IP Security Maintenance and Extensions (IPsecME) WG

IETF 105

Tuesday, 23 July 2019 at 1520

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:

- Two note takers
- One jabber scribe

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

MeetEcho: http://www.meetecho.com/ietf105/ipsecme

Etherpad: https://etherpad.ietf.org/p/notes-ietf-105-ipsecme

Agenda

1. **Agenda bashing, Logistics** – Chairs (15:20-15:25)
2. **WG Status Report** (15:25-15:35)
3. **Work Items**
   - Intermediate Exchange in the IKEv2 Protocol -- Valery Smyslov (15:35-15:40)
     draft-ietf-ipsecme-ikev2-intermediate
   - Labeled IPsec Traffic Selector support for IKEv2 -- Paul Wouters (15:40-15:45)
     draft-ietf-ipsecme-labeled-ipsec
   - Group Key Management using IKEv2 -- Valery Smyslov (15:45-16:00)
     draft-yeung-g-ikev2
4. **Other Presentations**
   - Framework to Integrate Post-quantum Key Exchanges into IKEv2 -- Valery Smyslov (16:00-16:10)
     draft-tjhai-ipsecme-hybrid-qske-ikev2
   - IP Traffic Flow Security -- Christian Hopps (16:10-16:20)
     draft-hopps-ipsecme-iptfs
   - IKEv2 Optional SA&TS Payloads in Child Exchange -- Wei Pan/Sandeep Kampati (16:20-16:35)
     draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt

WG Status Report

Publication requested:

- Implicit IV for Counter-based Ciphers in Encapsulating Security Payload (draft-ietf-ipsecme-implicit-iv)
- Postquantum Preshared Keys for IKEv2 (draft-ietf-ipsecme-qr-ikev2)

Work in Progress:

- IKEv2 Notification Status Types for IPv4/IPv6 Coexitence (draft-ietf-ipsecme-ipv6-ipv4-codes)

Milestones Status

Date	Milestone
May 2019	Postquantum cryptography document for IKEv2 to IESG
Mar 2019	Signature algorithm negotiation for IKEv2 to IESG
Jan 2019	The security labels support for IKEv2 to IESG
Dec 2018	G-DOI for IKEv2 to IESG
Dec 2018	The ESP on contrained network to IESG
Oct 2018	The internal address failure indication in IKEv2 to IESG
Done	IETF Last Call on partially quantum resistant IKEv2 draft-ietf-ipsecme-qr-ikev2
Done	IETF Last Call on Implicit IV in IPsec draft-ietf-ipsecme-implicit-iv
Done	IETF Last Call on Split-DNS Configuration for IKEv2 draft-ietf-ipsecme-split-dns