edns-key-tag

dnsop

IETF 95 Buenos Aires

Memory Refresh

- Method by which validators can report their trust anchors (key tags) to zone operators
- Provide data to zone operators during KSK rollovers
- Modeled after RFC6975
  - Signaling DNSSEC algorithm support via EDNS0

When To Send

- Stub or Recursive
- Query only
- query type = DNSKEY
- SHOULD for configured trust anchor
- MAY for cached DS records
- MUST NOT otherwise

Since Last Time

- Adopted by dnsop wg
  - draft-ietf-dnsop-edns-key-tag-00
- Discussion on mailing list
  - draft-ietf-dnsop-edns-key-tag-01
- Changes
  - s/intersection/union/ for stub forwarding case

Open Question: EDNS0 vs qname

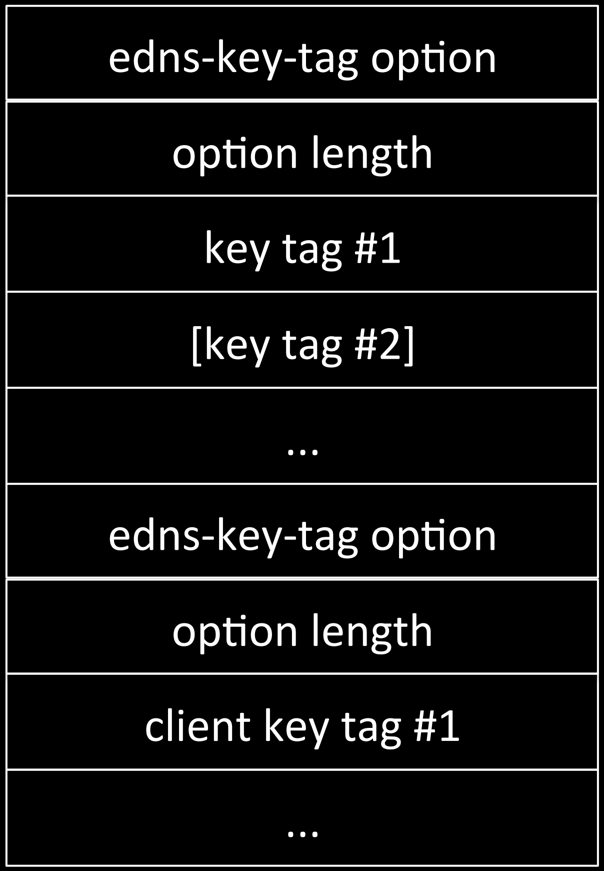
- Should Key Tags be sent as EDNS option?
- Or “normal” query in qname?

EDNS0 Encoding

edns-key-tag option
option length
key tag #1
[key tag #2]
...

- Piggybacks on regular DNSKEY query
- obfuscated in OPT_RR?
- New option code hinders adoption?

EDNS0 Encoding - forwarding



edns-key-tag option

option length

key tag #1

[key tag #2]

...

edns-key-tag option

option length

client key tag #1

...

- Piggybacks on regular DNSKEY query
- obfuscated in OPT_RR?
- New option code hinders adoption?

Qname Encoding

- Separate query
- Mark Andrews Approved™
- qname = _ta-xxxx.<domain>
- e.g. for root: _ta-4a5c
- qtype = NULL
- mulitple key tags

  _ta-xxxx,xxxx,xxxx.<domain>