HPKE

draft-irtf-cfrg-hpke

Barnes, Bhargavan, Lipp, Wood — IETF 111 — CFRG

Registry Conflicts

Resolving registry concerns

IANA maintains a registry for AEAD algorithms:

https://www.iana.org/assignments/aead-parameters/aead-parameters.xhtml

HPKE defines a *new* registry for AEAD algorithms:

https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hpke#section-7.3

HPKE requires the registry to specify `Nk` (key) and `Nn` (nonce) lengths

HPKE's analysis requires each AEAD be IND-CCA2 secure

Moving Forward

Resolving registry concerns

Options:

1. Continue using the HPKE-defined AEAD registry
2. Switch to the existing registry, and request that `Nk`/`Nn` columns be added
   Note: this is a breaking change

Considerations:

- Not all AEADs in the existing registry are suitable for HPKE — 64-bit AEAD tags have < 128 bits of security, etc.
- Would the existing registry need any *more* columns particular to HPKE?