IP Security Maintenance and Extensions (IPsecME) WG

IETF 125, Thursday, March 19th, 2026

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Deb Cooley

Note Well

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies. For a linked version of this text, please visit *www.ietf.org/note-well* or use the QR code below.

- IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see *RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy*). If you have any concerns about behavior, please contact the *Ombudsteam* who have a duty of confidentiality and extensive powers to act, as set out in *RFC 7776: IETF Anti-Harassment Procedures*.
- If you are aware that any IETF contribution (as defined in *RFC 5378: Rights Contributors Provide to the IETF Trust*) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see *RFC 8179: Intellectual Property Rights in IETF Technology*).
- For detailed process information consult *RFC 2026: Internet Standards Process* and *RFC 2418: IETF Working Group Guidelines and Procedures* and updates to those.
- The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the *IETF Privacy Statement*.

For advice, please talk to Working Group chairs or Area Directors.

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-125-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (2 min) (11:30-11:32)
- Document Status – Chairs (3 min) (11:32-11:35)
- Presentations
  - Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM – Wang Guilin (9 min) (11:35-11:44)
  - KEM Auth in IKEv2 – Valery Smyslov (9 min) (11:44-11:53)
  - Fragmenting large messages – Valery Smyslov (9 min) (11:53-12:02)
  - PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2 – Tirumal Reddy (9 min) (12:02-12:11)
  - ESP in UDP for Load-Balancing – Tiger Xu (9 min) (12:11-12:20)
  - Multi-Path Secret Sharing for QKD Key Relay – Jinming Li (5 min) (12:20-12:25)
  - Multi-Authentication in IKEv2 with Post-quantum Security – Wang Guilin (5 min) (12:25-12:30)
- AOB + Open Mic (0 min) (12:30-12:30)

WG Status Report

- Published as RFCs
  - Renaming the Extended Sequence Numbers (ESN) Transform Type in the Internet Key Exchange Protocol Version 2 (IKEv2) as RFC9827
  - Group Key Management Using the Internet Key Exchange Protocol Version 2 (IKEv2) as RFC9838
  - Mixing Preshared Keys in the IKE_INTERMEDIATE and CREATE_CHILD_SA Exchanges of the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-Quantum Security as RFC9867
- In RFC Editor AUTH48 queue:
  - Nothing now
- Publication requested:
  - Nothing now.

WG Status Report

- Waiting for write-up / AD Followup (shepherd review done):
  - draft-ietf-ipsecme-ikev2-pqc-auth
  - draft-ietf-ipsecme-ikev2-mlkem
- WG LC done
  - draft-ietf-ipsecme-ikev2-downgrade-prevention
  - draft-ietf-ipsecme-ikev2-diet-esp-extension
  - draft-ietf-ipsecme-diet-esp
    - Waiting for the draft-mglt-ipsecme-dscp-np, proposing to make that experimental and then do WG adoption, and WGLC and then send all three out.
- Ready for WG LC
  - None now. Most likely after this meeting some are…

WG Status Report

- Work in progress:
  - draft-ietf-ipsecme-hybrid-kem-ikev2-frodo
  - draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
  - draft-ietf-ipsecme-ikev2-reliable-transport
  - draft-ietf-ipsecme-ikev2-beet-mode
  - draft-ietf-ipsecme-eesp
  - draft-ietf-ipsecme-eesp-ikev2
  - draft-ietf-ipsecme-esp-ping / draft-ietf-ipsecme-encrypted-esp-ping
  - draft-ietf-ipsecme-ikev2-prf-plus
  - draft-salter-ipsecme-sha3
  - draft-pwouters-ipsecme-child-pfs-info
- In WG Adoption calls:
  - Nothing now

Presentations

• Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM	Wang Guilin
• KEM Auth in IKEv2	Valery Smyslov
• Fragmenting large messages	Valery Smyslov
• PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2	Tirumal Reddy
• ESP in UDP for Load-Balancing	Tiger Xu
• Multi-Path Secret Sharing for QKD Key Relay	Jinming Li
• Multi-Authentication in IKEv2 with Post-quantum Security	Wang Guilin

Presentations

• **Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM**	**Wang Guilin**
• KEM Auth in IKEv2	Valery Smyslov
• Fragmenting large messages	Valery Smyslov
• PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2	Tirumal Reddy
• ESP in UDP for Load-Balancing	Tiger Xu
• Multi-Path Secret Sharing for QKD Key Relay	Jinming Li
• Multi-Authentication in IKEv2 with Post-quantum Security	Wang Guilin

Presentations

• Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM	Wang Guilin
• **KEM Auth in IKEv2**	**Valery Smyslov**
• Fragmenting large messages	Valery Smyslov
• PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2	Tirumal Reddy
• ESP in UDP for Load-Balancing	Tiger Xu
• Multi-Path Secret Sharing for QKD Key Relay	Jinming Li
• Multi-Authentication in IKEv2 with Post-quantum Security	Wang Guilin

Presentations

- Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM — Wang Guilin
- KEM Auth in IKEv2 — Valery Smyslov
- **Fragmenting large messages** — **Valery Smyslov**
- PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2 — Tirumal Reddy
- ESP in UDP for Load-Balancing — Tiger Xu
- Multi-Path Secret Sharing for QKD Key Relay — Jinming Li
- Multi-Authentication in IKEv2 with Post-quantum Security — Wang Guilin

Presentations

- Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM — Wang Guilin
- KEM Auth in IKEv2 — Valery Smyslov
- Fragmenting large messages — Valery Smyslov
- **PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2 — Tirumal Reddy**
- ESP in UDP for Load-Balancing — Tiger Xu
- Multi-Path Secret Sharing for QKD Key Relay — Jinming Li
- Multi-Authentication in IKEv2 with Post-quantum Security — Wang Guilin

Presentations

- Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM — Wang Guilin
- KEM Auth in IKEv2 — Valery Smyslov
- Fragmenting large messages — Valery Smyslov
- PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2 — Tirumal Reddy
- **ESP in UDP for Load-Balancing** — **Tiger Xu**
- Multi-Path Secret Sharing for QKD Key Relay — Jinming Li
- Multi-Authentication in IKEv2 with Post-quantum Security — Wang Guilin

Presentations

• Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM	Wang Guilin
• KEM Auth in IKEv2	Valery Smyslov
• Fragmenting large messages	Valery Smyslov
• PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2	Tirumal Reddy
• ESP in UDP for Load-Balancing	Tiger Xu
• **Multi-Path Secret Sharing for QKD Key Relay**	**Jinming Li**
• Multi-Authentication in IKEv2 with Post-quantum Security	Wang Guilin

Presentations

• Post-quantum Hybrid Key Exchange in IKEv2 with FrodoKEM	Wang Guilin
• KEM Auth in IKEv2	Valery Smyslov
• Fragmenting large messages	Valery Smyslov
• PQ/T Hybrid Composite Key Exchange and Reliable Transport for IKEv2	Tirumal Reddy
• ESP in UDP for Load-Balancing	Tiger Xu
• Multi-Path Secret Sharing for QKD Key Relay	Jinming Li
• **Multi-Authentication in IKEv2 with Post-quantum Security**	**Wang Guilin**

Open Discussion

- Other points of interest?