draft-barnes-cfrg-hpke

Richard Barnes, Cisco
Karthik Bhargavan, Inria

Why?

Lots of use cases for “encrypt to a public key”: MLS, ESNI, 5G, nacl/box, etc.

Older [EC]IES standards use old primitives, lack test vectors, don’t address common usage patterns, etc.

Objectives:

- Agility w.r.t. primitives (in particular, quantum-safe primitives)
- Formal verification
- Cover common use cases

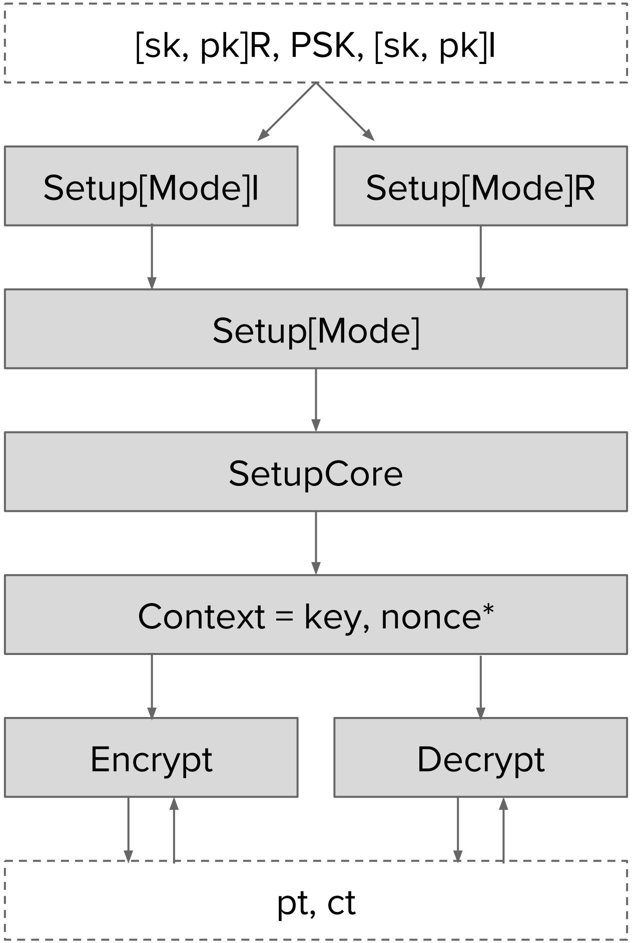
What?

Composition of (KEM, AEAD) to obtain PKE

General composition with three different modes:

1. Base: “Encrypt to this public key”
2. PSK: “Encrypt to this public key, and authenticate possession of a PSK”
3. Auth: “Encrypt to this public key, and authenticate possession of a private key”

A given encapsulated key can be used for multiple AEAD encryptions



Past and Future

2019-01-19 - draft-barnes-cfrg-hpke-00

- First effort, DH-only, one mode / one-shot
- List discussion positive, multiple suggestions of using KEM

2019-03-11 - draft-barnes-cfrg-hpke-01

- Converts to KEM
- PSK / auth modes, “streaming” encryption

2019-XX-XX - Call for adoption?