LAMPS

Limited Additional Mechanisms for PKIX and S/MIME

IETF 121

Tuesday, 5 November 2024 at 13:00 local

Wednesday, 6 November 2024 at 15:00 local

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)

Living the IETF Code of Conduct

A brief reminder of key points from RFC 7154:

- IETF participants extend respect and courtesy to their colleagues at all times.
- IETF participants have impersonal discussions.
- IETF participants devise solutions for the global Internet that meet the needs of diverse technical and operational environments.
- Individuals are prepared to contribute to the ongoing work of the group.

LAMPS WG Agenda (1 of 7)

0) Minute Taker, Jabber Scribe, Bluesheets

1) Agenda Bash

2) Recently Published RFCs

a) draft-ietf-lamps-ocsp-nonce-update (RFC 9654)

b) draft-ietf-lamps-x509-policy-graph (RFC 9618)

c) draft-ietf-lamps-cms-kemri (RFC 9629)

LAMPS WG Agenda (2 of 7)

3) RFC Editor

a) draft-ietf-lamps-e2e-mail-guidance (DKG)

b) draft-ietf-lamps-rfc5990bis (Russ)

c) draft-ietf-lamps-cms-sha3-hash (Russ)

d) draft-ietf-lamps-cms-cek-hkdf-sha256 (Russ)

e) draft-ietf-lamps-rfc8708bis (Russ)

f) draft-ietf-lamps-rfc5019bis (Tadahiko)

LAMPS WG Agenda (3 of 7)

4) With IESG

a) draft-ietf-lamps-cert-binding-for-multi-auth (Alie, Rebecca, Mike)

b) draft-ietf-lamps-header-protection (DKG, Alexey, Bernie)

c) draft-ietf-lamps-im-keyusage (Rohan)

d) draft-ietf-lamps-x509-shbs (Kaveh, Scott, Stefan-Lukas, Daniel, Stavros)

e) draft-ietf-lamps-rfc4210bis (Hendrik, David O, Mike, John)

f) draft-ietf-lamps-rfc6712bis (Hendrik, David O, Mike, John)

g) draft-ietf-lamps-rfc7030-csrattrs (Michael)

LAMPS WG Agenda (4 of 7)

5) Active PKIX-related Documents

a) draft-ietf-lamps-dilithium-certificates (Jake, Panos, Sean, Bas)

b) draft-ietf-lamps-kyber-certificates (Sean, Panos, Jake, Bas)

c) draft-ietf-lamps-csr-attestation (Mike)

d) draft-ietf-lamps-x509-slhdsa (Kaveh, Scott, Stefan-Lukas, Daniel, Stavros)

e) draft-ietf-lamps-attestation-freshness (Hannes, Hendrik)

f) draft-ietf-lamps-pq-composite-sigs (Mike, John, Max, Jan, Scott)

g) draft-ietf-lamps-rfc{5272,5273,5274}bis (Joseph, Sean)

h) draft-ietf-lamps-rfc9579bis (Alicja)

i) draft-ietf-lamps-cms-ml-dsa (Ben, Adam, Daniel)

LAMPS WG Agenda (5 of 7)

6) Active S/MIME-related Documents

a) draft-ietf-lamps-cms-kyber (Ludovic, Julien, Mike)

b) draft-ietf-lamps-cms-sphincs-plus (Russ, Scott, Panos, Bas)

c) draft-ietf-lamps-pq-composite-kem (Mike, John)

LAMPS WG Agenda (6 of 7)

7) Special Topic: EUF-CMA for CMS SignedData

LAMPS WG Agenda (7 of 7)

7) Under consideration for adoption

a) draft-wang-lamps-root-ca-cert-rekeying (Guilin)

b) draft-harvey-cfrg-mtl-mode (John)

c) draft-lamps-okubu-certdiscovery (John)

d) draft-lamps-bonnell-keyusage-crl-validation (Corey)

e) draft-brockhaus-lamps-automation-keyusages (Hendrik)

f) draft-davidben-x509-alg-none (David)

g) draft-sun-lamps-hybrid-scheme (Shuzhou)

8) Wrap up