LAMPS virtual interim on 13 September 2021 at 14:00 UTC

Minutes based on notes from John Gray.

The virtual interim was focused on Post Quantum Cryptography (PQC) in PKIX certificates and CMS.

Slides

https://datatracker.ietf.org/meeting/interim-2021-lamps-03/materials/slides-interim-2021-lamps-03-sessa-chair-slides-00

https://datatracker.ietf.org/meeting/interim-2021-lamps-03/materials/slides-interim-2021-lamps-03-sessa-lamps-pqc-discussion-00

PQC KEM algorithms in CMS and PKIX

The LAMPS charter says NIST-approved or CFRG-approved Algorithms must be the basis of this work. We know that NIST is planning to announce winners in their PQC competition at the end of this year. No algorithms have been submitted to the CFRG for vetting, so there will not be additional algorithms from the CFRG by the end of the year.

Should LAMPS define a new CMS recipient info for KEMs (KEMRecipientInfo)? The alternative is to define conventions for using KEMs with KeyAgreeRecipientInfo or KeyTransRecipientInfo.

Defining a new PKIX certificate keyUsage will be hard. One possibility is to combine the keyUsage with a new extended key usage (EKU) to indicate that a KEM is being used. It was pointed out that when RSA-KEM was specified, KeyTransRecipientInfo was used.

- Ludovic Perret: NIST is going to define standards beginning of next year, then it will take 1-2 years for the specification to be published.
- Scott Fluhrer: If FALCON is chosen, different parameter sets may be used.
- Russ Housley: Yes, there may be tweaks to the parameters. We need to account for the possibility of parameter changes in the final stages.
- Yoav Nir: Our process takes 1-2 years, so the possiblity of parameter change is not a bar for adopting an Internet-Draft.
- Uri Blumenthal: Why is this a concern? We will use whatever NIST blesses by end of January. It will be a KEM with a very fixed interface. An OID can identify the algorithm plus parameter set. There will be a separate definition of how to implement a PQC KEM algorithm. Why should it be more complicated than this?
- Tim Hollebeek: Some parameter changes may influence performance, size, and other things. However

there should be plenty of time to adapt.

- Uri: We do not need to take performance into account, whatever NIST decides, we will use as specified. If decoding a CMS message takes longer or shorter, that is fact of life. We should not change the parameters.
- Tim: Suspect parameters will not have a big impact, but we should keep an eye on it.
- Russ: We could investigate the same approach as RSA-KEM and see if it fits with the NIST candidates. If it fits, then propose that for adoption.
- Russ: Later in the meeting, we will ask for volunteers to author documents.

Hybrid Key Establishment

We want to allow more than one key establishment algorithm to be used at the same time. Have recently completed a draft-ounsworth-pq-composite-encryption.

- Russ: This is an example of a way forward. I think there are some choices. We need to get to an Internet-Draft that the whole working group likes, then ask CFRG to look at it.
- Ludovic: Philosophy of different drafts? (It will discussed laterin this meeting if time allows.)
- Russ: We can start the discussion on the list and come to agreement. Having an Internet-Draft is a good way to start the discussion. Alternative is to adopt the draft and completely re-work it. We should get feedback before moving forward.
- Uri: Hybrid is only useful for one use-case. I personally believe it is an overkill that adds very little usefulness.
- Ludovic: Certification of protocol products require a hybrid mode to obtain certification. With key exchange there are groups that are dealing with the issue. The IPsecME WG is dealing with the topic as well. Would be good to synchronize.
- Russ: I think there is going to be a fair amount of time in transition. People will need time to get familiar with the new algorithms and their implementations. Hybrid offers a way to mix a classic algorithm with PQC to provide a safety net. The cost to do classic algorithm in addition to a PQC algorithm is pretty small increase.
- Uri: Not so small, extra code requires extra validation.
- Mike Ounsworth: RSA had a long time to mature, PQC algorithms will likely need time to work out implementation CVE's. Within context of CMS, hybrid key exchange is different than other standards.

PQC signatures

- Russ: Work is much simpler. We don't have a recipient info decisions for signatures. Just use the OIDs that NIST assigns, and then write down the conventions for use of parameters. This should not be time consuming. We could draft it now, just insert the algorithm names and OIDs when NIST publishes the specifications. We should wait on this one for NIST.

Dual signatures

There are two approaches. Need to kick off a mail list discussion of the pros and cons of the two approaches. Should we use separate certificates for the classic algorithm and the PQC algorithm? One certificate or two, still end up with multiple signatures in CMS.

Action for Mike Ounsworth: Post a description of the differences between composite OR and composite AND to the mailing list.

- Serge Mister: Question on extension marks use in ASN.1. It is not compatible with RFC 5280? Would it be the intent to pick up the newer extensions when the need arises.
- Sean Turner: We might look at the X.509 extension marks, but we have not made a commitment to include all of them. Will have to check if it impacts interoperability.

Design Choices

Mike Ounsworth went over the design choices. We have "generic composite". What you would expect if you were creating software for flexibility. Do you require users to use ALL the keys (composite AND) or only some of the keys (Composite OR).

- Eliot Lear: Question on AND or OR mode. Does anyone have advice when to use which mode?
- Mike: For closed PKI's more likely the OR mode would be more useful.
- John Gray: The OR mode can be used for migration from one algorithm (classic algorithm) to another one (PQC algorithm). I prefer AND mode as it is more secure and simpler to implement correctly.
- Serge: Explicit composite is much more rigid (see slide 12). It defines in ASN.1 combination of algorithms. Generic is more flexible, but more can go wrong. For explicit, who is going to define the pairs? Is there going to be a master list somewhere?
- Russ: Concern with Explicit composite. In PKIX, algorithms were specified, but none of them were mandtory-to-implement. That decision was left to the applications that used certificates. Likewise in CMS, different algorithms were specified, but none were mandatory-to-implement. That was left to applications, like S/MIME. Choosing the explicit pairs seems to be making these types of choices. Why do you think the LAMPS group is the right group to do it?
- Serge: We can define the way to combine them together without selecting the pairs. We can leave pair selection to be chosen by application.
- Uri: Question on whether pairing in LAMPs is different than specifying a container format. Explicit has enough value to move forward. It may be useful for other things as well. Might want to specify a KEM paired with a signature, and so on.
- Roman: This seems like an important design decision. This should move to the list.

Final discussion was about slide 15, whether all 3 methods were needed. Some discussion on whether one could be used (option 3), and if the first 2 were actually needed.

Volunteers

- Russ: Do we have any volunteers for KEM and hybrid?

- Sean: for KEM for PKIX certificates.
- Ludovic: I will volunteer, but I am not sure which document yet.