LAMPS WG at IETF 115 -- Wed., 9 Nov 2022 at 9:30 GMT

Minute Taker, Jabber Scribe, Bluesheets, Agenda Bash

With the IESG or the RFC Editor

draft-ietf-lamps-documentsigning-eku (Sean)

No status update.

draft-ietf-lamps-cmp-algorithms (Hendrik)

Nothing new to report, one minor fix in AUTH48.

draft-ietf-lamps-cmp-updates and draft-ietf-lamps-lightweight-cmp-profile (Hendrik)

Some improvement to Appendix C is necessary. An old ASN.1 definition was in use (the RFC2511 definition was used instead of RFC 4211). This change will be made during AUTH48 with AD approval.

draft-ietf-lamps-rfc3709bis (Russ)

No updates to share.

draft-ietf-lamps-5g-nftypes (Russ)

No update to share.

Roman wanted confirmation that no more coordination is required with 3GPP; there is none.

Active PKIX-related Documents

draft-ietf-lamps-rfc4210bis and draft-ietf-lamps-rfc6712bis (Hendrik)

These I-Ds were prepared as requested by the IESG.

Draft -00 of 4210bis is the original text, updated for current XML format.

Draft -01 merged in content from CMP updates. Subsequent updates are detailed in slides.

Regarding support for KEM keys, the authors will wait for a new I-D that addresses proof of possession for KEM keys. An indirect mechanism is already available. MAC-based message protection was discussed. Ladder diagram in slides.

Mike Ounsworth noted that waiting on KEM support was agreed last time, but the current status seems to be different.

Russ Housley noted that we ended up in this situation because the IESG requested bis documents for CMP. The KEM mechanism is still being discussed on the mailing list.

Sean Turner asked whether other mechanisms might be defined as well.

Mike Ounsworth noted that Panos would likely advocate for HPKE.

Russ Housley advises proceeding with current mechanism, and then add other mechanism later if they gain consensus.

Regarding rfc6712bis, similar approach to versions as for 4210bis. Change summary in slides. Document is quite stable.

Sean Turner notes rfc8446bis is in flight, so references should be adjusted.

draft-ietf-lamps-pkcs12-pbmac1 (Hubert)

Skipped.

draft-ietf-lamps-rfc7030-csrattrs (Michael provided a report by email)

Still bugs in examples, so Michael Richardson knows there is work to do. Expects to be finished by end of November 2022. He would like assistance from co-authors to update the examples.

draft-ietf-lamps-dilithium-certificates (Jake)

Carl Wallace asks whether the OCTET STRING tag/length should be dropped or kept? The I-D currently defines the OCTET STRING, and then it is not used. Why not encode directly into the BIT STRING in SubjectPublicKeyInfo?

Mike Ounsworth observes that there was also a proposal to include the seed of public key instead of the full public key, is this still on the table?

Jake Massimo: Yes.

Russ Housley points out that Some structures are proposed in draft-uni-qsckeys-dilithium-00.

John Gray pointed out that there are many use cases where a pre-hash of data is needed to sign large data to conserve bandwidth. Instead of a 32 byte hash, a Dilithium signature requires the full message, which could be megabytes. This could break existing infrastructure. If this problem needs to be solved outside the Dilithium document, is a different group going to look at this problem, perhaps CFRG?

Jonathan Hammell suggests using direct encoding, instead of wrapping a structure in OCTET STRING.

draft-ietf-lamps-kyber-certificates (Sean)

I-D was recently adopted by working group. Several TODOs in the slides, but waiting on NIST for OIDs. Similar issue regarding private key format as discussed for dilithium.

draft-ietf-lamps-key-attestation-ext (Carl)

No update.

Active S/MIME-related Documents

draft-ietf-lamps-header-protection (Alexey)

No update. Editors will try to get together next week to work on an update.

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

Update released recently. Include guidance around email attacks described in feedback. Several TODOs remain. Would like more review. Not ready for WGLC.

draft-ietf-lamps-kyber (Julian)

Change summary in slides. Using KeyTransRecipientInfo to communicate algorithm information. Algorithms to be used listed in slides. Depends on PQC certificate work, needs some new OIDs to be defined. Open question regarding algorithm limitations.

Markku Kojo suggests adopting 256 bits (192 is not used by TLS, suggest dropping).

John Gray asked if RecipientInfo decision received sufficient discussion and whether KeyTransRecipientInfo is best choice.

Russ Housley and Mike Ounsworth offered clarification.

Quynh Dang agrees about dropping 192 bits. Suggests keeping Kyber768.

Sean Turner agrees that less is more. Suggest minimal set of choices.

draft-ietf-lamps-cms-sphincs-plus (Russ)

I-D is a placeholder. Nothing to discuss at right now.

Under consideration for adoption

draft-becker-guthrie-cert-binding-for-multi-auth (Mike)

Some objections were based on perceiving document to apply more broadly than intended. Other objections based on incomplete understanding as document was being worked. The extension is not meant to be an alternative to composite. Extension can provide linkage between two independently issued certificates (e.g., as U.S. DoD is planning to transition away from tradition certificates to strictly-PQC certificates). I-D aims to address transition challenges.

Mike Ounsworth raises two questions. First, there is already an other certificates mechanism.

Mike Jenkins observes that mechanism leaves certificate requests out of scope.

Mike Ounsworth thinks it is reasonable for a CA to issue two certificates that are bound; likewise for an RA. He objects to extending the CSR mechanism due to issues of validating certificates from other CAs or infrastructures.

Mike Jenkins sees where this could be an issue.

Tim Hollebeek notes that in a public CA case, the CSR with certificate from other organization could just be rejected. Should a separate (and more generically applicable) I-D be written about information in CSRs from other CAs and how to handle such information?

Sean Turner asks if any checks are done beyond path validation?

Mike Jenkins answers "no", CAs do other checks as well. The CSR mechanism will establish the binding.

Tim Hollebeek notes that in order to support this I-D a CA would need to check that bound certificates are controlled by the same entity.

Russ Housley asked if subject or SAN must be the same?

Tim Hollebeek notes this may not hold across organizations, but mandating that the certificates be issued by the same organization could be reasonable.

Rob Lee asks what details apply. It could require the same certificate policy. The language will need to be careful to ensure the document accurately represents what the certificate binding guarantees.

Russ Housley asked Mike Jenkins to send a summary to the mailing list.

draft-ounsworth-pq-composite-keys and draft-ounsworth-pq-composite-sigs (Max)

Max provided an overview (see slides), and then a description of a notional "algorithm X" that is very much different from currently contemplated algorithms. A brief overview of a related K-of-N draft was provided. Recent annoucement regarding ISARA's patents on hybrid certificates was provided.

John Gray provided hackathon results.

Max Pala asked for working group adoption of composite key document; however, K-of-N is not ready for adoption yet. Asked if discussion related to hackathon should occur on LAMPS mailing list?

Sean Turner notes that "letting a thousand flowers bloom" may not be the best path forward, will slow down deployments.

Bas Westerbaan agreed Sean. He added that he thinks we may not see sigature composites at all.

Markku Kojo notes that composites should go forward. He is not supportive of the ISARA approach.

Carl Wallace echoed suggestion in slides about discussing generic composite vs explicit composite. Several implementations of generic composite were developed during hackathon and achieved interoperation.

Max Pala notes that generic composite with restrictions is still problematic regarding implementations that do not honor the restrictions.

Someone notes that can be addressed via checking OIDs as with today.

Daniel Kahn Gillmor notes that generic construction need not be expressed in certificate itself, as each implementor will need to decide which combinations to support. He thinks this is a recipe for interoperation pain and favors explicit composite.

John Gray notes generic and explicit can coexist. Pleasing everyone with explicit composite may be difficult.

Aron Wussler notes leaving unrestricted will result in weird combinations.

Max Pala suggests this is no different than configuring supported algorithms today.

John Gray notes there is a composite KEM I-D that needs review too (possibly from CFRG).

Russ Housley suggests a discussion about generic vs. explicit on the mailing list, then a call for adoption.

draft-gazdag-x509-hash-sigs (Stefan)

No slides. I-D was recently published, and it addresses demand for stateful and stateless using hash-based signature algorithms with X.509. Document aims to provide unified nomenclature.

Russ Housley notes that the signature mechanism for HSS/LMS should be same as defined for CMS (RFC 8708).

Wrap up

Out of time.