HPKE

draft-irtf-cfrg-hpke
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:


HPKE requires the registry to specify $N_k$ (key) and $N_n$ (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 $N_k/N_n$ 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?