certspec (in brief)

Sean Leonard, Penango, Inc.
IETF 84 PKIX
Wednesday, August 1, 2012
What is certspec?

urn:cert:issuersn:CN=Atlantis;2A

• Uniform syntax for
• identifying
• a *specific* certificate
• in a textual format
URN Primer

• Resource identifiers that are **persistent, location-independent, text-based** (transcribable by keyboard & recognizable by humans), **mappable** to other URIs

• RFC 2141; urnbis

• Examples:
  – urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
  – urn:oid:1.3.6.1.4.1
  – urn:ietf:rfc:2141
  – urn:isbn:0-395-36341-1
Motivation

• Apps
  – in preferences for runtime retrieval
  – for exchange

• Protocols
Mechanisms

urn:cert:SHA-256:0de4564b...fa592f58

• by-reference
  – by-hash (SHA-1, SHA-2)
    (not “parameterized”)
  – by-data (issuersn)

• by-value
  – data (base64, hex)
Compare certspec with others

- Existing preferences not portable, exchangeable, or algorithm-agile
- Different protocols reinvent the wheel
- Want by-value and by-ref agility
  - eliminates DoS vector, lookup time

<table>
<thead>
<tr>
<th>certspec URN</th>
<th>ni URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>URN for certs</td>
<td>URI for any digital object</td>
</tr>
<tr>
<td>Canonical enc / unique ID</td>
<td>No canonicalization / not unique</td>
</tr>
<tr>
<td>No truncation allowed (&quot;security&quot;)</td>
<td>Truncation encouraged (&quot;flexibility/brevity&quot;)</td>
</tr>
<tr>
<td>copy &amp; paste, visual comparison from existing crypto tools</td>
<td>Full support requires new implementations; base64url support</td>
</tr>
</tbody>
</table>
Next Steps

• (Probably) in Apps WG
• Harmonize with urnbis
• Want to publish something relevant to implementers and users
• Improve Motivation section

Questions?