EAP Tunnel Method
draft-ietf-emu-eap-tunnel-method-01

Hao Zhou, Nancy Winget, Joe Salowey, Steve Hanna

EMU WG group
IETF 82
Status

• Draft -01 submitted on Oct 20, 2011
• Only received a few review comments
  – Thanks Dan Harkins, Jim Schaad, and Sam Hartman for your comments
• Issue tracking list was created (total of 13):
• Need more reviews
## Issues Overview

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Method Name</td>
<td>Closed</td>
</tr>
<tr>
<td>29</td>
<td>Version</td>
<td>Closed</td>
</tr>
<tr>
<td>30</td>
<td>PAC Provision Not Fully Described</td>
<td>Closed</td>
</tr>
<tr>
<td>31</td>
<td>Support Outer TLVs</td>
<td>Closed</td>
</tr>
<tr>
<td>32</td>
<td>Include outer TLV and EAP-Type in crypto binding</td>
<td>Closed</td>
</tr>
<tr>
<td>33</td>
<td>Certificate enrollment and distribution</td>
<td>Open</td>
</tr>
<tr>
<td>34</td>
<td>Server unauthenticated provisioning</td>
<td>Open</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>Open</td>
</tr>
<tr>
<td>38</td>
<td>Crypto Binding TLV required for every authentication</td>
<td>Open</td>
</tr>
<tr>
<td>39</td>
<td>EAP-GTC in Example</td>
<td>Open</td>
</tr>
<tr>
<td>40</td>
<td>Clarification in Channel-binding TLV</td>
<td>Open</td>
</tr>
</tbody>
</table>
Issue #28

• Issue: Need new method name replacing EAP-FAST

• Status: Closed

• Proposed resolution:
  – Draft -01 uses Tunnel EAP (TEAP) as the new tunnel method name replacing EAP-FAST
Issue #29

• Issue: Need to change version number from 2 to 1

• Status: Closed

• Proposed resolution:
  – Draft -01 changes version from 2 to 1
Issue #30

• Issue: Draft-00 did not fully describe PAC provisioning through RFC 5077 or within Phase 2

• Status: Closed

• Proposed resolution:
  – Draft -01 describes PAC provisioning through RFC 5077 in Section 3.2.2 and PAC provisioning in Phase 2 in Section 3.8
Issue #31

- Issue: Draft -00 did not support outer TLVs in the initial messages
- Status: Closed
- Proposed resolution:
  - Draft-01 adds the support for outer TLVs. Authority ID is now sent as an outer TLV
Issue #32

• Issue: Include outer TLV and EAP-Type in crypto binding to verify their integrity

• Status: Closed

• Proposed resolution:
  – In Draft-01 the outer TLVs and EAP type are included in the crypto-binding compound MAC.
Issue #33

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

• Status: Open

• Proposed resolution:
  – In Draft-01, a PKCS#10 TLV is added. PKCS#7 TLV was also included from EAP-FAST to complete the definition. However there needs to be more description somewhere on how enrollment is done
Issue #34

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

- Status: Open

- Proposed resolution:
  - This is still under discussion on the list.
  - Option:
    - Do nothing on the spec as it is already noted as an optional feature
    - Should describe unauthenticated server provisioning in a separate document
Issue #35

• Issue: TLV numbering starts at 3. Number 0-2 was not used.

• Status: Closed.

• Proposed resolution:
  – Draft-01 uses the TLV number 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

• Proposed resolution:
  – Draft-01 uses the first authenticated identity.
Issue #37

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

• Status: Open.

• Proposed resolution:
  – Clarify 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: Open

• Proposed resolution:
  – Clarify 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-GTC.

• Status: Open

• Proposed resolution:
  – Update example to remove EAP-GTC 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: Open

• Proposed resolution:
  – Update Draft-02 to clarify that
Next step

• Submit next version of draft addressing issues discussed.
• Move on to WGLC?
Thank You!