Minutes for LAMPS WG Agenda at Virtual IETF 111

WG Chairs: Russ Housley and Tim Hollebeek.

Thanks to Jonathan Hammell for taking notes during the first session.

Thanks to Deb Cooley for taking notes during the second session.

FIRST SESSION -- Monday, 26 July 2021

CMP Updates

(draft-ietf-lamps-cmp-updates)

The changes since IETF 110 listed. All IETF 110 issues and subsequent issues from the LAMPS mailing list discussions addressed.

Remaining issues to address include the feedback from Sean (errata on RFC 4210), comments from Russ, comments from Lijun, and ASN.1 modules feedback from Russ. Once these are done, the authors think that the I-D will be ready for WG Last Call. This should happen before IETF 112.

CMP Algorithms

(draft-ietf-lamps-cmp-algorithms)

The changes since IETF 110 listed. John Gray added as author. All IETF 110 issues and subsequent issues from the LAMPS mailing list discussions addressed.

Only formatting nits remain to be addressed. Once these are done, the authors think that the I-D will be ready for WG Last Call. This should happen before IETF 112.

Russ: Does this document need to be advanced in lock-step with CMP Updates?

Hendrik Brockhaus: I don't think so.

Lightweight CMP Profile

(draft-ietf-lamps-lightweight-cmp-profile)

The changes since IETF 110 listed. All IETF 110 issues and subsequent issues from the LAMPS mailing list discussions addressed.

An issue with the polling mechanism was discovered during an internal review. It needs to be extended to message types other than certificate requests because it is not always feasible for asynchronous transport for delayed delivery for all message types. The proposal is to respond with error message to come back later to get the response. No feedback on the proposal was provided by the WG, so text with this approach will be added to the document.

Remaining issues to address include the addition of a section on use with BRSKI and SZTP, change delayed enrollment to delayed delivery, and add additional security considerations. Once these are done, the authors think that the document will be ready for WG Last Call. This should happen before IETF 112.

Russ: Does this sequence for the WG Last Calls make sense:
CMP Algorithms, then CMP Updates, then Lightweight CMP Profile.

Hendrik: Yes, I think so.

General Purpose Extended Key Usage for Document Signing X.509 Certificates

(draft-ito-documentsigning-eku)

The Extended Key Usage (EKU) certificate extension is common practice, but no public, general EKU asigned for Document Signing certificates. If an existing EKU were used for document signing, unexpected behaviours are possible. The proposal to define general document signing EKU to identify certificates indended to be used for validating signatures over document contents. Document contents are ones to be consumed by humans. The EKU object identifier is to be assigned by IANA.

Eliot Lear: Have the authors had talked to CAs about their willingness to implement.

Sean Turner: A post on CA/B Forum mailing list seemed to be supportive. Tadahiko Ito said that his CA is interested. Tomofumi Okubo said that his CA has clients want something other than the id-kp-emailProtection EKUs because the policies around that EKU are not appropriate for document signing.

Several people expresses support and willing ness to review the document, including Russ, Eliot, Joe Salowey, and Rich Salz. It was pointed out that Ryan Sleevi posted a lot of tutorial information about the Key Usage (KU) certificate extension position was as well as the EKU certificate extension, but it was not clear (to Russ) whether Ryan was supportive or not.

The WG Chairs will issue a call for adoption.

Update to RFC 7299

(draft-ietf-lamps-rfc7299-update)

RFC 7299 puts all of the PKIX OIDs into IANA registry; however, discussion of the CMP Updates document lead to the discovery that two OIDs that were assigned in RFC 4212 were missed. This I-D just adds those missing OIDs.

Rich: Suggest moving directly to WG Last Call.

Tim: We are going to try that.

SECOND SESSION -- Thursday, 29 July 2021

Discussion of the EST CSRATTRS for SubjectAltName was dropped from the agenda due to a schedule conflict.

Header Protection

(draft-ietf-lamps-header-protection)

Several revisions since IETF 110. There are now 40 test vectors, including unprotected messages, signed messages, signed+encrypted messages, replies these messages. Certificates are valid for decades, which should be long enough for our purposes. Considering adding tampered messages.

Authors ask WG participants to try these test these on your preferred client, and then send the screenshots. So far, no one has sent screenshots for a mobile client. The screenshots will let the authors build a list of issues and recommend a path forward.

There are many complex problems: people use multiple MUAs, people still use legacy MUAs, etc. There is a taxonomy of concerns in the document.

Authors ask WG participants to review the list. Did we miss issues?

Examples from Outlook 365 (see https://datatracker.ietf.org/meeting/111/materials/slides-111-lamps-sessb-header-protection-01).

Hernani Marques: Outlook is beyond repair. Apple mail.app, in the wrapped case, the email has a better display.

Jonathan Hammell: Volunteered to look at the screen shots, and asked whether the user agent was configured by default to encrypt?

Bernie Hoeneisen: I think it was set to encrypt by default.

Daniel Kahn Gillmor: In Apple mail.app, the default reply appears to be signed only, which of course, leaks everything.

Authors ask WG participants whether a design team should be formed to help recommend the best compromise. The authors were asked to start a thread on the mailing list to see who would be interested in serving on such a design team.

Samples

(draft-ietf-lamps-samples)

Samples are based on two chains: one RSA, one 25519. Samples also include cross-certificates and end entity certificates. There are been some issues importing the PKCS#12 objects into Apple products. The authors are looking for information on the source of the problem and how to fix it. Apparently, if one imports into Thunderbird and then exports it again, the Apple products will accept them. Once the PKCS#12 issue is resolved, the document will be ready for WG Last Call.

End-to-End Mail Guidance

(draft-dkg-lamps-e2e-mail-guidance)

This is a newly adopted document. The author is looking for comments and welcomes contributions from others. Also, the author seeks opinions about whether to include test vectors, example renderings of UI elements, or implementer checklists.

Tadahiko Ito (in jabber): Are there were display limits?

Alexey Melnikov: IMAP (IMAP4rev1, RFC 3501) has a 4 GB limit. IMAP4rev2 (about to be published as an RFC) has a limit of 63bits.