

IP Security Maintenance and Extensions (IPsecME) WG

IETF 118, Thursday, November 9th, 2023

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Roman Danyliw

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://meetings.conf.meetecho.com/ietf118/?group=ipsecme&short=&item=1>

Notes: <https://notes.ietf.org/notes-ietf-118-ipsecme>

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (5 min) (13:00-13:05)
- Document Status – Chairs (5 min) (15:05-13:10)
- Adoption calls – Chairs (5 min) (13:10-13:15)
- Presentations
 - Issues with DH with IKEv2 and rekeys – Paul Wouters (15 min) (13:15-13:30)
 - Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov (10 min) (13:30-13:40)
 - Update of multiple sequence counters – Steffen Klassert (10 min) (13:40-13:50)
 - Anti-replay sequence number subspaces – Pierre Pfister (10 min) (13:50-14:00)
 - Beet mode – Antony Antony (5 min) (14:00-14:10)
 - ESP trailer adjustment – Wei Pan (5 min) (14:10-14:15)
 - Delete info – Paul Wouters (5 min) (14:15-14:20)
 - RISAV Update – Yangfei Gui (5 min) (14:20-14:25)
- AOB + Open Mic (5 min) (14:25-14:30)

WG Status Report

- Published as RFCs
 - Labeled IPsec Traffic Selector Support for the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC9478](#)
- RFF Editor queue:
 - [draft-ietf-ipsecme-add-ike](#)
- Publication requested:
 - [draft-ietf-ipsecme-ikev2-auth-announce](#)

WG Status Report

- Waiting for write-up / AD Followup:
 - [draft-ietf-ipsecme-g-ikev2](#)
- Working Group Last Call:
 - [draft-ietf-ipsecme-multi-sa-performance](#)
- Work in progress:
 - [draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt](#)

WG Adoption calls

- draft-liu-ipsecme-ikev2-mtu-dect
- draft-mglt-ipsecme-dscp-np
- draft-mglt-ipsecme-diet-esp
- draft-mglt-ipsecme-ikev2-diet-esp-extension
- draft-smyslov-ipsecme-ikev2-cookie-revised

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- **Issues with DH with IKEv2 and rekeys – Paul Wouters**
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- **Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov**
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- **Update of multiple sequence counters – Steffen Klassert**
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- **Anti-replay sequence number subspaces – Pierre Pfister**
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- **Beet mode – Antony Antony**
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- **ESP trailer adjustment – Wei Pan**
- Delete info – Paul Wouters
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- **Delete info – Paul Wouters**
- RISAV Update – Yangfei Gui

Presentations

- Issues with DH with IKEv2 and rekeys – Paul Wouters
- Alternative Approach for Mixing PPKs in IKEv2 – Valery Smyslov
- Update of multiple sequence counters – Steffen Klassert
- Anti-replay sequence number subspaces – Pierre Pfister
- Beet mode – Antony Antony
- ESP trailer adjustment – Wei Pan
- Delete info – Paul Wouters
- **RISAV Update – Yangfei Gui**

Open Discussion

- Other points of interest?