Alternative Approach for Postquantum Preshared Keys in IKEv2

draft-smyslov-ipsecme-ikev2-qr-alt

Valery Smyslov
svan@elvis.ru

IETF 106
PPK for IKEv2

Defined in [draft-ietf-ipsecme-qr-ikev2]:

Initiator

**IKE_SA_INIT**
HDR,SAi1,KEi,Ni,N(USE_PPK)

**IKE_SA_INIT**
HDR,SAr1,KEr,Nr,N(USE_PPK)

**IKE_AUTH**
HDR,SK{IDi,AUTH,SAi2,TSi,TSr,N(PPK_IDENTITY)[,N(NO_PPK_AUTH)]}

**IKE_AUTH**
HDR,SK{IDr,AUTH,SAr2,TSi,TSr,N(PPK_IDENTITY)}

Responder
The Problem

- Initial IKE SA is not protected by PPK (WG decision)
  - it was assumed that no sensitive information was transferred over initial SA, and one could immediately rekey it to get protection
- G-IKEv2 ([draft-yeung-g-ikev2](https://datatracker.ietf.org/doc/draft-yeung-g-ikev2/)) uses initial IKE SA to immediately transfer session keys from Group Controller/Key Server (GCKS) to Group Member (GM)
  - the keys are not protected by PPK

<table>
<thead>
<tr>
<th>GM</th>
<th>GCKS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IKE_SA_INIT</strong></td>
<td><strong>IKE_SA_INIT</strong></td>
</tr>
<tr>
<td>HDR,SAi1,KEi,Ni,N(USE_PPK)</td>
<td>HDR,SAr1,KEr,Nr,N(USE_PPK)</td>
</tr>
<tr>
<td><strong>GSA_AUTH</strong></td>
<td><strong>GSA_AUTH</strong></td>
</tr>
<tr>
<td>HDR,SK{IDi,AUTH,IDg,</td>
<td>HDR,SK{IDr,AUTH,N(PPK_IDENTITY),</td>
</tr>
<tr>
<td>N(PPK_IDENTITY)[,N(NO_PPK_AUTH)]}</td>
<td>GSA,KD}</td>
</tr>
</tbody>
</table>
Currently G-IKEv2 draft suggests the following sequence of exchanges to get the protection with PPK:

**GM**

**IKE_SA_INIT**
HDR,SAi1,KEi,Ni,N(USE_PPK)

**GSA_AUTH**
HDR,SK{IDi,AUTH,IDg,
N(PPK.IDENTITY) [, N(NO_PPK_AUTH)]}

**CREATE_CHILD_SA**
HDR,SK{SAi,KEi,Ni}

**INFORMATIONAL**
HDR,SK{D}

**GSA_REGISTRATION**
HDR,SK{IDg}

**GCKS**

**IKE_SA_INIT**
HDR,SAr1,KEr,Nr,N(USE_PPK)

**GSA_AUTH**
HDR,SK{IDr,AUTH,N(PPK.IDENTITY),
N(REKEY_IS_NEEDED)}

**CREATE_CHILD_SA**
HDR,SK{SAr,KEr,Nr}

**INFORMATIONAL**
HDR,SK{}

**GSA_REGISTRATION**
HDR,SK{GSA,KD}
Alternative Approach

Proposed in draft-smyslov-ipsecme-ikev2-qr-alt:

\[
\begin{align*}
\text{IKE-SA\_INIT} & \quad \text{IKE-SA\_INIT} \\
\text{GSA\_AUTH} & \quad \text{GSA\_AUTH}
\end{align*}
\]
Comparison

• For G-IKEv2:
  – 3 exchanges instead of 5 (4 round trips)
  – 1 DH shared key computation instead of 2
  – 1 computation of AUTH in case of optional PPK instead of 2
  – initiator can propose several PPK_ID

• Can also be used in IKEv2:
  – 3 exchanges instead of 2
    • but PPK_ID can be piggybacked if IKE_INTERMEDIATE is also used for other purposes
  – 1 computation of AUTH in case of optional PPK instead of 2
  – initiator can propose several PPK_ID
Coexistence

• The proposed approach is **not intended to replace** the existing one, both can co-exist:
  – for G-IKEv2 the proposed approach can be a primary one (or the only one?)
  – for IKEv2 the proposed approach can be an alternative one (e.g. if IKE identities need to be protected)
Thanks

- Comments? Questions?
- More details in the draft
- WG adoption?