LAMPS at IETF 112

Administrivia

Chairs: Russ Housley and Tim Hollebeek

Minute Taker: Deb Cooley

Review the NOTE WELL and IETF Code of Conduct

Agenda Bash: None

With the RFC Editor or the IESG

a) draft-ietf-lamps-rfc7299-update [RFC Ed] (Russ)

Puts two OIDs in the IANA registries, but no further actions.

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

Fixed minor formatting nits, then WG Last Call in October 2021.

AD review led to updates to Section 7, which is deprecating algorithms in RFC 4210 Appendix D.2, like MD5, SHA-1, DSA, RC5, CAST-128, 3DES, and X9.9 MAC. (PBMAC1 is not deprecated.)

A summary of the algorithms providing comparable security is needed in Section 7. The authors proposed two different version of algorithm tables, and the verdict was to let the authors pick the version that renders the best.

c) draft-ietf-lamps-samples [IESG] (DKG)

There has been a review by the ADs, and the document is moving forward. The document is in IETF Last Call.

Active CMP-related Documents

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

Intense review resulted in good comments, and the authors fixed many of them.

In the document, polling has been expanded to include some non-enrollment messages, updated version handling, fixed some ASN.1.

Left to do: register two OIDs for CRL update retrieval.

The authors suggested reordering some existing OIDs, but concerns were raised about changes that would impact the OIDs that were already allocated by IANA.

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

References to SZTP-CSR and BRSKI-AE were added, removed the 'rootCACert' from general info and added it to the 'genm' body, simplified the handing of nonces for delayed delivery, updated the security considerations, moving some of the earlier text to draft-ietf-lamps-cmp-updates. Added general info messages for CRL updates.

Left to do: update based on AD feedback to draft-ietf-lamps-cmp-algorithms.

Russ asked if there is a reason to not to WG Last Call. There was no response.

Russ asked about the order of submission - Hendrik said draft-ietf-lamps-cmp-updates should be next, but then said that they should all go together so that comment resolution can keep them in sync.

Active S/MIME-related Documents

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

This document has been stalled. There are multiple options and unclear how to choose. All proposals work for new clients; the sticking point is how legacy clients handle the proposals. The assumption is that legacy clients will not be updated to better handle this proposal. There was discussion and speculation about whether we can incentivize clients to make updates. There was general agreement to ignore the encryption case because to encrypt to a client needs some prior knowledge. So the decision should focus on how legacy clients handle signed-only messages.

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

There is little to report, but some fixes in the draft. Please review this draft.

Under consideration for adoption (PKIX-related)

a) draft-ito-documentsigning-eku (Sean)

There is a new version of this document as of last night. The authors have made changes due to comments on the mailing list, including clarified the scope of document signing, added a section for how to use the public key/certificate, and addressed concerns about the extended key usage as a policy identifier, and added to the security considerations. Sean asked for working group adoption. The WG chairs will take that call for adoption to the mailing list.

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

CSR attributes was unclear in RFC 7030. As a result, both BRSKI and ACP made assumptions, but there were issues with the ASN.1. One proposal is that there would be a new attribute. If that is done, then it can be extensible. Sean suggested that there could be several new attributes to avoid jamming values into incorrect attributes. The question is how to get it all written in ASN.1.

Russ asked the authors to up a proposed solution in the Internet-Draft. Michael agreed to do so.

John Gray agrees with GeneralName (not GenericName as shown in the slides).

c) NIST PQC KEM public keys in certificates (Sean)

The document will describe how to put NIST PQC KEM public keys into X.509 certificates once NIST announces the winning algorithms. He followed the format from the CURDLE WG for key agreement with X25519 and X448. Alternatively, we could follow the NIST OIDs that identified both the algorithm and the parameters.

Russ asked whether the document was using 'keyAgreement' or 'keyTransport', which lead to discussion about how KEMs fit into the current structure. Sean agreed to research that topic, update the document, and then request a call for adoption.

d) Hybrid Non-composite Multi-certificate (Alison, Rebecca, Daphanie)

The presentation offers PQC migration goals with a focus on cryptographic algorithm agility, which requires some discussion of hybrid design. NSA defines 'hybrid' as a framework for backwards and forward compatibility during the transition from traditional public key algorithms to PQC algorithms, which also considers performance and latency. NSA anticipates that hybrid will be used to maintain interoperability during the transition to PQC-only algorithms. There are two alternative:

- Composite design - where traditional and PQ algorithms function together as one entity.
- Non-composite design - where traditional and PQ algorithms function discretely.

The non-composite approach would employ two seperate certificates. The composite approach would employ a single certificate with two public keys. A list of pros and cons for both options was presented.

DKG: The analysis seems to be focused on authentication. How would it change for key exchange?

Joe Saloway: Key agreement would be different than authentication.

Mike Ounsworth: Good work. Concerned about the offline use cases like code signing and document signing, where the initiator cannot learn the capabilities of the recipient through a protocol exchange.

Tero: IPsec is just doing key agreement currently. Classic algorithms will be used to protect the PQC exchange, and then the classic shared secret and the PQC shared secret will be combined. In the future, IPsec might use pre-shared keys to protect the PQC exchange.

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

Quick status of the Internet-Drafts (almost out of time):

- The keys document - they may drop the composite-keys and stick with the explicit composite keys document.

- The sigs document - no work in a while, pretty mature, could be made explicit. If the working group decides on multiple certificates to validate a single signature, then there might need to be a container. Russ commented that CMS allows multipli signatures and the bag-of-certificates can carry as many certificates as desired. Russ pointed to RFC 5752 for guidance on using multiple signatures.
- The encryption document - there is more work to do regarding the differences between key transport algorithms and KEMs.

There are several possibilities for fitting KEMs into CMS (no draft yet). One approach is to generalize RSA KEM (see RFC 5990), but the parameters may not fit properly. Russ observes that the OIDs could include the parameters for the KEM, then the fit is better. A second option is to use OtherRecipientInfo. A third option is to use a new top-level KEMRecipientInfo, which is not backward compatible. The authors will take this decision to the mailing list.

Wrap up

Out of time.