IP Security Maintenance and Extensions (IPsecME) WG

IETF 101, Friday, March 23, 2018

Chairs: David Waltermire
        Tero Kivinen

Responsible AD: Eric Rescorla
Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

• By participating in the IETF, you agree to follow IETF processes and policies.

• If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

• As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

• Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

• As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
• BCP 9 (Internet Standards Process)
• BCP 25 (Working Group processes)
• BCP 25 (Anti-Harassment Procedures)
• BCP 54 (Code of Conduct)
• BCP 78 (Copyright)
• BCP 79 (Patents, Participation)
• https://www.ietf.org/privacy-policy/ (Privacy Policy)
Administrative Tasks

Bluesheets
We need volunteers to be:
• Two note takers
• One jabber scribe

Jabber: xmpp:ipsecme@jabber.ietf.org?join
MeetEcho: http://www.meetecho.com/ietf101/ipsecme/
Etherpad:
Agenda

- Agenda bashing, Logistics -- Chairs (5 min) (11:50-11:55)
- Rechartering – Chairs (5 min) (11:55-12:00)
- Draft Status -- Chairs, Valery (10 min) (12:00-12:10)
  - Update on QR IKEv2 -- Valery Smyslov - draft-ietf-ipseme-qr-ikev2
- Work / Other items (70 min)
  - Postquantum Key Exchange to IKE (15 min) - CJ Tjhai (12:10-12:25)
    - draft-tjhai-ipsecme-hybrid-qske-ikev2
  - Labeled IPsec (5 min) - Paul Wouters (12:25-12:30)
    - draft-sprasad-ipsecme-labeled-ipsec
  - Auxiliary Exchange in the IKEv2 Protocol (15 min) - Valery Smyslov (12:30-12:45)
    - draft-smyslov-ipsecme-ikev2-aux
  - Group Key Management using IKEv2 (15 min) – Brian Weis (12:45-13:00)
    - draft-yeung-g-ikev2
  - IKE_SA_INIT privacy concerns (10 min) - David Schinazi (13:00-13:10)
    - draft-dschinazi-ipsecme-sa-init-privacy-addition
  - Dynamic IPsec PMTU PLPMTUD (10 min) - Shibu Piriyath, Ron Bonica (13:10-13:20)
    - draft-spiriyath-ipsecme-dynamic-ipsec-pmtu
WG Status Report

Draft status
• [draft-ietf-ipsecme-eddsa-04](https://www.ietf.org/rfc/draft-ietf-ipsecme-eddsa-04.txt) – In RFC Ed Queue

Other drafts are near ready for WGLC
• [draft-ietf-ipsecme-implicit-iv-00](https://www.ietf.org/rfc/draft-ietf-ipsecme-implicit-iv-00.txt)
• [draft-ietf-ipsecme-qr-ikev2-02](https://www.ietf.org/rfc/draft-ietf-ipsecme-qr-ikev2-02.txt)

We have been reviewing new charter items on the wiki
https://trac.ietf.org/trac/ipsecme/wiki/recharter2017
## Milestones

<table>
<thead>
<tr>
<th>Date</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>IETF Last Call on Using EdDSA in the IKEv2</td>
</tr>
<tr>
<td>Requested</td>
<td>IETF Last Call on Split-DNS Configuration for IKEv2</td>
</tr>
<tr>
<td>Feb 2017</td>
<td>IETF Last Call on Implicit IV in IPsec</td>
</tr>
<tr>
<td>Jun 2017</td>
<td>IETF Last Call on partially quantum resistant IKEv2</td>
</tr>
</tbody>
</table>
Rechartering

- [https://www.ietf.org/mail-archive/web/ipsec/current/msg11865.html](https://www.ietf.org/mail-archive/web/ipsec/current/msg11865.html)
- Out of 4 additional items, we added two and left out two
  - Added to charter
    - Address Failure Errors
    - Labeled IPsec
  - Not added to charter
    - Responder MOBIKE
    - Privacy concerns
Discussion of Current / Proposed Work

• Postquantum Key Exchange to IKE (15 min) - CJ Tjhai
draft-tjhai-ipsecme-hybrid-qske-ikev2
• Labeled IPsec (5 min) - Paul Wouters
draft-sprasad-ipsecme-labeled-ipsec
• Auxiliary Exchange in the IKEv2 Protocol (15 min) - Valery Smyslov
draft-smyslov-ipsecme-ikev2-aux
• Group Key Management using IKEv2 (15 min) – Brian Weis
draft-yeung-g-ikev2
• IKE_SA_INIT privacy concerns (10 min) - David Schinazi
draft-dschinazi-ipsecme-sa-init-privacy-addition
• Dynamic IPsec PMTU PLPMTUD (10 min) - Shibu Piriyath, Ron Bonica
draft-spiriyath-ipsecme-dynamic-ipsec-pmtu
Open Discussion

• Other points of interest?