LAMPS WG Agenda at Virtual IETF 110

draft-ietf-lamps-cms-aes-gmac-alg and draft-ietf-lamps-crmf-update-algs

Slides: https://datatracker.ietf.org/meeting/110/materials/slides-110-lamps-draft-ietf-lamps-cms-aes-gmac-alg-and-draft-ietf-lamps-crmf-update-algs-01

These documents are with the IESG and the RFC Editor. No discussion.

draft-ietf-lamps-header-protection

Slides: https://datatracker.ietf.org/meeting/110/materials/slides-110-lamps-header-protection-00

Daniel Kahn Gilmor (a.k.a. DKG) gave the presentation.

Slide 15:

Bernie Hoeneisen: Can you click the attachment and reply to the message?

DKG: No, the Injected Headers message doesn't even show an attachment.

Bernie: The difference is that Wrapped there is a double header?

DKG: There are three differences: the double header, the .eml attachment, and broken signature.

Bernie: If you clicked the attachment would it work?

DKG: Never tried it.

Deb Cooley: You are seeing the contents of the attachment on the left.

DKG: Yes, clicking might put you in a different view, but did not occur to me to try.

Russ: The broken signature can be important.

DKG: Yes. I do not know why it appear broken. If anyone can help with that...

Alexey: I managed to generate signatures that verify in Thunderbird.

DKG: Will appreciate help with that.

Russ: I think that Alexey is offering to compare the result from his client to Thunderbird, which should tell us if the problem is with the test message or a bug in Thunderbird.

Bernie: I believe we need more than just text in the examples. We should explore multipart alternative and attachment in the same message. It may lead to different paths. Hope I'm wrong.

DKG: Three structures: text/plain+text/html ; text/plain+attachment ; multipart+attachment. Do people feel we need so many test vectors?

Alexey (on jabber): Multipart/mixed is enough.

Bernie: Multipart/alternative + attachment. Can do more complicated as an option.

DKG: Who would be up to testing a dozen messages with a MUA that hasn't been tested yet?

[Several people volunteered, including Alexey and Tim.]

DKG: The current set of messages messages are here: https://header-protection.cmrg.net/

DKG: Would people object to a large appendix with the messages.

Roman: I do not object.

Russ: several people speaking for adoption of draft-dkg-lamps-samples, none against. Will do an official call on the mail list.

CMP Algorithms, CMP Updates, and Lightweight CMP Profile

Slides: https://datatracker.ietf.org/meeting/110/materials/slides-110-lamps-lightweight-cmp-profile-updates-cmp-and-cmp-algorithms-00

Hendrik Brockhaus gave the presentation.

Slide 6:

Hendrik: If you use another key, does this make the entity an RA? What is the reason it’s in CMC?

Russ: The EKU is also used in EST and BRSKI.

Deb Cooley: You are reusing the entity. Is it signing the certificate or is it acting as RA?

Hendrik: Able to use a different key on a different machine.

Deb: So does the delegated entity sign the certificate?

Hendrik: No. What we need to know is whether we need the CA to sign or an RA would be enough.

Deb: We use RAs all the time. Not sure about CMP.

Hendrik: No real RA action needed here. This just passes along the signed certificate.

Deb: RA does nto have to be in the delivery path.

draft-dkg-lamps-e2e-mail-guidance

Daniel Kahn Gilmor (a.k.a. DKG) spoke without slides.

Plan is to send the proposed charter and run an adoption call in parallel.

Verification-Friendly ECDSA

Slides: https://datatracker.ietf.org/meeting/110/materials/slides-110-lamps-verification-friendly-ecdsa-00

René Struik gave the presentation.

Scott Fluhrer: Does Certicom have a patent for this idea?

René: IPR issues are now gone for the signing side and batch verification, and other IPR will expire within four years.

Scott: Just wanted the group to be informed that there might be an issue.

Slide 10:

Dmitry Belyavskiy: Will there be speed-ups with co-factor not equal to 1?

René: Like in GOST scheme? I think not for batch, but it will for single verification.

Dmitry: Can you confirm that ECDSA* are verifiable by an ECDSA validator?

René: Correct, with optional extension. That is essential for transition. People have the option to ignore speed-ups.

Russ: The patent issue may be a problem. Will discuss on the mail list and see what people think. If people are not concerned, then we can do a call for adoption. Will start the discussion with Mike Ounsworth's comment from the jabber regarding the effort to improve ECC performance when starting to think abot a transition to post-quantum.