Confidential DNS

- Draft-wijngaards-dnsop-confidentialdns `-03`
- DNS privacy – Dprive WG wants adoption?
  - Does not solve unrelated problems
- UDP (and TCP), algorithm agility, cachable, IPv4and6, onPort53
- Deployable: opportunistic overcomes obstacles with insecure fallback. Possible 'default on'
- Latency: 1 extra query per TTL of the result (0 for initial transmit in DS record)

Updates 02 → 03

- Simplified – others are increasingly complex
- Also encrypt DNS RCODE
- *Optional* authenticated keys with DNSSEC
  - Transmit 'keybearing' DS record in referral
  - Lookup key at reverse-IP-address.arpa
    - For recursives, this is using the currently available contact information for ISP resolver, the IP address.
    - Could use a 'forward' name, `_encrypt._dns.isp.example`, but that would require configuration at the client or a DHCP option to transmit it

Confidential DNS RRType

- "ENCRYPT" 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 (and "wrong-key" signal)
- Query ". ENCRYPT", get KEY(s), send encrypted query, get encrypted answer, if failure fallback to insecure