IP Security Maintenance and Extensions (IPsecME) WG

IETF 112, Monday, November 8th, 2021

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Benjamin Kaduk

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: https://meetings.conf.meetecho.com/ietf112/?group=ipsecme&short=&item=1

Notes: https://codimd.ietf.org/notes-ietf-112-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (12:00-12:05)
- Document Status – Chairs (10 min) (12:05-12:15)
- Work items
  - IPTFS – Christian Hopps (20 min) (12:15-12:35)
  - Quantum-resistent IKEv2 and big keys – Stefan-Lukas Gazdag (10 min) (12:35-12:45)
  - Group Key Management using IKEv2 – Valery Smyslov (10 min) (12:45-12:55)
  - Announcing Supported Authentication Methods in IKEv2 – Valery Smyslov (10 min) (12:55-13:05)
- AOB + Open Mic (55 min) (13:05-14:00)

WG Status Report

Publication requested:

- draft-ietf-ipsecme-ikev2-intermediate

Waiting for write-up / Chair review:

- draft-hopps-ipsecme-iptfs
- draft-fedyk-ipsecme-yang-iptfs
- draft-ietf-ipsecme-mib-iptfs
- draft-ietf-ipsecme-ikev2-multiple-ke
- draft-ietf-ipsecme-ikev1-algo-to-historic
- draft-ietf-ipsecme-labeled-ipsec

Work in progress:

- draft-ietf-ipsecme-g-ikev2
- draft-ietf-ipsecme-rfc8229bis

More detailed status of drafts in progress

- Group Key Management using IKEv2
  - draft-ietf-ipsecme-g-ikev2
  - Need more reviews
- Announcing Supported Authentication Methods in IKEv2
  - draft-smyslov-ipsecme-ikev2-auth-announce
  - Should be ready for WG adoption call
- TCP Encapsulation of IKE and IPsec Packets
  - draft-ietf-ipsecme-rfc8229bis
  - Ready for WGLC?

Presentations

- **IPTFS –**
  Christian Hopps
- Quantum-resistent IKEv2 and big keys –
  Stefan-Lukas Gazdag
- Group Key Management using IKEv2 –
  Valery Smyslov
- Announcing Supported Authentication Methods in IKEv2 –
  Valery Smyslov

Presentations

- IPTFS –
  Christian Hopps
- **Quantum-resistent IKEv2 and big keys –
  Stefan-Lukas Gazdag**
- Group Key Management using IKEv2 –
  Valery Smyslov
- Announcing Supported Authentication Methods in IKEv2 –
  Valery Smyslov

Presentations

- IPTFS –
  Christian Hopps
- Quantum-resistent IKEv2 and big keys –
  Stefan-Lukas Gazdag
- **Group Key Management using IKEv2 –
  Valery Smyslov**
- Announcing Supported Authentication Methods in IKEv2 –
  Valery Smyslov

Presentations

- IPTFS –
  Christian Hopps
- Quantum-resistent IKEv2 and big keys –
  Stefan-Lukas Gazdag
- Group Key Management using IKEv2 –
  Valery Smyslov
- **Announcing Supported Authentication Methods in IKEv2 –**
  Valery Smyslov

Open Discussion

- Other points of interest?