Mapping Nonce-based 3-Party Authenticated Key Establishment Protocols

For a REST OAuth PoP-token Solution
Nonce-based Three Party Authenticated Key Establishment (AKE)

**Otway-Rees/Bauer-Berson-Feiertag (BBF)**

1. A
2. B
3. TTP
4. A

**Yahalom**

1. A
2. B
3. TTP
4. A

**Bellare-Rogaway (3PKD)**

1. A
2. B
3a. TTP
3b. TTP

**Boyd**

1. A
2. B
3. TTP
4. (If Key Confirmation)

* At the end of the document there are links to detailed descriptions of the protocols
Considerations

• Either RS or C can be mapped to be the sender of the first message of the AKE protocol (« A » in the Key Establishment literature)
  – We will map both alternatives for each AKE protocol (« A=C » and « A=RS »)

• In the Case of RS not having connectivity with AS the only possible solution of the studied protocols is BBF or Otway-Rees and RS acting as « A »

• On this document we focus on the flow of messages and not on the content/crypto properties.
Design Principles

• C always sends the first REST/OAuth message
• Messages are REST Request/Response Always
  – Some mappings can be improved if some REST Responses are delayed and piggyback information that in the present mappings are sent as a separate Req/Response pair of messages. No such improvements were made here.
Nomenclature/Notation

• Messages of the AKE Protocol
  – Enumeration mapped as: « 1 » \(\rightarrow\) \(\alpha\); « 2 » \(\rightarrow\) \(\beta\); « 3 » \(\rightarrow\) \(\gamma\); « 4 » \(\rightarrow\) \(\delta\)
  – We mark the AKE protocol messages in RED.

• Once Protocol has finished both C and RS are in possession of the PoP-Token and the Associated fresh PSK. C can securely interact with RS. This exchange (Request and Response) is shown in GREEN.
Otway-Rees/BBF (A=RS)
Otway-Rees/BBF (A=C)

Undesired?: * RS has to push to C (msg. 5)

1) $\alpha$
2) $\beta$
3) $\gamma$
4) $\delta$
5) $\epsilon$
6) $\zeta$
Undesired?:
* RS has to push to C (Msg. 7)
Yahalom (A=C)
3PKD (A=RS)
3PKD \((A=C)\)
Boyd (A=RS)
Boyd (A=C)

Undesired?:
* RS has to push to C (Msg. 5)
## Nr. Of Messages Per Entity

<table>
<thead>
<tr>
<th></th>
<th>RS</th>
<th>C</th>
<th>AS</th>
<th>Observations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AKE Msgs</td>
<td>REST Msgs</td>
<td>AKE Msgs</td>
<td>REST Msgs</td>
</tr>
<tr>
<td>Otway-Rees/BBF (A=RS)</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Otway-Rees/BBF (A=C)</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Yahalom (A=RS)</td>
<td>3</td>
<td>6</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Yahalom (A=C)</td>
<td>3</td>
<td>6</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>3PKD (A=RS)</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>3PKD (A=C)</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Boyd (A=RS)</td>
<td>3</td>
<td>6</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Boyd (A=C)</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

* We don’t count the (GREEN ) Messages of the Secured Req/Resp
** Obs: In the RS columns we marked in bold the minimum values (nr msg) for each column
(If we want to minimize the msgs of RS this helps on the choice of a suitable protocol)
A KE Protocols References

• Otway Rees:

• Bauer-Berson-Feiertag:
  – [https://dl.acm.org/citation.cfm?id=357373](https://dl.acm.org/citation.cfm?id=357373) (Needs ACM Subscription)

• Yahalom:

• Bellare-Rogaway (3PKD)

• Boyd