Status

• Draft -02 submitted on March 12, 2012
• Addressed most of the open issues
• Only received a few review comments
  – Thanks Jim Schaad and Sam Hartman for your comments
• New issue tracking list was created (total of 7):
• Need more reviews
## Issues Overview

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Certificate enrollment and distribution</td>
<td>Closed</td>
</tr>
<tr>
<td>34</td>
<td>Server unauthenticated provisioning</td>
<td>Closed</td>
</tr>
<tr>
<td>35</td>
<td>TLV numbering</td>
<td>Closed</td>
</tr>
<tr>
<td>36</td>
<td>Peer ID and server ID for sequenced authentication</td>
<td>Closed</td>
</tr>
<tr>
<td>37</td>
<td>Clarification in Version Negotiation</td>
<td>Closed</td>
</tr>
<tr>
<td>38</td>
<td>Crypto Binding TLV required for every authentication</td>
<td>Closed</td>
</tr>
<tr>
<td>39</td>
<td>EAP-GTC in Example</td>
<td>Closed</td>
</tr>
<tr>
<td>40</td>
<td>Clarification in Channel-binding TLV</td>
<td>Closed</td>
</tr>
<tr>
<td>41</td>
<td>Missing TLS Exporter Label and Identity Type in IANA Consideration</td>
<td>New</td>
</tr>
<tr>
<td>42</td>
<td>Support username/password processing function other than SASLPrep in Basic-Password-Auth TLVs</td>
<td>New</td>
</tr>
<tr>
<td>43</td>
<td>Peer requests channel binding using Request-Action TLV</td>
<td>New</td>
</tr>
<tr>
<td>44</td>
<td>More discussion on separation of TEAP server and inner method server and MITM attacks</td>
<td>New</td>
</tr>
<tr>
<td>45</td>
<td>More examples for Section 3.3</td>
<td>New</td>
</tr>
<tr>
<td>46</td>
<td>TLV ordering</td>
<td>New</td>
</tr>
<tr>
<td>47</td>
<td>Better Session ID</td>
<td>New</td>
</tr>
</tbody>
</table>
Issue #33

• Issue: Certificate provisioning was described using PKCS#10 TLV, however no mechanism to send certificate provisioning request.

• Status: Closed

• Resolution:
  – In Draft-02, a new section 3.9 Certificate Provisioning Within the Tunnel is added to describe how certificate is provisioned inside the tunnel.
Issue #34

- Issue: Mandatory to Implement (MTI) inner authentication method for server unauthenticated provisioning

- Status: Closed

- Resolution:
  - Described the property of the inner EAP method.
  - MTI not specified as it is an optional feature.
Issue #35

- **Issue**: TLV numbering starts at 3. Number 0-2 was not used. There are also some gaps in the TLV number.

- **Status**: Closed.

- **Proposed resolution**:
  - Draft-02 uses the consecutive TLV numbers starting from 1.
Issue #36

- Issue: If multiple authentications occur in tunnel establishment or within the tunnel, what is the peer ID and server ID to be used.

- Status: Closed

- Resolution:
  - Draft-02 states all authenticated identity need to be exported.
Issue #37

• Issue: Section 3.1, Version negotiation
  – What happens if peer only supports a higher version than the server supports?

• Status: Closed

• Resolution:
  – Clarified that peer should send a NAK with other proposed EAP method if available.
Issue #38

• Issue:
  1. Draft-00 not clear about whether crypto-binding is run after a single EAP inner authentication.
  2. Crypto-binding not run after inner method being skipped.

• Status: Closed

• Resolution:
  – Clarified that crypto-binding will always be run after every single EAP authentication (in a sequence or not), also even if there is no inner EAP authentication or, to ensure the outer TLVs and EAP type, version are verified.
Issue #39

- Issue: Example section still reference EAP-FAST-GTC.

- Status: Closed

- Proposed resolution:
  - Update example to replace EAP-FAST-GTC with Basic-Password-Auth TLVs in Draft-02.
Issue #40

• Issue: Channel Binding TLV should match Channel Binding draft. Clarify that Channel Binding TLV can be used to transmit bidirectional channel binding data and verification result.

• Status: Closed

• Proposed resolution:
  – Draft-02 is updated to clarify that
Issue #41

• Issue: Missing TLS Exporter Label and Identity Type in IANA Consideration

• Status: New

• Proposed resolution:
  – Update in Draft-03
Issue #42

• Issue: How to support username/password processing function other than SASLPrep in Basic-Password-Auth TLVs?

• Status: New

• Proposed resolution:
  – New Byte field to indicate the processing function
  – Mandatory to implement – SASLPrep
  – Server sends all processing functions it supports and client picks the one it supports or NAK it.
Issue #43

- Issue: How would peer request channel-binding if the server already sends back Result-Success?

- Status: New

- Proposed resolution:
  - Peer sends Request-Action TLV with code 1 – Process TLV along with Request-Action TLV
  - Upon receiving it, server could send back the channel-binding Result
Issue #44

- Issue: More discussion on separation of TEAP server and inner method server and MITM attacks

- Status: New

- Proposed resolution:
  - Update section 7.3 & 7.4.
Issue #45

• Issue: More examples to understand Section 3.3, Protected Termination and Acknowledged Result Indication

• Status: New

• Proposed resolution:
  – Add examples for:
    • Peer requests an inner EAP method even when the server is happy to offer success in the first message
    • Peer wished to send certificate using TLS renegotiation after server sends inner method in Phase 2
    • Channel bindings interaction with the result indications.
Issue #46

- Issue: Is TLV ordering important for parsing and processing?
- Status: New
- Proposed resolution:
  - Change Request-Action TLVs to be a nested TLV to eliminate ordering.
  - No other ordering of TLV is needed.
Issue #47

• Issue:
  – Current Session-Id is defined as \( \text{Session-Id} = \text{teap_type} \ || \ \text{client_random} \ || \ \text{server_random} \)
  – Would something already standardized like tls-unique in section 3 of RFC 5929 be a better choice?

• Status: New

• Proposed resolution:
  – Reference RFC 5247 for Session-Id
  – Look into RFC5929 to see if it can be used.
Next step

• Submit new revision of draft addressing review comments and issues discussed.
• Move on to WGLC?
Thank You!