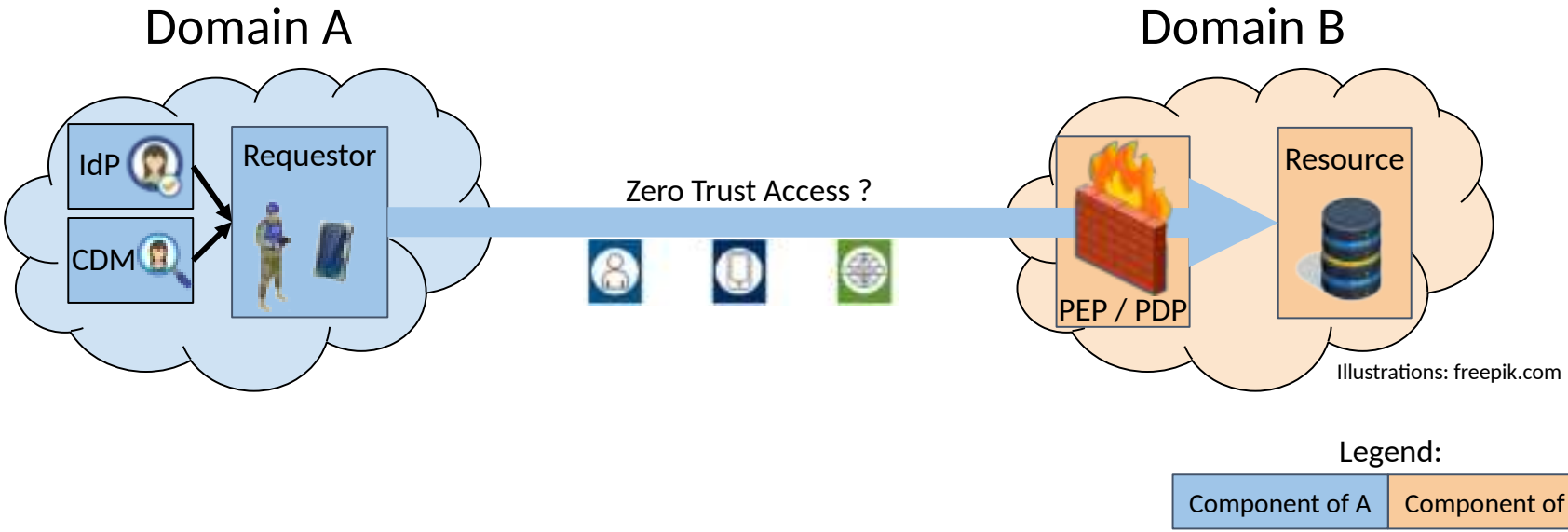


Illustrations: freepik.com

Problem Statement

IdP: Identity Provider
CDM: Continuous Diagnostics & Mitigation

PEP/PDP: Policy Enforcement / Decision Point



Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

Three different possibilities:

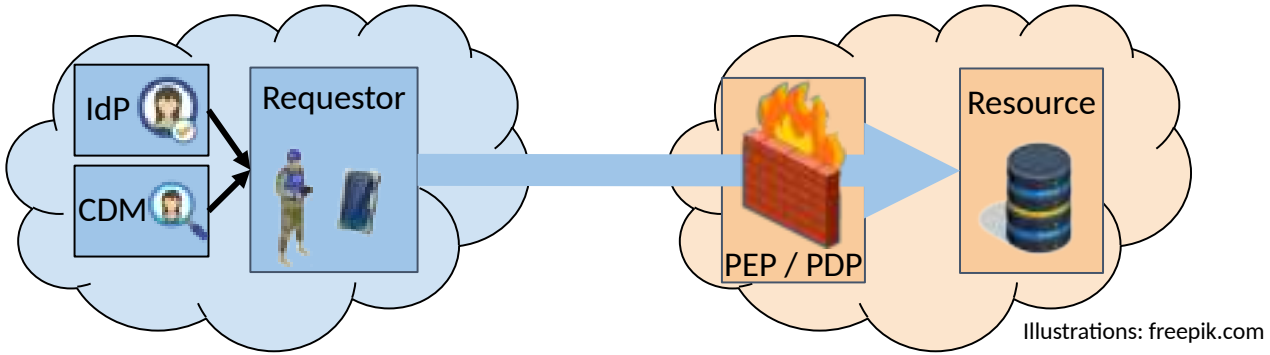
1) Implicit Trust
2) Device Agent
3) Trusted Third-Party / Hierarchy

Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

Three different possibilities:

1) **Implicit Trust**
2) Device Agent
3) Trusted Third-Party / Hierarchy



Implicit Trust solution

Legend:

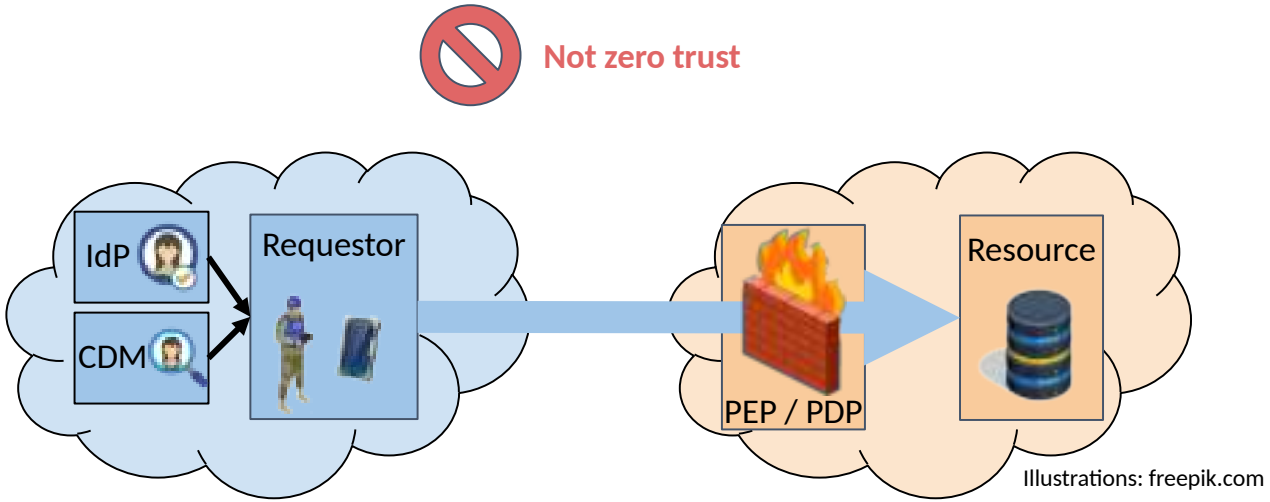
Component of A	Component of B

Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

Three different possibilities:

1) **Implicit Trust**
2) Device Agent
3) Trusted Third-Party / Hierarchy



Implicit Trust solution

Legend:

Component of A	Component of B

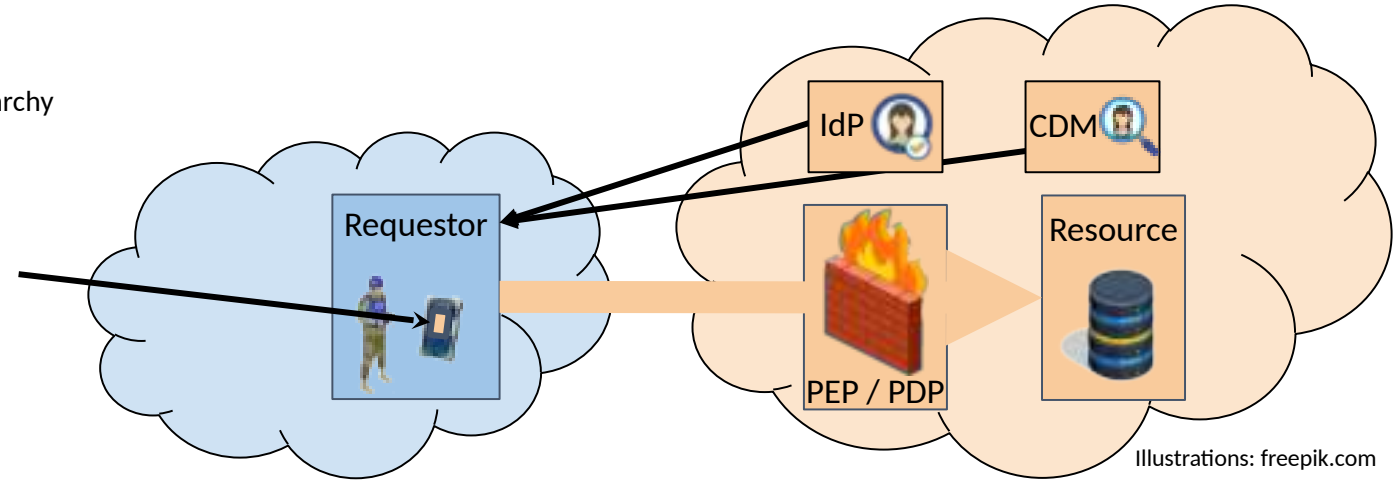
Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

Three different possibilities:

1) Implicit Trust
2) **Device Agent**
3) Trusted Third-Party / Hierarchy

A device agent is installed **on every device** of domain A.



Device Agent solution

Legend:

Component of A	Component of B

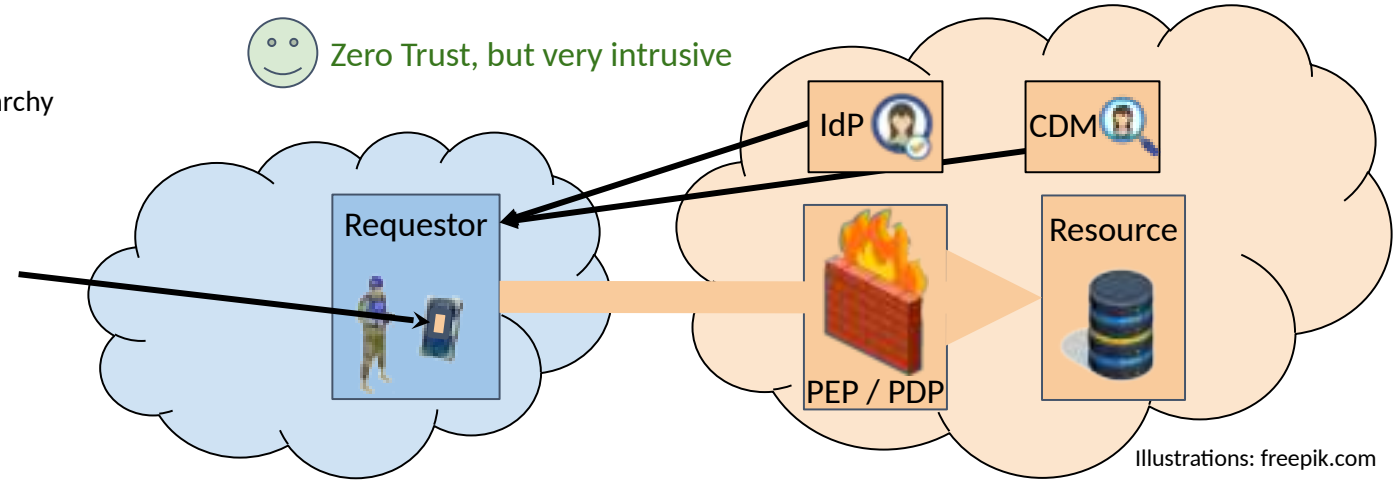
Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

Three different possibilities:

1) Implicit Trust
2) **Device Agent**
3) Trusted Third-Party / Hierarchy

A device agent is installed **on every device** of domain A.



Device Agent solution

Legend:

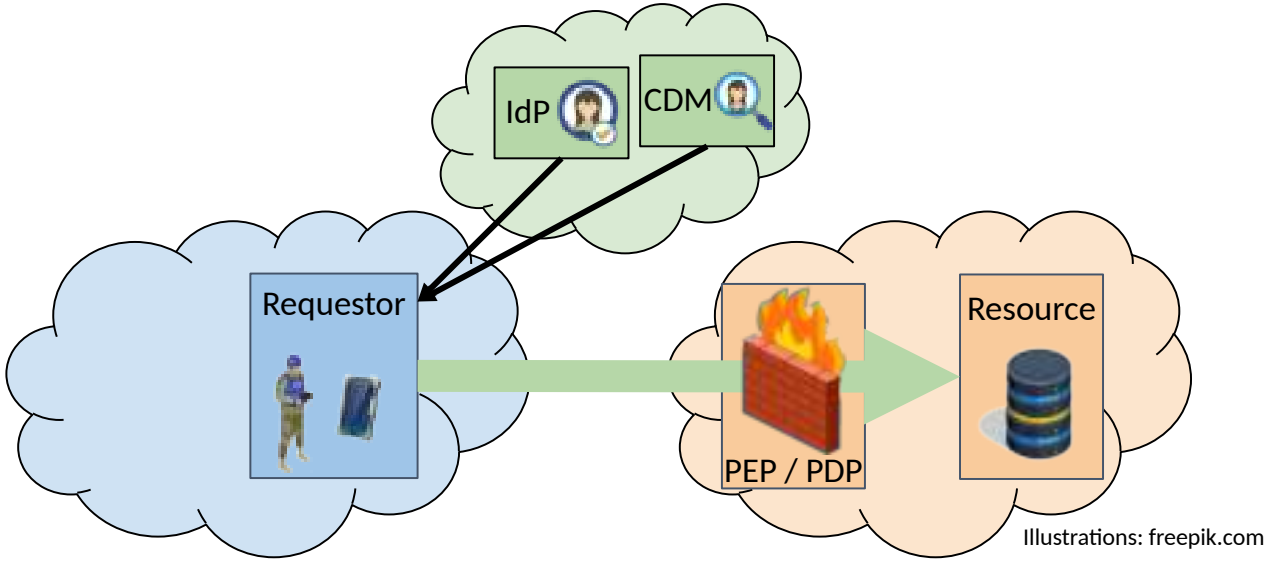
Component of A	Component of B

Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

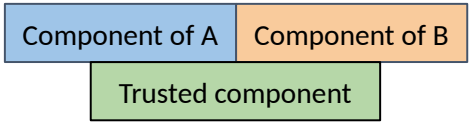
Three different possibilities:

1) Implicit Trust
2) Device Agent
3) **Trusted Third-Party / Hierarchy**



Trusted Third-Party solution

Legend:



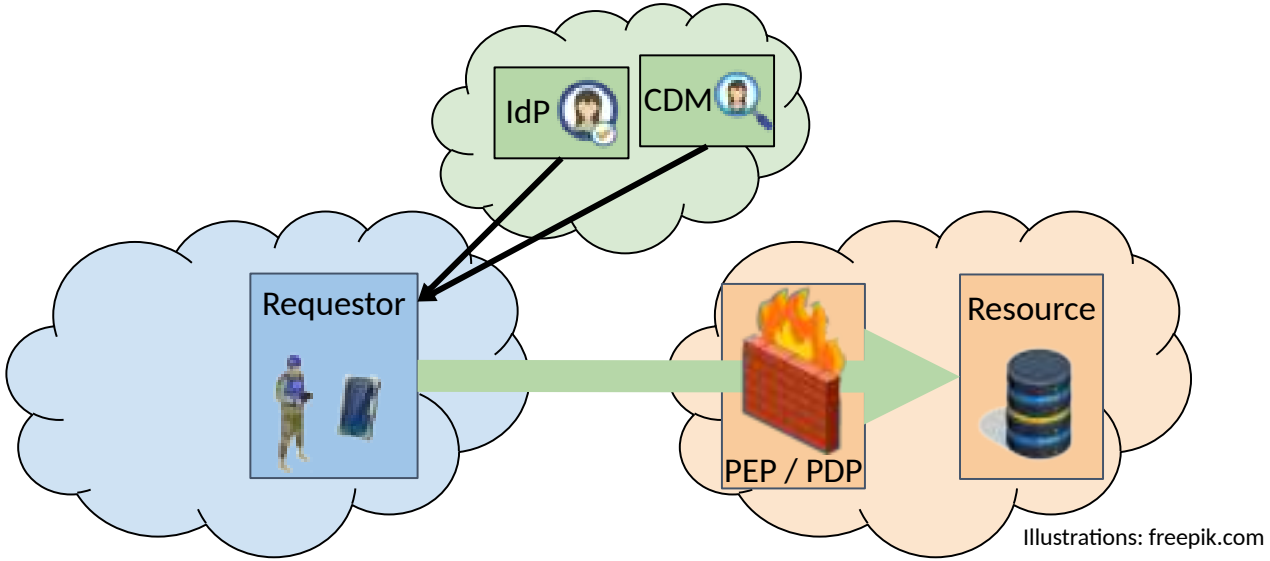
Related Work

K. Olson and E. Keller, “Federating trust,” in Proceedings of the SIGCOMM '21 Poster and Demo Sessions. ACM, aug 2021.

Three different possibilities:

1) Implicit Trust
2) Device Agent
3) **Trusted Third-Party / Hierarchy**

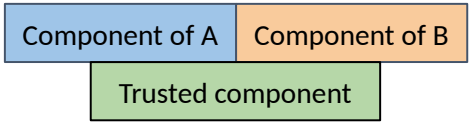
Not zero trust



Illustrations: freepik.com

Trusted Third-Party solution

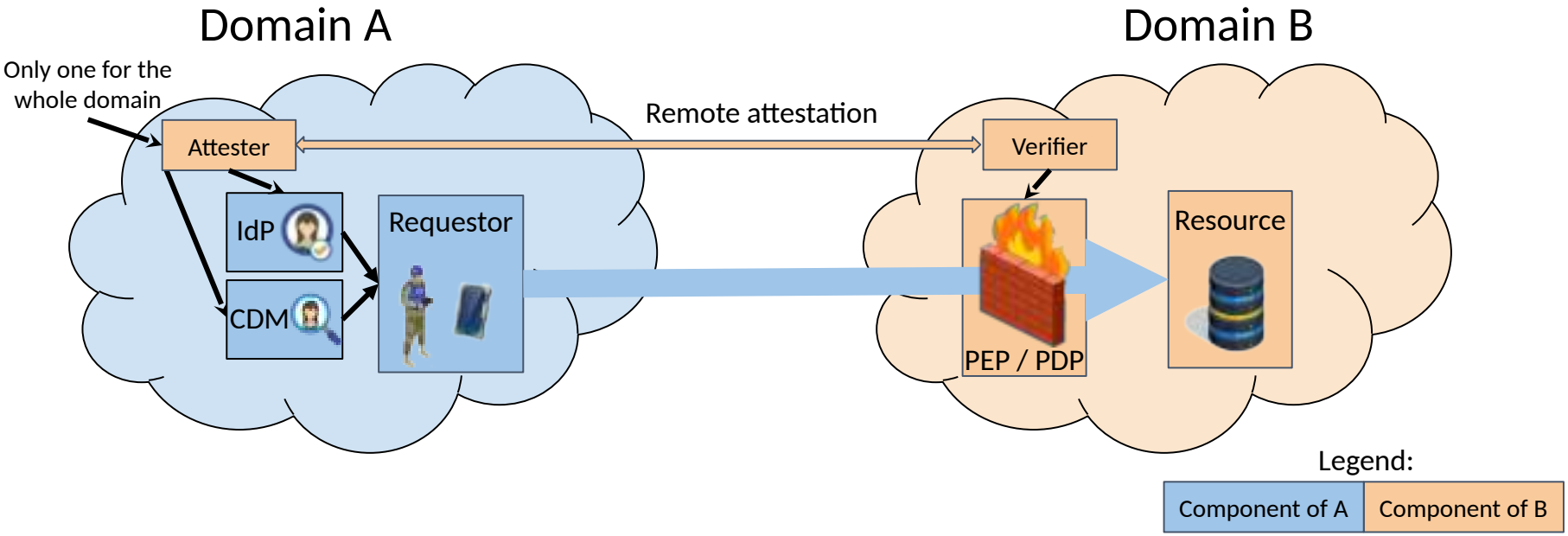
Legend:



Proposed Zero Trust Federation

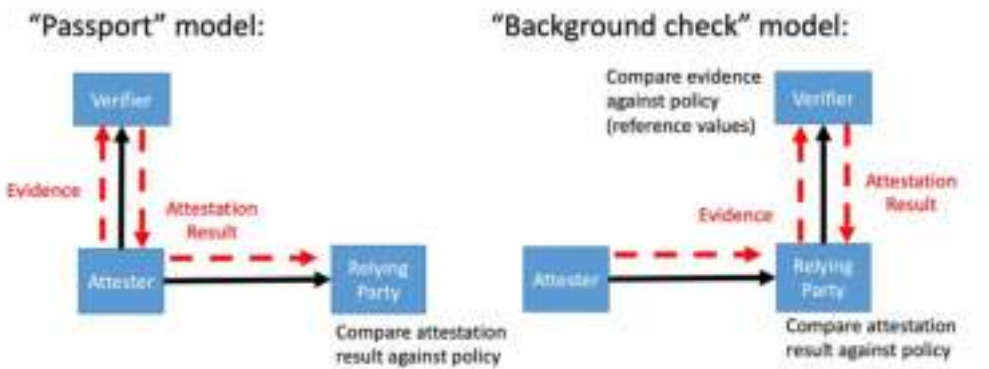
IdP: Identity Provider
CDM: Continuous Diagnostics & Mitigation

PEP/PDP: Policy Enforcement / Decision Point



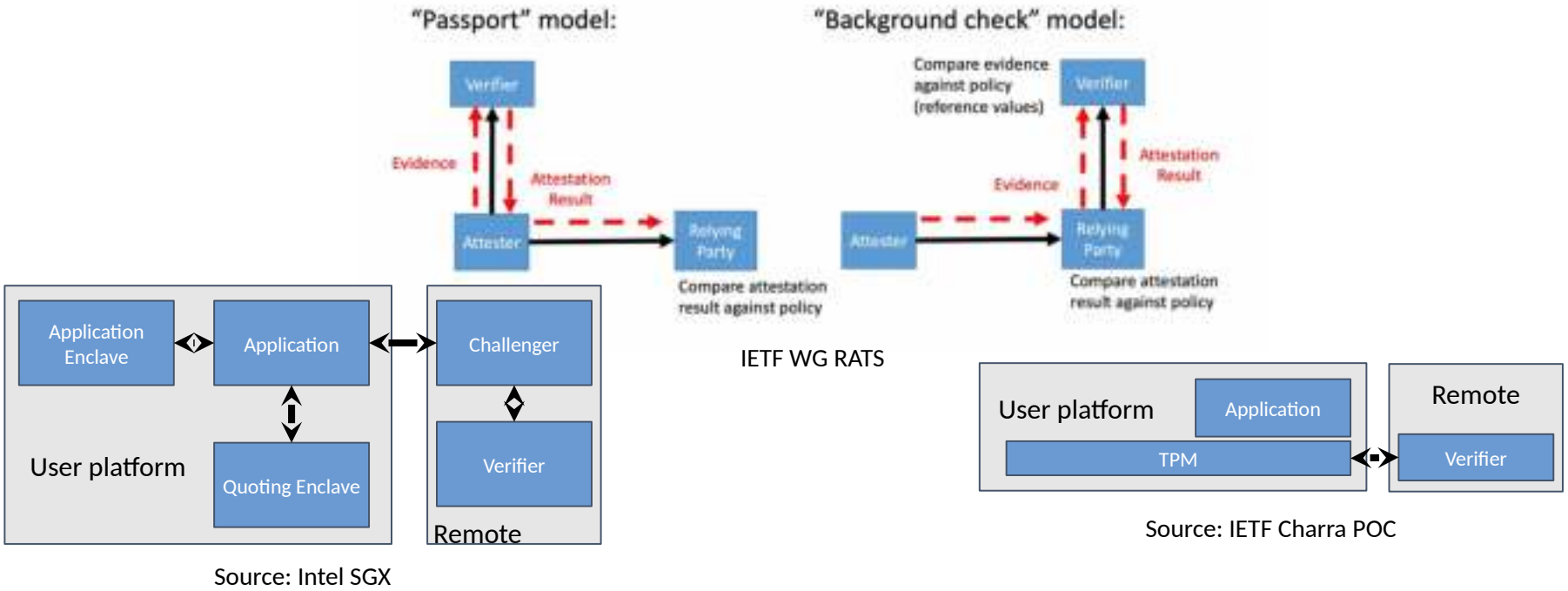
Illustrations: freepik.com

Remote Attestation



IETF WG RATS

Remote Attestation



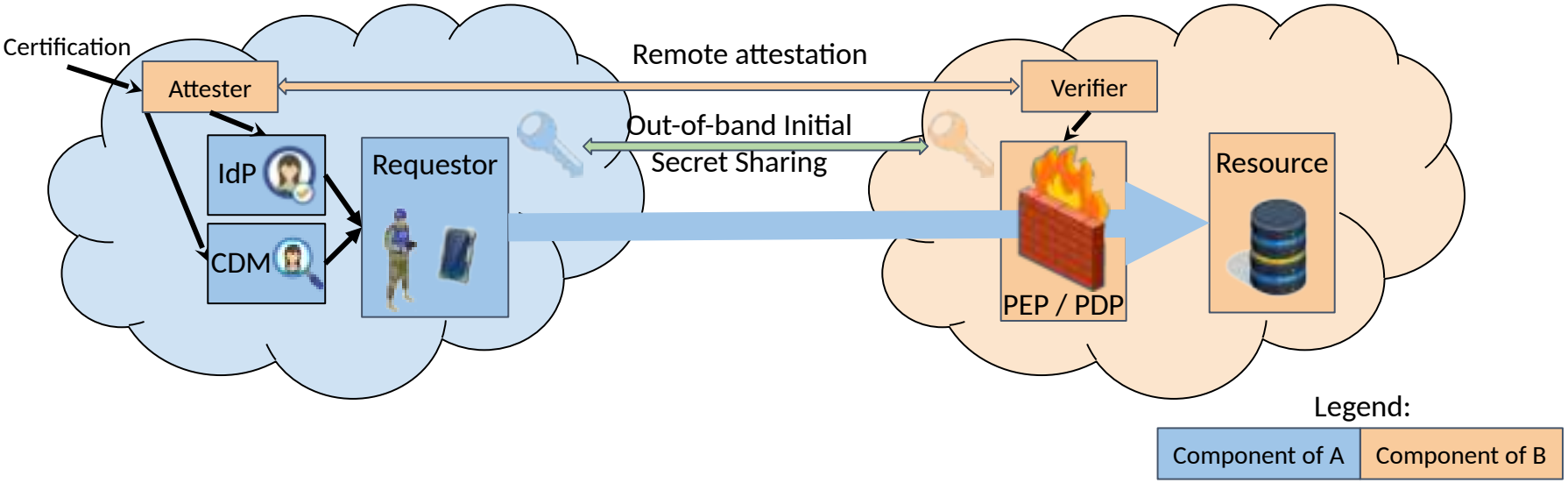
Source: Intel SGX

Source: IETF Charra POC

Root of Trust

Initial trust between domains:

- Certification of remote attestation components
- Onboarding (shared secrets)



Illustrations: freepik.com

Proof of Concept


```
Message Data Received:
{"action": "remote_attestation", "attestation_result": true "client_sdpid": "12347"}
Message parsed
Message received from SDP ID 12350
JSON-Parsed Message Data Received:
key: action    value: remote_attestation
key: attestation_result    value: true
key: client_sdpid    value: 12347


SENDING MESSAGE:
{"action":"remote_attestation_ack"}
```

```
Trying to match:
rank=OF-2
{
  'urn:oid:2.5.4.4': [ 'Poirrier' ],
  rank: [ 'OF-2' ],
  'urn:oid:1.2.840.113549.1.9.1': [ 'alexandre.poirrier@polytechnique.edu' ],
  'urn:oid:2.5.4.42': [ 'Alexandre' ]
}
```

Proof of Concept

Zero Trust Architecture

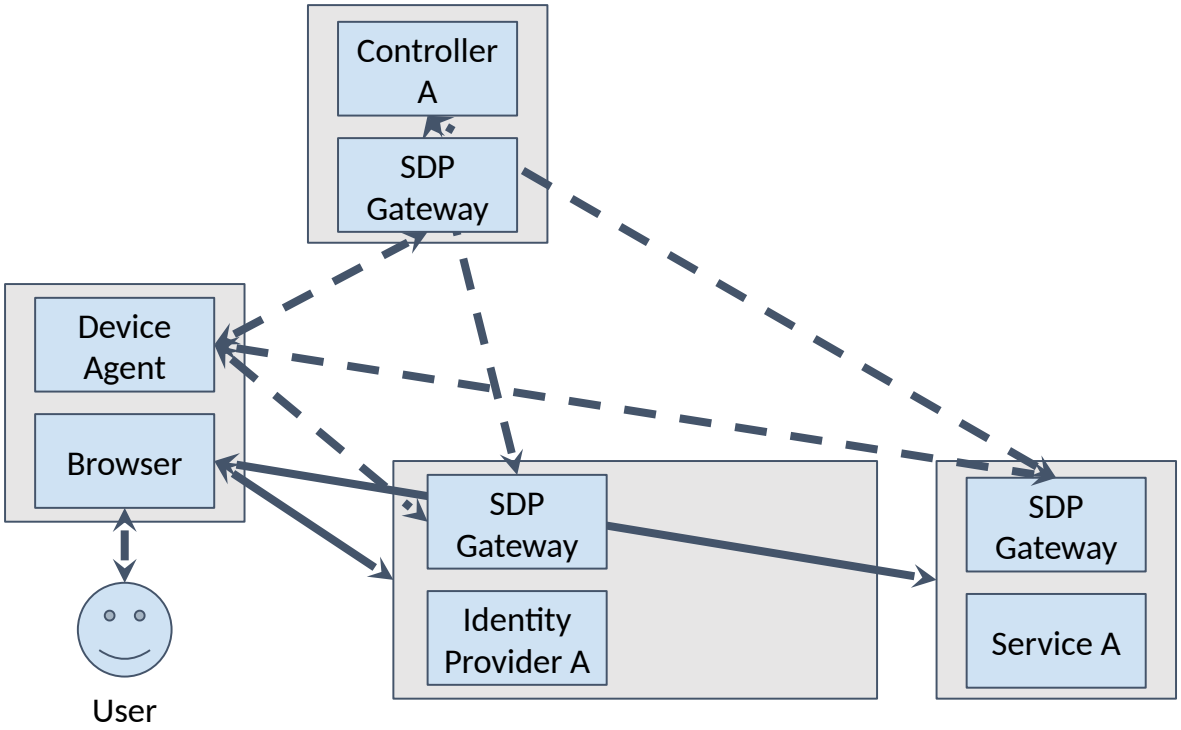
Software-Defined Perimeter

Identity Provider

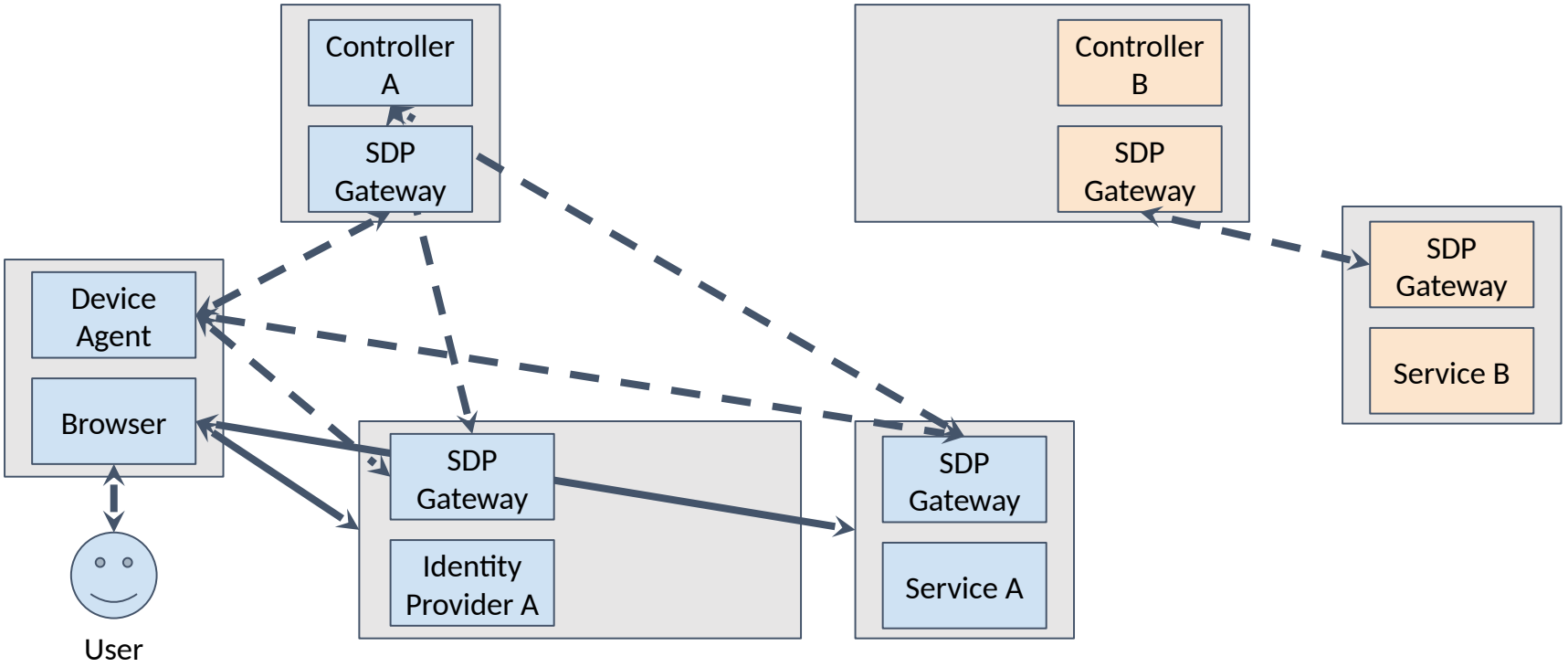
Remote Attestation

IETF Charra

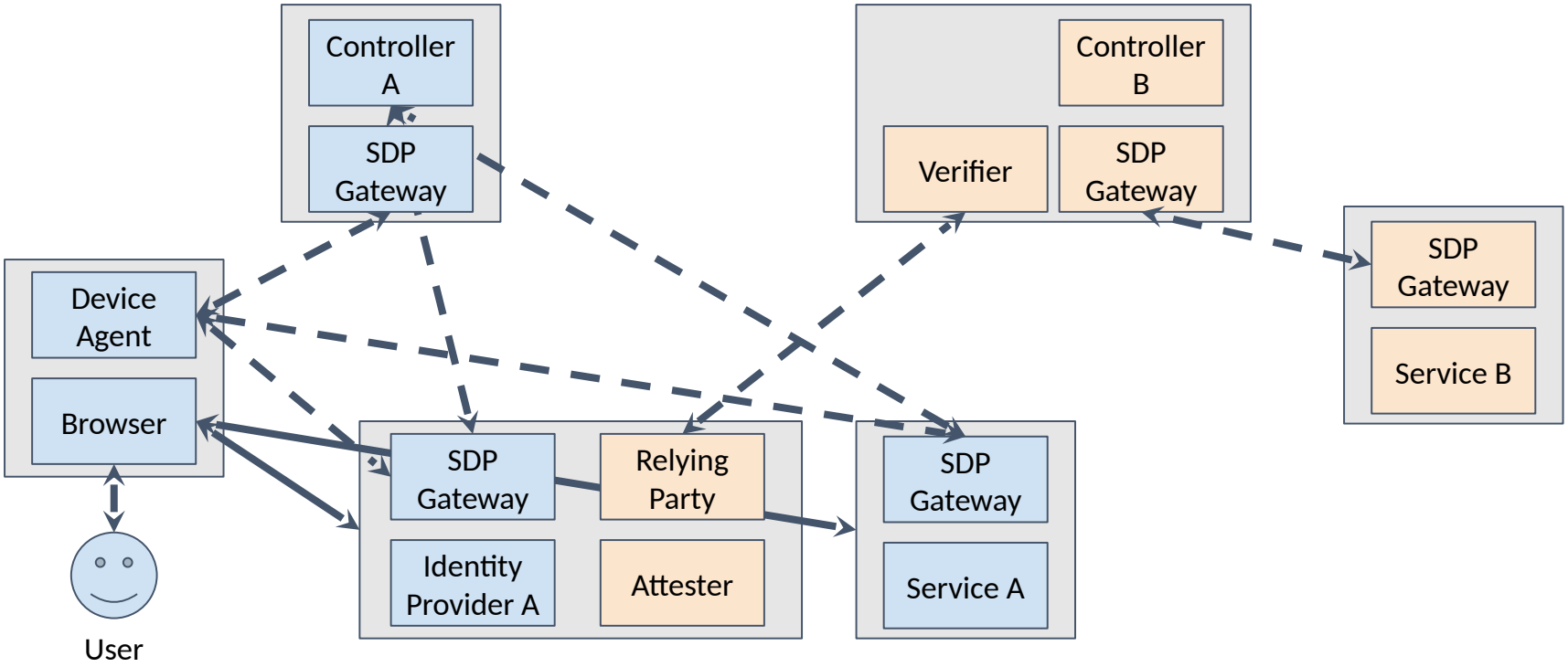
Proof of Concept



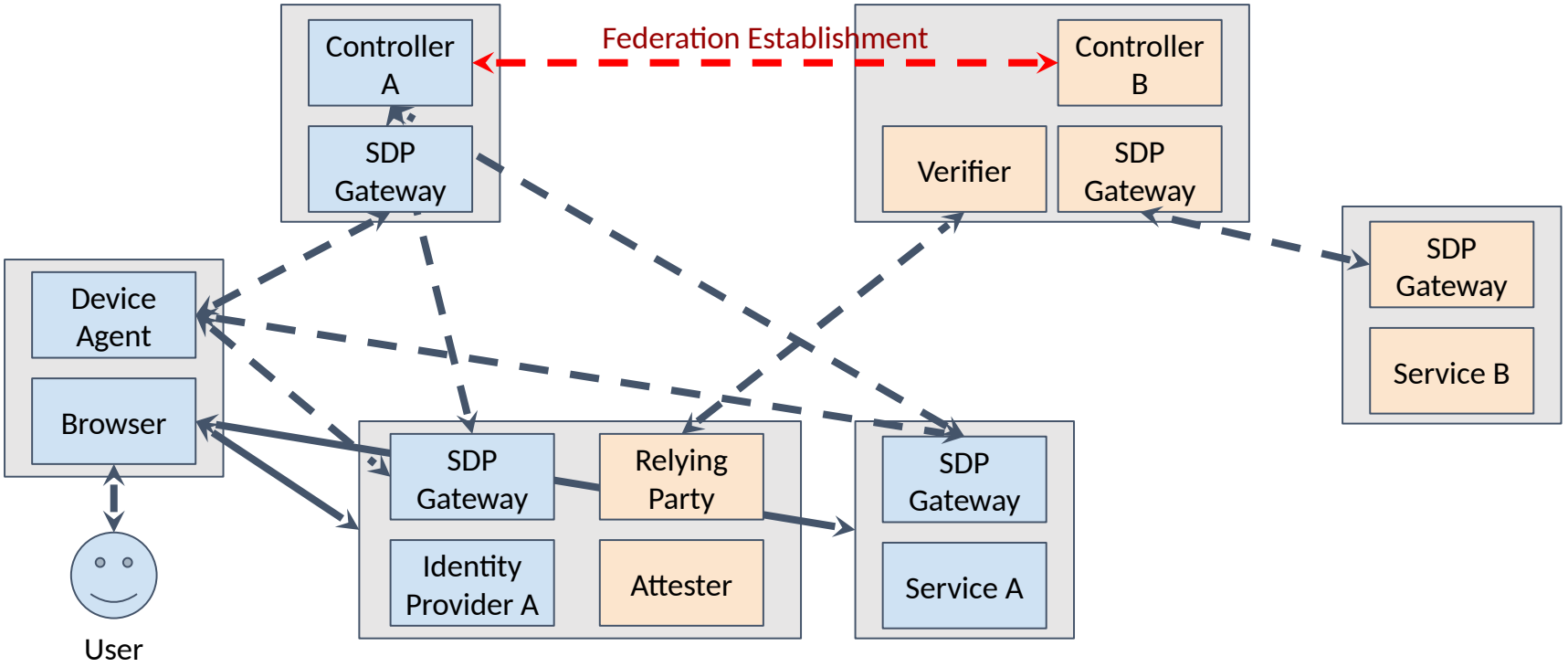
Proof of Concept



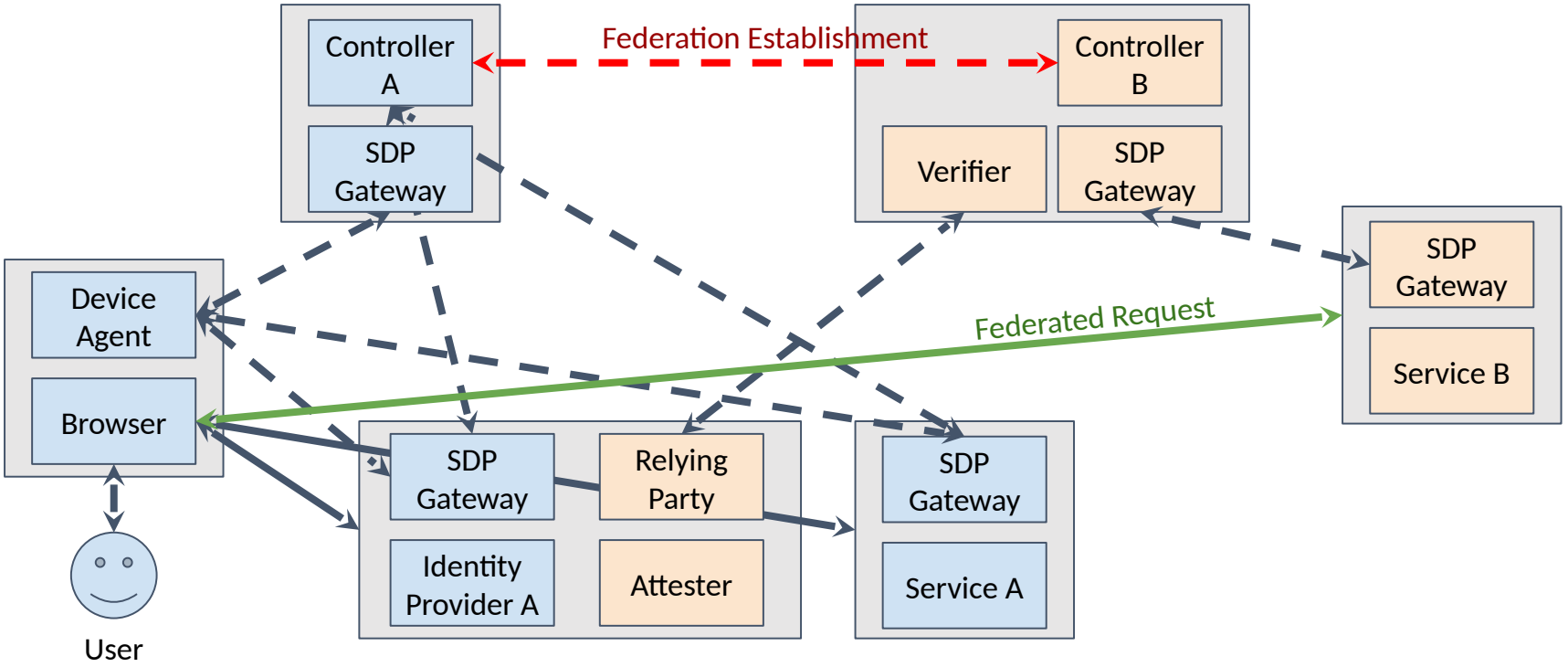
Proof of Concept



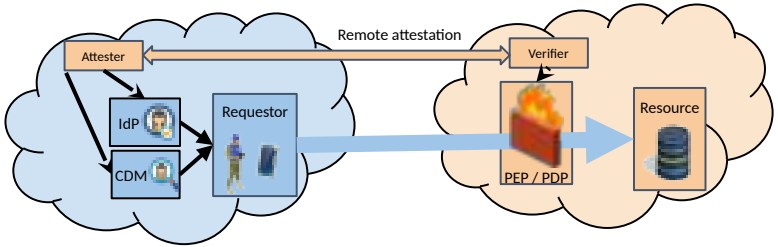
Proof of Concept



Proof of Concept



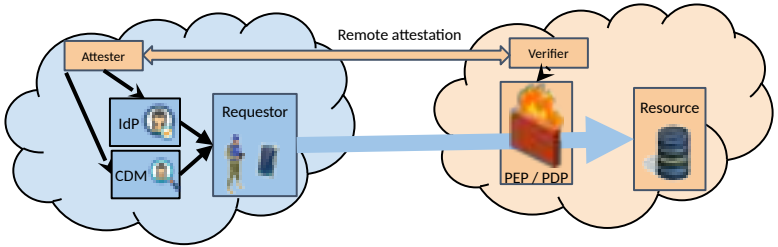
Contributions



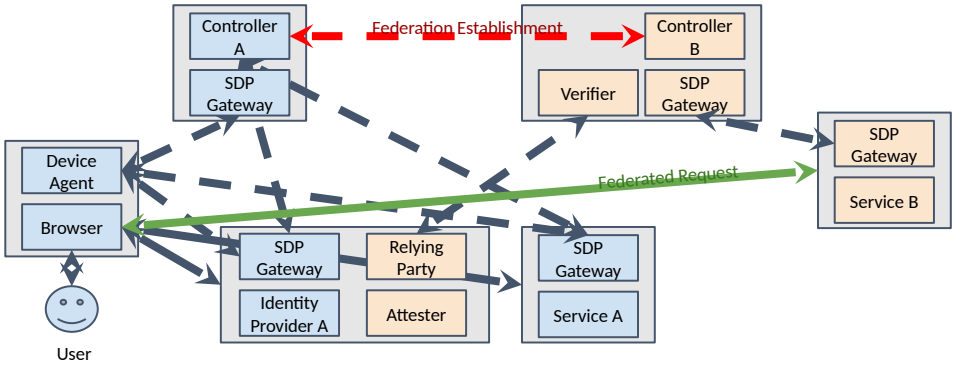
Zero Trust Federation based on remote attestation

Contributions

Illustrations: freepik.com



Zero Trust Federation based on remote attestation



SDP-based proof-of-concept

European Cyber Week

POLE D'EXCELLENCE by CYBER

Thank you!

ÉCOLE POLYTECHNIQUE

IP PARIS

DGA
DIRECTION GÉNÉRALE DE L'ARMEMENT