LAMPS

Limited Additional Mechanisms for PKIX and S/MIME

IETF 118

Monday, 6 November 2023 at 17:30 - 18:30 CET

Wednesday, 8 November 2023 at 14:30 - 16:30 CET

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 5)

0) Minute Taker, Jabber Scribe, Bluesheets

1) Agenda Bash

2) Recently Published RFCs

a) draft-ietf-lamps-caa-issuemail published as RFC 9495

b) draft-ietf-lamps-cmp-algorithms published as RFC 9481

c) draft-ietf-lamps-cmp-updates published as RFC 9480

d) draft-ietf-lamps-lightweight-cmp-profile as RFC 9483

3) With the RFC Editor or the IESG

a) draft-ietf-lamps-cms-kemri (Russ, John, Tomo)

b) draft-ietf-lamps-nf-eku (Tirumal, Jani, Daniel)

LAMPS WG Agenda (3 of 5)

4) **Active PKIX-related Documents**
   a) draft-ietf-lamps-rfc4210bis (Hendrik, David H, Mike, John)
   b) draft-ietf-lamps-rfc6712bis (Hendrik, David H, Mike, John)
   c) draft-ietf-lamps-pkcs12-pbmac1 (Hubert)
   d) draft-ietf-lamps-rfc7030-csrattrs (Michael)
   e) draft-ietf-lamps-dilithium-certificates (Jake, Panos, Sean, Bas)
   f) draft-ietf-lamps-kyber-certificates (Sean, Panos, Jake, Bas)
   g) draft-ietf-lamps-cert-binding-for-multi-auth (Alie, Rebecca, Mike)
   h) draft-ietf-lamps-x509-policy-graph (David B)
   i) draft-ietf-lamps-csr-attestation (Mike)
   j) draft-ietf-lamps-rfc5019bis (Corey)

LAMPS WG Agenda (2 of 5)

5) **Special Topic**
   a) AEAD-to-CBC Downgrade Attacks on CMS (Falko)
   b) an alternative mitigation for the above issue (Russ)

LAMPS WG Agenda (4 of 5)

6) Active S/MIME-related Documents

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

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

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

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

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

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

g) draft-ietf-lamps-rfc8398bis/-rfc8399bis (Alexey, Wei, Corey)

LAMPS WG Agenda (5 of 5)

7) **Under consideration for adoption**
   a) draft-mpalmer-key-compromise-attestation (Matt)
   b) CMC-bis: draft-mandel-lamps-rfc5272bis/-rfc5273bis/-rfc5274bis (Sean)
   c) draft-housley-lamps-cms-sha3-hash (Russ)
   d) draft-gazdag-x509-hash-sigs (Stefan)
   e) draft-tschofenig-lamps-nonce-cmp-est (Hendrik)
   f) draft-ounsworth-pq-composite-sigs (John)
   g) draft-ounsworth-lamps-cms-dhkem (Mike)
   h) draft-ounsworth-lamps-pq-external-pubkeys (David H)
   i) draft-lamps-okubo-certdiscovery (Tomofumi)
8) **Wrap up**