IP Security Maintenance and Extensions (IPsecME) WG

IETF 111, Monday, July 26th, 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/ietf111/?group=ipsecme&short=&item=1

Notes: https://codimd.ietf.org/notes-ietf-111-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (21:30-21:35)
- Document Status – Chairs (5 min) (21:35-21:40)
- Work items
  - Hybrid IKEv2 Interoperability Testing – Valery Smyslov (5 min) (21:40-21:45)
  - Improvements for Post-Quantum IKEv2 – Daniel Herzinger (5 min) (21:45-21:50)
  - Management of IPTFS (Yang and SNMP drafts) – Christian Hopps (10 min) (21:50-22:00)
- New items
  - IKEv2 Configuration for Encrypted DNS – Valery Smyslov (10 min) (22:00-22:10)
  - Beyond 64kB limit of IKEv2 Payloads – Valery Smyslov (10 min) (22:10-22:20)
  - IKEv2 Optional SA & TS Payloads in Child Exchange – William Panwei (5 min) (22:20-22:25)
  - IKEv2 Support for Per-Queue Child SAs – Paul Wouters (5 min) (22:25:22:30)
- AOB + Open Mic (0 min) (22:30-22:30)

WG Status Report

Waiting for write-up / Chair review:

- draft-ietf-ipsecme-ikev2-intermediate
- draft-hopps-ipsecme-iptfs

In WGLC:

- draft-ietf-ipsecme-ikev1-algo-to-historic

Work in progress:

- draft-ietf-ipsecme-g-ikev2
- draft-ietf-ipsecme-ikev2-multiple-ke
- draft-ietf-ipsecme-labeled-ipsec
- draft-smyslov-ipsecme-rfc8229bis
- draft-fedyk-ipsecme-yang-iptfs
- draft-ietf-ipsecme-mib-iptfs

Presentations

- **Hybrid IKEv2 Interoperability Testing – Valery Smyslov**
- Improvements for post-quantum IKEv2 – Daniel Herzinger
- Management of IPTFS (Yang and SNMP draft) – Christian Hopps
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov
- Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei
- IKEv2 support for per-queue Child SAs – Paul Wouters

Presentations

- Hybrid IKEv2 Interoperability Testing – Valery Smyslov
- **Improvements for post-quantum IKEv2 – Daniel Herzinger**
- Management of IPTFS (Yang and SNMP draft) – Christian Hopps
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov
- Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei
- IKEv2 support for per-queue Child SAs – Paul Wouters

Presentations

- Hybrid IKEv2 Interoperability Testing – Valery Smyslov
- Improvements for post-quantum IKEv2 – Daniel Herzinger
- **Management of IPTFS (Yang and SNMP draft) – Christian Hopps**
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov
- Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei
- IKEv2 support for per-queue Child SAs – Paul Wouters

Presentations

- Hybrid IKEv2 Interoperability Testing – Valery Smyslov
- Improvements for post-quantum IKEv2 – Daniel Herzinger
- Management of IPTFS (Yang and SNMP draft) – Christian Hopps
- **Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov**
- Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei
- IKEv2 support for per-queue Child SAs – Paul Wouters

Presentations

- Hybrid IKEv2 Interoperability Testing – Valery Smyslov
- Improvements for post-quantum IKEv2 – Daniel Herzinger
- Management of IPTFS (Yang and SNMP draft) – Christian Hopps
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov
- **Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov**
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei
- IKEv2 support for per-queue Child SAs – Paul Wouters

Presentations

- Hybrid IKEv2 Interoperability Testing – Valery Smyslov
- Improvements for post-quantum IKEv2 – Daniel Herzinger
- Management of IPTFS (Yang and SNMP draft) – Christian Hopps
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov
- Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov
- **IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei**
- IKEv2 support for per-queue Child SAs – Paul Wouters

Presentations

- Hybrid IKEv2 Interoperability Testing – Valery Smyslov
- Improvements for post-quantum IKEv2 – Daniel Herzinger
- Management of IPTFS (Yang and SNMP draft) – Christian Hopps
- Internet Key Exchange Protocol Version 2 (IKEv2) Configuration for Encrypted DNS – Valery Smyslov
- Beyond 64KB Limit of IKEv2 Payloads – Valery Smyslov
- IKEv2 Optional SA&TS Payloads in Child Exchange – William Panwei
- **IKEv2 support for per-queue Child SAs – Paul Wouters**

Open Discussion

- Other points of interest?