Confidential DNS

- Draft-wijngaards-dnsop-confidentialdns -00
- Encrypt DNS traffic:
  - UDP ; server can be stateless.
  - Stub->resolver and resolver->authority.
  - probe for public keys in the clear (opportun)
  - Fallback to insecure on failures (opportun.)
  - One roundtrip latency, but cache key TTL
  - Algorithm agility
  - Does not stop reflection

Confidential DNS RRType

- “ENCRYPT” hop-by-hop RR type.
  - – . ENCRYPT <flag> <algo> <id> <bytes of data> [name TYPE octet octet octet remaining-rdata]
  - – ENCRYPT KEY : public key for remote server
  - – ENCRYPT RRS : encrypted query or reply records
  - – ENCRYPT SYM : encrypted symmetric secret
  - – ENCRYPT PAD : pad data to make length unusable for tracking purposes.
- Proto: query for server KEY, send own KEY and encrypted query. Reply is encrypted.