

COMPOSITES

IETF 117 – LAMPS

Mike Ounsworth, John Gray

Max Pala, Jan Klaussner



ENTRUST

SECURING A WORLD IN MOTION

RESULTS OF CALL-FOR-ADOPTION

- ▶ Here are our take-aways from the call-for-adoption:
 - ▶ There are concerns that composite-signatures is not the right design approach.
 - ▶ There are fewer concerns about composite-KEMs.
 - ▶ The document needs some editing, but has been adopted.

COMPOSITE SIGS

SUMMARY OF CORE OBJECTIONS

1. *“There still need to be some serious conversations about exactly what we are trying to achieve, and exactly how it is supposed to work.” - Tim*

The working group has not reached consensus on whether there is a legitimate problem to be solved.

2. Is Strong Non-Separability a needed property?
Consider “non-separable” or “true hybrid” variants from Bindel, Hale 2023 [1] or draft-nir-lamps-altcompsigs-00.
3. There seems to be some carryover objections from previous versions in reference to OR Modes; so we consider these objections to be moot.

1: “A note on Hybrid Signature Schemes” <https://eprint.iacr.org/2023/423.pdf>

2: <https://datatracker.ietf.org/doc/draft-nir-lamps-altcompsigs/>

WORK FOR COMPOSITE-KEMS

We're happy to move composite KEMs forward even if composite-sigs do not.

Edits we need to do:

- Make draft-composite-kems standalone by folding in the minimum necessary content from composite-keys and dropping the reference to composite-sigs.
- Re-work wire format and ASN.1 to remove vestiges of Generics.
- Make RSA keys fixed-length.
- Compress the public key format by not carrying redundant algID OIDs.
- Re-work section 4.1 (id-Kyber768-RSA-KMAC256) to
 - Reference 5990bis and its updated structures.
 - Remove RSA-KEM KDF params and make them implied by the OID; ie provide a profile of 5990bis.
- The ASN.1 module file include is broken in the published version (but correct on github).
- We need PEM samples ... during the 117 hackathon?
- Move this into github.com/lamps-wg
- Publish "DH-KEM for CMS" draft (dependency for this draft)

WORK FOR COMPOSITE-SIGS

- ❑ Intro: clarify the driving usecase(s) for AND-mode hybrid sigs.
- ❑ Compressing the signature format by removing redundant OIDs.
- ❑ Remove all parameters
 - ❑ RSA key size
 - ❑ RSA-PSS params
- ❑ Clear statements about revocation and algorithm deprecation.

We believed this was already covered in -keys “7.3 Policy for Deprecated and Acceptable Algorithms” and “7.5 Checking for Compromised Key Reuse”, but perhaps we need to revisit this text.