Agenda

- Blue Sheets, Agenda Bashing, Minutes - Chairs (2 min)
- WG Introduction - Russ Housley (3 min)
- Requirements and Problem Statement
  - Introduction - Chairs (5 min)
  - draft-vidya-eap-reauth-ps - Lakshminath Dondeti (10 min)
  - draft-nakhjiri-aaa-hokey-ps - Madjid Nakhjiri (10 min)
  - draft-ohba-preauth-ps - Yoshihiro Ohba (10 min)
  - Discussion (20 min)

- Keying Hierarchy
  - Introduction - Chairs (5 min)
  - draft-vidya-eap-er & draft-dondeti-eap-vkh - Vidya Naravanan (15 min)
  - draft-salowey-eap-emsk-deriv - Joe Salowey (10 min)
  - draft-nakhjiri-hokey-hierarchy - Madjid Nakhjiri (10 min)
  - Discussion (20 min)
HOKEY Description

• Extend EAP keying to facilitate handoff and roaming

• Expected solutions:
  – Reauth: Reauthentication to same authenticator
  – Handoff: Reauthentication to different authenticator in same domain
  – Roaming: Reauthentication to different authenticator in different domain
  – Preauth: Preauthentication using old, unexpired EAP keying material

• Requirements
  – Latency sensitive
  – Meet draft-housley-aaa-key-mgmt & draft-ietf-eap-keying
  – Access technology independent
  – Accommodate inter-technology handoff and roaming
  – No changes to EAP methods
# Milestones

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>-00</th>
<th>To IESG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Statement</td>
<td>Jan 07</td>
<td>Jul 07</td>
</tr>
<tr>
<td>EMSK Hierarchy</td>
<td>Jan 07</td>
<td>Apr 07</td>
</tr>
<tr>
<td>HRK Hierarchy</td>
<td>Feb 07</td>
<td>Aug 07</td>
</tr>
<tr>
<td>Reauth Protocol</td>
<td>Mar 07</td>
<td>Aug 07</td>
</tr>
<tr>
<td>Handoff Protocol</td>
<td>Mar 07</td>
<td>Sep 07</td>
</tr>
<tr>
<td>Roaming Protocol</td>
<td>Jun 07</td>
<td>Sep 07</td>
</tr>
<tr>
<td>Preauth Protocol</td>
<td>Sep 07</td>
<td>Mar 08</td>
</tr>
</tbody>
</table>
Problem Statement

• Problem statement
  – EAP re-authentication
  – Key management
• Milestones
  – January 2007: first draft
  – July 2007: submit to IESG
• Several documents, all covering somewhat different areas
• Need to merge into single document, need editor(s)
Keying Hierarchy

• Two hierarchies
  – EMSK keying hierarchy
  – Re-authentication and handoff keying hierarchy

• Milestones
  – January 2007: EMSK v00
  – February 2007: reauth/handoff v00
  – April 2007: EMSK I-D to IESG
  – August 2007: reauth/handoff to IESG

• Again, multiple documents
• Need editor(s)