Bring Your Own Identity
<table>
<thead>
<tr>
<th>Mech</th>
<th>Start/pw?</th>
<th>End/Iss/PI?</th>
<th>Integr. Proto</th>
<th>Xover</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML</td>
<td>Heavy</td>
<td>Possible v</td>
<td>v HTTP+SASL+...</td>
<td>PKI</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Infra</td>
<td>v</td>
<td>v GSSAPI</td>
<td>KXOVER</td>
</tr>
<tr>
<td>SASL</td>
<td>v [free choice] v</td>
<td>v</td>
<td>v</td>
<td>SXOVER</td>
</tr>
</tbody>
</table>

→ SASL wins
← except on HTTP

Mechs for Realm Crossover
HTTP - SASL

SXOVER (SASL crossover)

Req

req

realm mech

C2S = token
[ S2S = server state ]

resp

S2C = token
S2S = server state
realm mechlist

req + cached

S2S = server state
\rightarrow cached from zoo OK

channel binding

idP

@realm

Diameter:
- TLS (mutual)
- DNSSEC, DANE
K XOVER (Kerberos Crossover)

- std clients
- KDC extension
- impromptu KEX
- DNSSEC, DANE, TLS
- Quantum Crypto!!