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
<table>
<thead>
<tr>
<th>DNS + CAs</th>
<th>UNS + UCA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain-centric</strong></td>
<td><strong>Entity-centric</strong></td>
</tr>
<tr>
<td>Entities are <em>mere resources</em> in domains</td>
<td>Entities have <em>independent existence</em></td>
</tr>
<tr>
<td><em>Bolted-on</em> cryptographic security</td>
<td><em>Built-in</em> cryptographic security</td>
</tr>
<tr>
<td><em>Administered</em></td>
<td><em>Automated and generated</em></td>
</tr>
<tr>
<td>Global “Zero Trust” <em>impossible</em></td>
<td>Global “Zero Trust” <em>possible</em></td>
</tr>
</tbody>
</table>
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
Domain name / path / resource
Entity StemID  # relationship  # keyname

# is the HMAC key derivation function
Chaining entities (not blocks)
Fully automated, no humans in the middle

People — Orgs

CLIENT A — UCA — CLIENT B

Digital Things — Physical Things
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