## Comparison with draft-das

<table>
<thead>
<tr>
<th></th>
<th>draft-das</th>
<th>draft-wei</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Model</strong></td>
<td>similar</td>
<td>similar</td>
</tr>
<tr>
<td><strong>Messages</strong></td>
<td>INIT-REQ/RESP REG-REQ/RESP DBQUERY-REQ/RESP DBNOTIF-REQ/RESP DEVVALID-REQ/RESP</td>
<td>REG-REQ/RESP AVAILWS-REQ/RESP CHUSAGE-REQ/RESP DEVVALID-REQ/RESP</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Server certificate &amp; client Digest based on shared secret</td>
<td>Server &amp; client certificate validated during TLS</td>
</tr>
<tr>
<td><strong>Encoding</strong></td>
<td>Suggests JSON</td>
<td>Defines XML schema</td>
</tr>
<tr>
<td><strong>Usage of HTTP</strong></td>
<td>POST in both directions</td>
<td>PUT (registration, chusage); GET (query, validation) Responses are in HTTP Responses (200 OK)</td>
</tr>
</tbody>
</table>
Security Discussion

- The Digest in draft-das is not HTTP Digest
  - It is a re-implementation of Digest at the application layer
- Digest is subject to Asokan-style attacks
  - Need a secure binding between the TLS authentication and the Digest authentication
- Digest requires a shared symmetric key
  - Key distribution is difficult to do securely
  - If the master device changes database providers, key redistribution would be required
- Suggestion: add option for client certs
- More on security later from Yang Cui
Encoding Discussion

• XML Schema vs. JSON
  – XML schema is more rigorously defined
HTTP Usage Discussion

• Responses more appropriate than server-to-client POST method
  – Can be 200 OK with body
Messages Discussion

• To support Digest-style authentication, would need to add one more XML message type to convey the server nonce