draft-irtf-cfrg-dnhpke

A MODEST PROPOSAL FOR HPKE

Dan Harkins, HPE
IETF 117, July 2023
ISSUES WITH HPKE (RFC 9180)

- **HPKE has some bloat**—Serialization of key is > twice as big as it needs to be
  - **Problem for:**
    - Constrained devices and networks
    - One-shot HPKE usage with small messages where message is dwarfed by overhead

- **HPKE assumes guaranteed in order delivery of packets**
  - **Problem because:**
    - Any packet loss would put HPKE contexts out of sync, impossible to debug or resync
    - Lossy networks that could use a security toolbox with HPKE in it

- **Key wrapping is not really the point of HPKE, but...**
  - It's a valid and obvious use case though
  - Good to have a purpose-built key wrapping algorithm in HPKE

* For KEMs using P-256, P-384, and P-521
DRAFT ADDS THE FOLLOWING...

- **Compact representation of public keys (RFC 6090)**
  - New KEMs for NIST curves with compact (de)serialization

- **Deterministic Authenticated Encryption (RFC 5297)**
  - Provable security treatment for key wrapping
  - Addresses lossy networks for certain types of traffic

- **RFC 2401-style anti-replay window**
  - Addresses lossy networks for traffic that can’t use DAE
Internet-Draft:

Source code:
https://github.com/danharkins/hpke-wrap

- Compliant with RFC 9180
- Supports compact representation with new KEM values*
- Supports deterministic authenticated encryption ciphers*
- Complete test vectors

* Took the liberty of stealing some values reserved to IANA for test vector generation
OK, what now?

• Draft is stable, code is very stable
• Currently -01 but it was based on an -02 so…
• Not a lot of discussion/comments on list

Maybe an RGLC?

It would be nice to point to an RFC for this stuff when proposing the use of HPKE in some protocols….