edns-key-tag

dnsop

IETF 94 Yokohama

Problem

- Root Zone KSK Rollover being planned.
- RFC-5011 FTW!
  - But can we measure it?
- Very difficult to externally measure deployment of new DNSSEC trust anchors.

Validators

- Validators have Trust Anchors

```
. initial-key 257 3 8
        "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
        FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
        bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
        X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
        W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
        Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
        QxA+Uk1ihz0=";
```

Key Tags

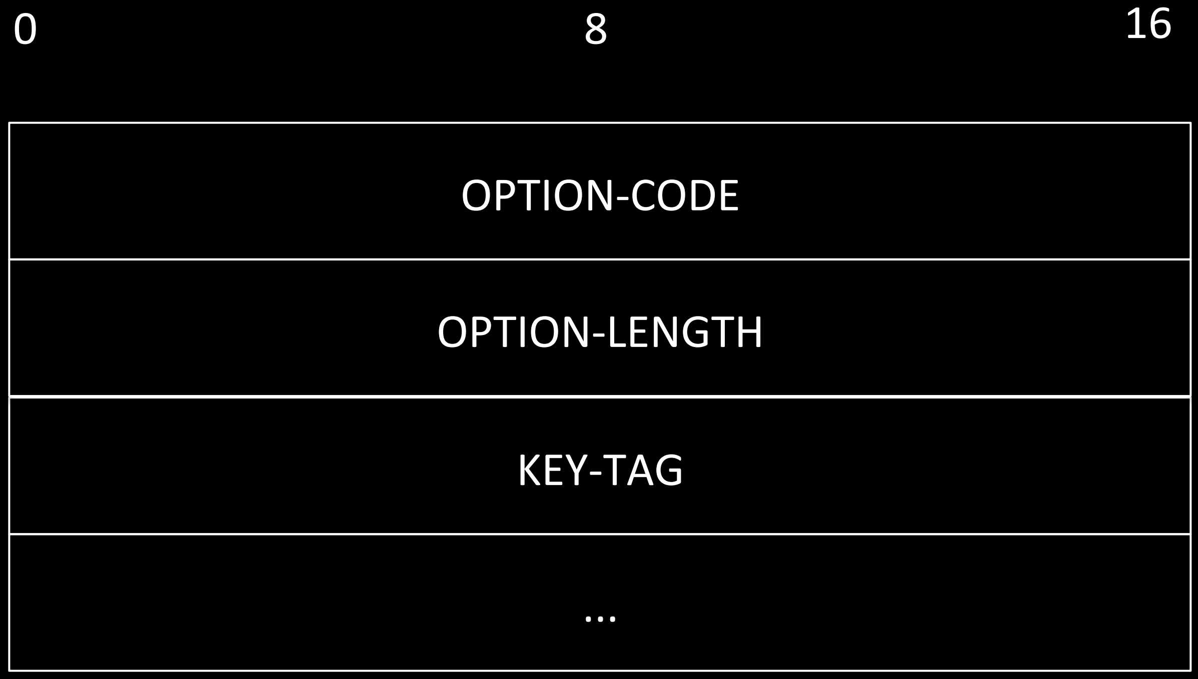
- Trust Anchors have Key Tags

```
;; ANSWER SECTION:
.                       43316   IN      DNSKEY  257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=  ; KSK; alg = RSASHA256; key id = 19036
```

Proposal

- Validators (clients) can transmit Trust Anchor Key Tags in queries toward authoritative servers.
- Servers can collect and analyze Key Tags to monitor progress of key rollover.
- Modeled after RFC 6975 - Signaling Cryptographic Algorithm Understanding

Option Format



0

8

16

OPTION-CODE

OPTION-LENGTH

KEY-TAG

...

KEY-TAG: One or more 16-bit Key Tag values

When To Send

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

Forwarding edns-key-tag

- Validating stub sending queries to validating recursive.
- Recursive combines stub’s Key Tag(s) with its own.
  - – currently defined as union
  - – intersection has been proposed

Privacy Considerations

- Key Tags could be used for fingerprinting
- Not required to send for every DNSKEY query
- Not required to send for every TA/zone

Security Considerations

- Key Tag values can be faked
- Can identify users of old, possibly compromised, keys
- Key Tags not required to be unique in a zone

Q&A

- Please review
- Consider adoption by the WG

- Questions?