IP Security Maintenance and Extensions (IPsecME) WG

IETF 121, Monday, November 4th, 2024

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Deb Cooley

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

MeetEcho: https://meetecho.ietf.org/client/?group=ipsecme

Notes: https://notes.ietf.org/notes-ietf-121-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (09:30-09:35)
- Document Status – Chairs (10 min) (09:35-09:45)
- Presentations
  - Anti replay notification – Wei Pan (15 min) (09:45-10:00)
  - Enhanced Encapsulated Security Payload – Steffen Klassert (15 min) (10:00-10:15)
  - Sha-3 – Ben Salter (10 min) (10:15-10:25)
  - FrodoKEM in IKEv2 – Wang Guilin (10 min) (10:25-10:35)
  - Beet mode – Antony Antony (5 min) (10:35-10:40)
  - Encrypted ESP Ping – Antony Antony (10 min) (10:40-10:50)
  - PQC Auth – Tirumal Reddy (10 min) (10:50-11:00)
  - PQT Hybrid Auth – Jun Hu (10 min) (11:00-11:10)
  - Lightweight auth for IP header – Linda Dunbar (10 min) (11:10-11:20)
- AOB + Open Mic (10 min) (11:20-11:30)

WG Status Report

- Published as RFCs
  - Nothing since last meeting

WG Status Report

- Waiting for write-up / AD Followup (shepherd review done):
  - draft-ietf-ipsecme-g-ikev2
- WG LC done?
  - draft-smyslov-ipsecme-ikev2-qr-alt
    - Only comments on list were from me, does not really seem to have that much interest on this?
- Ready for WG LC?
  - draft-mglt-ipsecme-ikev2-diet-esp-extension (expired)
  - draft-mglt-ipsecme-diet-esp
- Work in progress:
  - draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

• **Anti replay notification**	**Wei Pan**
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

- Anti replay notification — Wei Pan
- **Enhanced Encapsulated Security Payload — Steffen Klassert**
- Sha-3 — Ben Salter
- FrodoKEM in IKEv2 — Wang Guilin
- Beet mode — Antony Antony
- Encrypted ESP Ping — Antony Antony
- PQC Auth — Tirumal Reddy
- PQT Hybrid Auth — Jun Hu
- Lightweight auth for IP header — Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• **Sha-3**	**Ben Salter**
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• **FrodoKEM in IKEv2**	**Wang Guilin**
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• **Beet mode**	**Antony Antony**
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• **Encrypted ESP Ping**	**Antony Antony**
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• **PQC Auth**	**Tirumal Reddy**
• PQT Hybrid Auth	Jun Hu
• Lightweight auth for IP header	Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• **PQT Hybrid Auth**	**Jun Hu**
• Lightweight auth for IP header	Linda Dunbar

Presentations

• Anti replay notification	Wei Pan
• Enhanced Encapsulated Security Payload	Steffen Klassert
• Sha-3	Ben Salter
• FrodoKEM in IKEv2	Wang Guilin
• Beet mode	Antony Antony
• Encrypted ESP Ping	Antony Antony
• PQC Auth	Tirumal Reddy
• PQT Hybrid Auth	Jun Hu
• **Lightweight auth for IP header**	**Linda Dunbar**

Open Discussion

- Other points of interest?