IP Security Maintenance and Extensions (IPsecME) WG

IETF 114, Monday, July 25th, 2022

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Roman Danyliw

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

We need volunteers to be:

- Two note takers

Jabber: xmpp:ipsecme@jabber.ietf.org?join

MeetEcho: https://meetings.conf.meetecho.com/ietf114/?group=ipsecme&short=&item=1

Notes: https://notes.ietf.org/notes-ietf-114-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (15:00-15:05)
- Document Status – Chairs (15 min) (15:05-15:20)
- Work items
  - IKEv2 Downstream Fragmentation Notification Extension – Daniel Migault (20 min) (15:20-15:40)
  - IKEv2 Count Based SA Extension – Daniel Migault (20 min) (15:40-16:00)
  - IPsec Multi SA – Paul Wouters (10 min) (16:00-16:10)
  - Charter Update and Status – Chairs (10 min) (16:10-16:20)
- AOB + Open Mic (60 min) (16:20-17:00)

WG Status Report

- Published as RFC
  - draft-ietf-ipsecme-ikev2-intermediate published as RFC9242
- Publication requested:
  - draft-ietf-ipsecme-iptfs IESG Eval
  - draft-ietf-ipsecme-rfc8229bis IESG Eval
  - draft-ietf-ipsecme-yang-iptfs IETF Last Call
  - draft-ietf-ipsecme-ikev1-algo-to-historic AD eval
  - draft-ietf-ipsecme-mib-iptfs AD eval
  - draft-ietf-ipsecme-ikev2-multiple-ke Pub req
- Waiting for write-up / Chair review:
  - draft-ietf-ipsecme-labeled-ipsec
- Work in progress:
  - draft-ietf-ipsecme-auth-announce
  - draft-ietf-ipsecme-g-ikev2
  - draft-ietf-ipsecme-add-ike

Presentations

- IKEv2 Downstream Fragmentation Notification Extension –
  Daniel Migault
- IKEv2 Count Based SA Extension –
  Daniel Migault
- IPsec Multi SA –
  Paul Wouters

Presentations

- **IKEv2 Downstream Fragmentation Notification Extension – Daniel Migault**
- IKEv2 Count Based SA Extension – Daniel Migault
- IPsec Multi SA – Paul Wouters

Presentations

- IKEv2 Downstream Fragmentation Notification Extension –
  Daniel Migault
- **IKEv2 Count Based SA Extension –**
  Daniel Migault
- IPsec Multi SA –
  Paul Wouters

Presentations

- IKEv2 Downstream Fragmentation Notification Extension –
  Daniel Migault
- IKEv2 Count Based SA Extension –
  Daniel Migault
- **IPsec Multi SA –**
  Paul Wouters

Charter Update and Status

- Items finished (given to IESG):
  - PPK – RFC8784
  - Implicit IV – RFC8750
  - Post Quantum – RFC 9242 + Multiple ke
  - RFC8229bis
  - TFC + Yang + Mib for it
- Items still in charter:
  - G-doi
  - Constrained ESP
  - Signature algorithm negotiation
  - Security Labels

Charter Other Items

- Work items not in charter, but agreed as WG items:
  - ADD – IKEv2 config for Encrypted DNS
  - IKEv1 to historic
- Items not in charter, but being worked on:
  - draft-pwouters-ipsecme-multi-sa-performance
  - draft-liu-ipsecme-mtu-detect
  - draft-liu-ipsecme-ikev2-rekey-redundant-sas
- Old items, nothing happening lately:
  - draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt
  - draft-mglt-ipsecme-diet-esp
  - draft-smyslov-ipsecme-ikev2-cookie-revised
  - draft-tjhai-ikev2-beyond-64k-limit

Open Discussion

- Other points of interest?