LAMPS at IETF 113

Administrivia

- Chairs: Russ Housley and Tim Hollebeek
- Minute Taker: Deb Cooley
- Review the NOTE WELL
- Agenda Bash: Agenda is too full, will go as far as we can. Rene dropped his request to talk, he will bring it directly to the mailing list.

2) With the IESG or the RFC Editor

a) draft-ietf-lamps-cmp-updates (Hendrik, David)

- Hendrik Brockhaus listed the changes since IETF 112, which address things raised during the AD Review.
- CMP update vs. RFC4210bis: Roman Danyliw says that it does not need a bis document; however, the reason for an update (as opposed to a bis document) needs to be explained. Russ explained that the update was originally expected to be more modest. Tero Kivinen says that it is easier for a developer when the specification is all in one document, and Tero asked that a single specification be produced before advancing CMP to Internet Standard. Michael Richardson (MCR) said it would be nice to have a more concise document by removing anything that is not used, but of course, that would be a bis document; however, it is not worth delaying this work for years. Tero points out that that a bis document can advance to Internet Standard without further changes, but the update document would need to be merged to advance the CMP specification. Conclusion was to continue with the update document, and if the WG wants to make it an Internet Standards in the future, then a bis will be written.
- /.well-known: Ben Kaduk was concerned that the current use of .well-known is not allowing future updates to delegate to new protocol features. There was some confusion about whether it was a protocol label or a profile label. Four options were explored:

  1. Keep alignment with EST;
  2. Use a query element;
  3. Move the profile label; or
  4. Give up using .well-known URIs altogether.

  Conclusion was a combination of 1 and 3, with a profile label.

b) draft-ietf-lamps-cmp-algorithms (Hendrik, Hans, Mike, John)

- Hendrik listed the changes since IETF 112. He updated the algorithms based on suggestion from NIST.

c) draft-ietf-lamps-lightweight-cmp-profile (Hendrik, Steffen, David)

- Hendrik listed the changes, and the things yet to be done. Need to make the .well-known changes and some clarifications.

d) draft-ietf-lamps-samples (DKG)

- Daniel Kahn Gillmor (DKG) said that the document is in AUTH48. There are a couple of questions and clarifications, but the document should be published soon.

3) Active PKIX-related Documents

a) draft-ietf-lamps-documentsigning-eku (Tadahiko, Tomofumi, Sean)

- The -02 draft was published in early March, some review was done, changes in the works to address the current WG Last Call comments. WG Last Call ends next week.

b) draft-ietf-lamps-rfc3709bis (Stefan, Russ, Trevor, Leonard)

- In WG Last Call. The goal was to make the RFC future proof by stating that the hash used to sign the certificate will also be used for integrity protection of the logotype. Please review before WG Last Call ends next week.

c) draft-ietf-lamps-8410-ku-clarifications (Sean, Simon, Daniel, Tadahiko)

- Sean Turner said that this Internet-Draft was recently upgraded to a WG document; it clarifies which key usage flags can be set with the CFRG curves (X25519 and x448). DKG asked Sean to compare with the certificates in the samples Internet-Draft. Sean agreed to do so. Sean asking for WG Last Call. Russ would like to issue the WG Last Call when the previous two have completed.

4) Active S/MIME-related Documents

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

- DKG said that good progress has been made.
- Wrapped message: looks like a forwarded message.
- Injected headers: obscure header fields were invisible, the fix doesn't work everywhere (i.e., in Outlook). However, putting the protected headers in a slightly different location appears to work.
- The authors recommend a MUST do Injected headers, and MAY do Wrapped Message.
- The design team has been meeting every two weeks, and they would like to expand the design team to include an implementer, especially from a major MUA.
- The ask: The authors have test vectors that they would like to test on other MUAs, to include mailing lists,

and so on.
- Question: hcp_minimal or hcp_strong: minimal protects only the subject, and strong protects all of the headers. The design team favors minimal as the mandatory-to-implement.
- Question: The Legacy Display elements injected or not? Deciding what to signal, ways to signal, or how to do that.
- Question: Automated Mail Systems (e.g., RT): does Legacy Display Elements interfer with command processing?
- Question: Is the injected message easy enough for clients to insert?
- Question: How should message headers be displayed to indicate that they are encrypted? what is a match?
- Discussion of Questions: MCR asks for clarification, about subject line changes. There is no way to tell if the outer subject line is different than the encrypted subject line. Aaron asked if it could be made easier for a machine to make the decisions. Tero asked about how these obscured subject lines will be handled (reply, forward, etc), and that the rules will have to be extremely strict. Alexey agreed that the rules will have to be strict and the proposal in the draft seems a good way forward. Tero said that we can reach more people by presenting it at https://www.m3aawg.org/ (which is scheduled to meet in June 2022 in London).

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

- DKG reported that the was one update since the last meeting. DKG is reaching out to different developers about e2e guidance about how they work today.

5) Under consideration for adoption

a) draft-richardson-lamps-rfc7030-csrattrs (Michael)

- MCR said that the issue is that EST (RFC 7030) doesn't specify CSR attributes. So, a EST client can query the EST server for the details on what will be accepted for algorithms, names, etc.
- Option A: The ACP usage by adding a new CHOICE to allow adding. Sean suggested that the example in RFC7030 is just incorrect, and he does not think that the additional CHOICE is needed, and he pointed back to RFC 8295
- Option B: Create a new encoding to address name/keyspec needs. Sean spoke against Option B.
- Conclusion: Design team will review the existing ASN.1 structure to see if is meets all of the use cases.

b) draft-uni-qsckeys (Christine, Silvio, Basil, Tamas, Michael, Dieter, Joppe)

- Michael Osborne pointed out that NIST has not looked at how private keys are serialized as part of the PQC competition. There is an implicit structure (strength, versions, compression). There are many varients, especially when a hybrid schemes are added. Algorithm IDs currently point to implicit private key format.
- MCR asked whether this presentation was about public keys or private keys. Response: Private keys. This is about storage, and moving the keys in and out of the encryption engine.
- Thom Wiggers observed that compression of private keys often changes the algorithm. Specifically, in

Rainbow's CZ parametersets keygen is different. In other cases, it often is not a matter of compressing, but possibly more deterministic key regeneration (compression for storage).
- DKG asked why there is not just an upgrade path to handle larger key sizes. Response: seeking smoothest path to providing a quantum safe computing solution. The goal is to move the largest number of applications quickly and securely. The proposal the key formats that are needed to do so.
- DKG asked if they have looked at stateful signature schemes. Response: no; it is a scope issue.
- Scott Fluhrer contributed that for stateful signature private keys would be much more work. Too much for this draft.
- Julian Prat stated that there are many compression schemes. How will they all be managed? Response: To get a smaller private key structure, the implementation needs to compute intermediate values. To get minimal computation, the intermediate values need to be included in the structure, so it is bigger.

c) draft-turner-lamps-nist-pqc-kem-certificates (Sean, Panos, Jake, Bas)

- Sean says that the goal for this document is a RFC5480-like specification about how to put PQC keys into certificates.
- Currently, it is the format for the public keys from NIST, OIDs assigned by NIST, with no parameters. One public key, one certificate.
- Sean is asking for WG adoption.
- Panos observes that KEMs and signatures are different, and he recommends putting them in seperate drafts.

--- out of time ---

d) draft-perret-prat-lamps-cms-pq-kem (Ludovic, Julien, Mike)

- Postponed.

e) Hybrid Composite Certificates (Mike, Max, John, Serge)

```
    --  draft-ounsworth-pq-composite-encryption
    --  draft-ounsworth-pq-composite-keys
    --  draft-ounsworth-pq-composite-sigs
    --  draft-ounsworth-pq-explicit-composite-keys
```

- Postponed.

f) draft-struik-lamps-verification-friendly-ecdsa (Rene)

- Postponed.

6) Wrap up

Russ: We will schedule a virtual interim to continue the discussion.