Verifiable Identity using Distributed Authentication (VIDA)

Dr. Neal Krawetz
Hacker Factor

IETF 119 HotRFC
Problem Space

• Need reliable way to attribute content to author
  “Is it authentic?”
  “Was it altered?”
  “Who created this?”
  • False attribution
  • Non-repudiation
Existing Proposed Solutions

- **Blockchain**
  - Fails to scale to high volume
  - Many use proprietary details

- **C2PA** (Content Coalition for Provenance and Authentication)
  - Corporate-driven solution, closed-door design
  - 100% based on “trust”
    - Trust metadata & content is legitimate
    - Trivial to make cryptically authenticated forgeries
  - Pay to Play (no self-signed X.509 certs)
Proposed Solution

- Anti-Spam got it right!
  - DKIM (RFC 6376, DomainKeys Identified Mail)

![Diagram showing the process of DKIM]

Public Key

Private Key

DNS TXT DKIM

Neal Krawetz, Hacker Factor

IETF 119 HotRFC
Proposed Solution

- VIDA: validation based on DKIM

- VIDTX: Public Key
- VIDA: Private Key
- DNS
- TXT VIDA

- Domain/host for DNS lookup
- Optional: Parameters for signature
- Signature (bytes)
# VIDA Provides

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribution</td>
<td>Attributed to the domain or hostname</td>
</tr>
<tr>
<td>Authentication</td>
<td>It came from the domain; private key prevents forgeries</td>
</tr>
<tr>
<td>Validation</td>
<td>Cryptographic signature identifies tampering</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Only your domain has private key, so it came from your domain!</td>
</tr>
<tr>
<td>Low cost</td>
<td>Domain required, but permits signing services! (Cheaper than X.509)</td>
</tr>
<tr>
<td>Privacy</td>
<td>DNS relays, no centralized validator, signer cannot track usage</td>
</tr>
<tr>
<td>Distributed</td>
<td>DNS! Anyone can use this; no dependency on single vendor</td>
</tr>
</tbody>
</table>

Neal Krawetz, Hacker Factor  
IETF 119 HotRFC
What I Need...

• Help!
  – Ironing out specification details
  – Writing up the RFC
    • Navigating the RFC submission process
    • Reducing my long essays to minimal RFC documentation
  – Implementing
    • Working examples and public tools/libraries
Verifiable Identity using Distributed Authentication (VIDA)

Contact:
Dr. Neal Krawetz
Hacker Factor
pasta@hackerfactor.com

Thank you for your time!