EAP-TEAP-BRKSI   ???

Eliot Lear, Owen Friel, Dan Harkins, Nat Cam-Winget
IETF 106
Draft-lear-eap-teap-brski changes

• Diagrams have been simplified
• Rework of discussion around NAI
• Beginning of restructuring toward a different target:
  • Rather than focus just on BRSKI, focus on overall TEAP update
# Goals: Go through RFC 7170 Errata

<table>
<thead>
<tr>
<th>Erratum</th>
<th>Reported by</th>
<th>Topic</th>
<th>Proposed Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5127</td>
<td>Tuure Vartiainen</td>
<td>Typo “</td>
<td>” instead of “,” in TLS_PREF call</td>
</tr>
<tr>
<td>5128</td>
<td>Tuure Vartiainen</td>
<td>Typo “,” instead of “</td>
<td>” in TLS_PREF</td>
</tr>
<tr>
<td>5765</td>
<td>Juoni Malinen</td>
<td>Authority TLV only required in outer</td>
<td>Accept</td>
</tr>
<tr>
<td>5767</td>
<td>Juoni Malinen</td>
<td>Clarify Intermediate-Result language within tunnel</td>
<td>Discuss</td>
</tr>
<tr>
<td>5768</td>
<td>Juoni Malinen</td>
<td>Incompatible field lengths, and TLS version issues</td>
<td>Discuss</td>
</tr>
<tr>
<td>5770</td>
<td>Juoni Malinen</td>
<td>S-IMCK[j] derivation confusion</td>
<td>Discuss</td>
</tr>
<tr>
<td>5775</td>
<td>Juoni Malinen</td>
<td>CMK derivation confusion</td>
<td>Discuss</td>
</tr>
<tr>
<td>5844</td>
<td>Juoni Malinen</td>
<td>Crypto binding used when Intermediate result should be used</td>
<td>Accept</td>
</tr>
<tr>
<td>5845</td>
<td>Juoni Malinen</td>
<td>Method completion text unclear</td>
<td>Discuss (but it’s close)</td>
</tr>
</tbody>
</table>
New TLVs

- Voucher
- CSRATTRs
- Root certs
- NAI
- ???
Key issue

• How does TEAP interact with other 802.11 capabilities?
  • DPP
  • Other...
Next Steps

• Should we have a section that just accepts errata and update?
• Do we deal with TLS 1.3 or should that be in the TLS 1.3 doc?
• Proposal
  • Less focus on BRSKI, more focus on update
  • Roll it slow. Get some coding done
  • Maybe adopt draft as WG draft but not plan for approval until we nail above, plus any proposed new TLVs