IP Security Maintenance and Extensions (IPsecME) WG

IETF 106, Thursday, November 21, 2019

Chairs: David Waltermire
Tero Kivinen

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: http://www.meetecho.com/ietf106/ipsecme

Etherpad:

https://etherpad.ietf.org/p/notes-ietf-106-ipsecme

NOKIA
AMS

Agenda

- Agenda bashing, Logistics – Chairs (5 min) (15:50-15:55)
- Draft Status – Chairs (10 min) (15:55-16:05)
- Work items
  - Hybrid QSKE Interop –
    Valery Smyslov (5 min) (16:05-16:10)
  - IP Traffic Flow Security –
    Christian Hopps (10 min) (16:10-16:20)
  - Labeled IPsec TS support for IKEv2 –
    Paul Wouters (10 min) (16:20-16:30)
- Other presentations
  - Optional SA & TS Payloads in Child Exchange –
    Wei Pan (10 min) (16:30-16:40)
  - IKEv1 graveyard –
    Paul Wouters (5 min) (16:40-16:45)
  - An Alternative Approach for Postquantum Preshared keys –
    Valery Smyslov (15 min) (16:45-17:00)
  - Multiple Sas in one create child SA exchange –
    Daniel Migault (10 min) (17:00-17:10)

WG Status Report

Published as RFC:

- draft-ietf-ipsecme-split-dns published as RFC8598

In RFC Editor queue:

- draft-ietf-ipsecme-implicit-iv

Publication requested:

- draft-ietf-ipsecme-qr-ikev2

WGLC done:

- draft-ietf-ipsecme-ipv6-ipv4-codes

Work in progress:

- draft-ietf-ipsecme-ikev2-intermediate
- draft-ietf-ipsecme-labeled-ipsec

Adopted as WG draft:

- draft-hopps-ipsecme-iptfs
- draft-tjhai-ipsecme-hybrid-qske-ikev2
- draft-yeung-g-ikev2

Work items

- Work items
  - Hybrid QSKE Interop – Valery Smyslov
    - draft-tjhai-ipsecme-hybrid-qske-ikev2
  - IP Traffic Flow Security – Christian Hopps
    - draft-hopps-ipsecme-iptfs
  - Labeled IPsec TS support for IKEv2 – Paul Wouters
    - draft-ietf-ipsecme-labeled-ipsec
- Other presentations
  - Optional SA & TS Payloads in Child Exchange – Wei Pan
    - draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt
  - IKEv1 graveyard – Paul Wouters
    - draft-pwouters-ikev1-ipsec-graveyard
  - An Alternative Approach for Postquantum Preshared Keys in IKEv2 – Valery Smyslov
    - draft-smyslov-ipsecme-ikev2-qr-alt
  - Multiple Sas in one create child SA exchange – Daniel Migault
    - draft-mglt-ipsecme-multiple-child-sas (not yet posted)

Open Discussion

- Other points of interest?