Universal Name System (UNS)

Global and unified cryptographic namespace
for person and non-person entities

Universal Certificate Authority (UCA)

Global and automated cryptographic infrastructure
to solve code and data provenance, integrity,
authenticity, confidentiality and privacy

DNS + CAs	UNS + UCA
Domain-centric	**Entity**-centric
Entities are **mere resources** in domains	Entities have **independent existence**
Bolted-on cryptographic security	**Built-in** cryptographic security
Administered	**Automated and generated**
Global “Zero Trust” **impossible**	Global “Zero Trust” **possible**

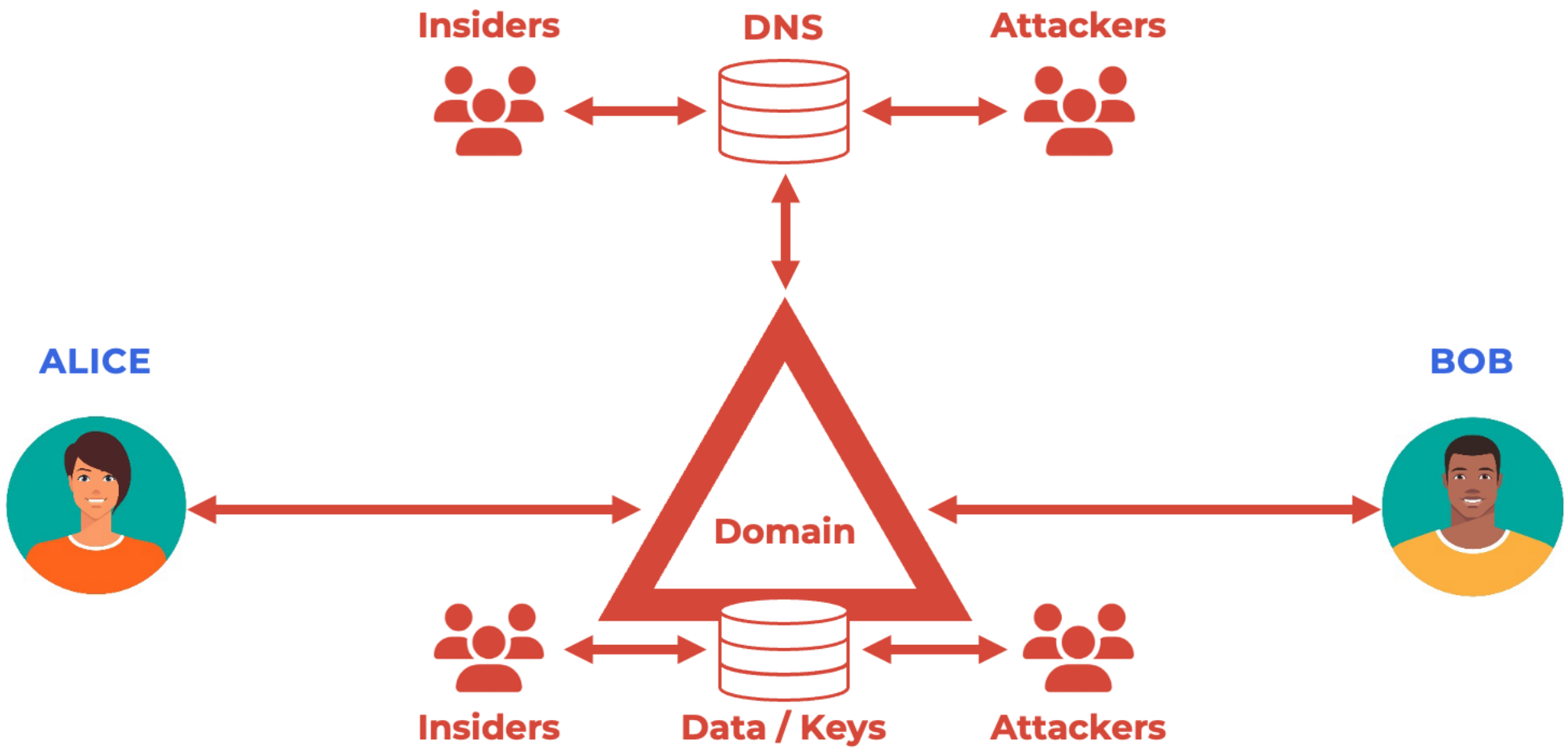
Enabled by Confidential Computing (TEEs)

1. **Cryptographic protection of data in use**, even from system admins
2. **Remote attestation and verification** of HW and SW authenticity
3. **Verifiable confidential entropy** for decentralized cryptography

World Wide Weaknesses

#1 – Privileged insiders

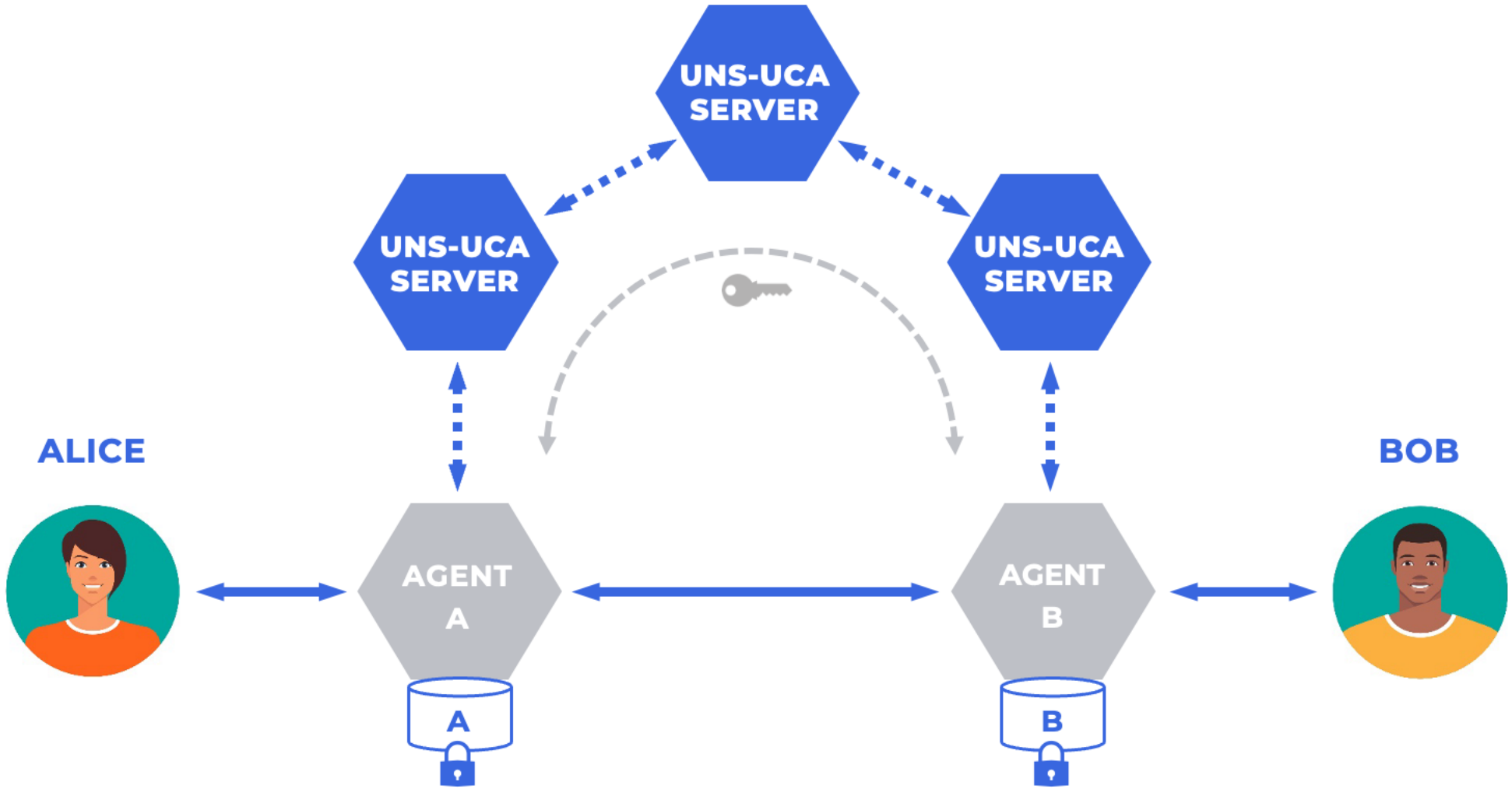
#2 – Weak relational links


Insiders
DNS
Attackers
ALICE
BOB
Domain
Insiders
Data / Keys
Attackers

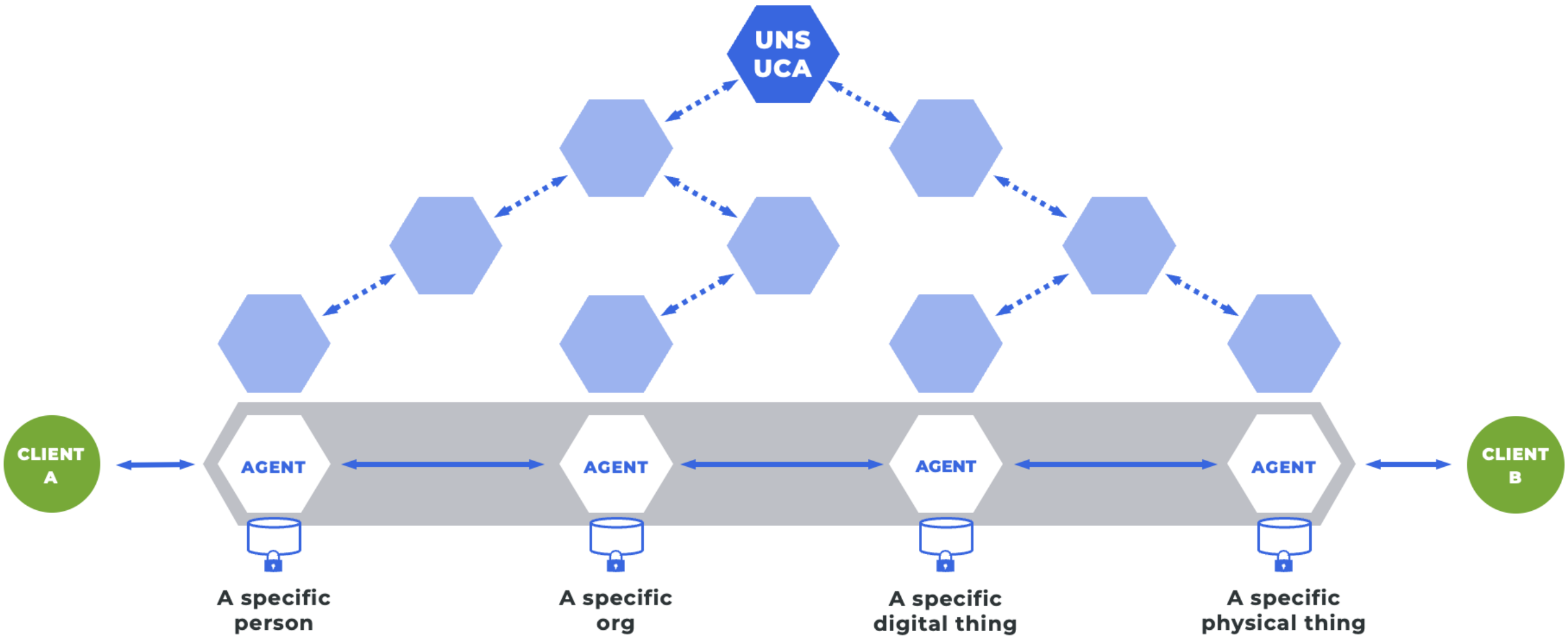
Domain name / path / resource

Entity StemID # relationship # keyname

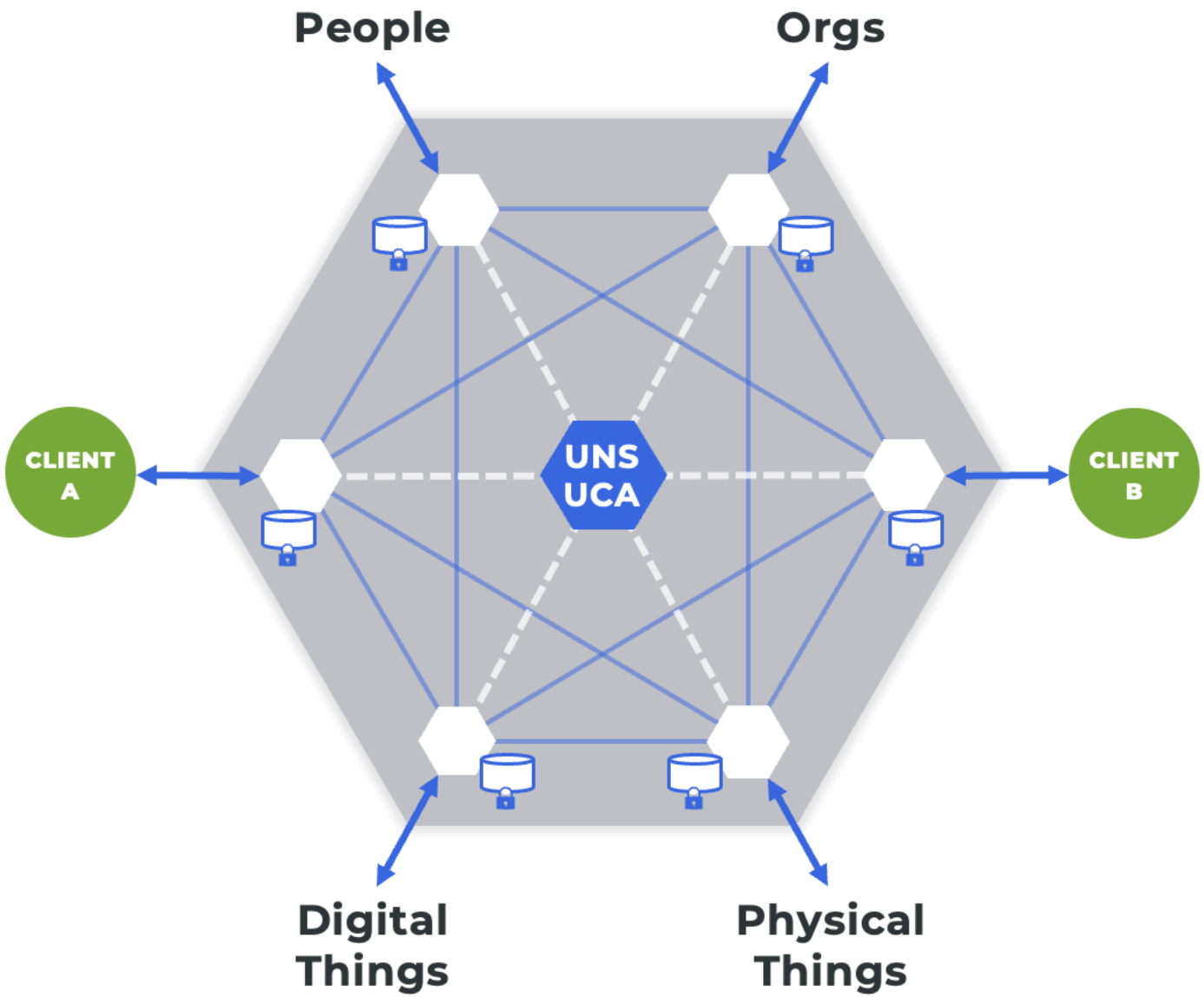
is the HMAC key derivation function


UNS-UCA SERVER
UNS-UCA SERVER
UNS-UCA SERVER
ALICE
BOB
AGENT A
AGENT B
A
B

Chaining entities (not blocks)



Fully automated, no humans in the middle



Present and discuss this work

Figure out where in IETF this work should go

Starting coalition for **global and neutral governance**

Side Meeting in **Palmovka 1/2** on **Monday @ 14:00**

manu@hushmesh.com