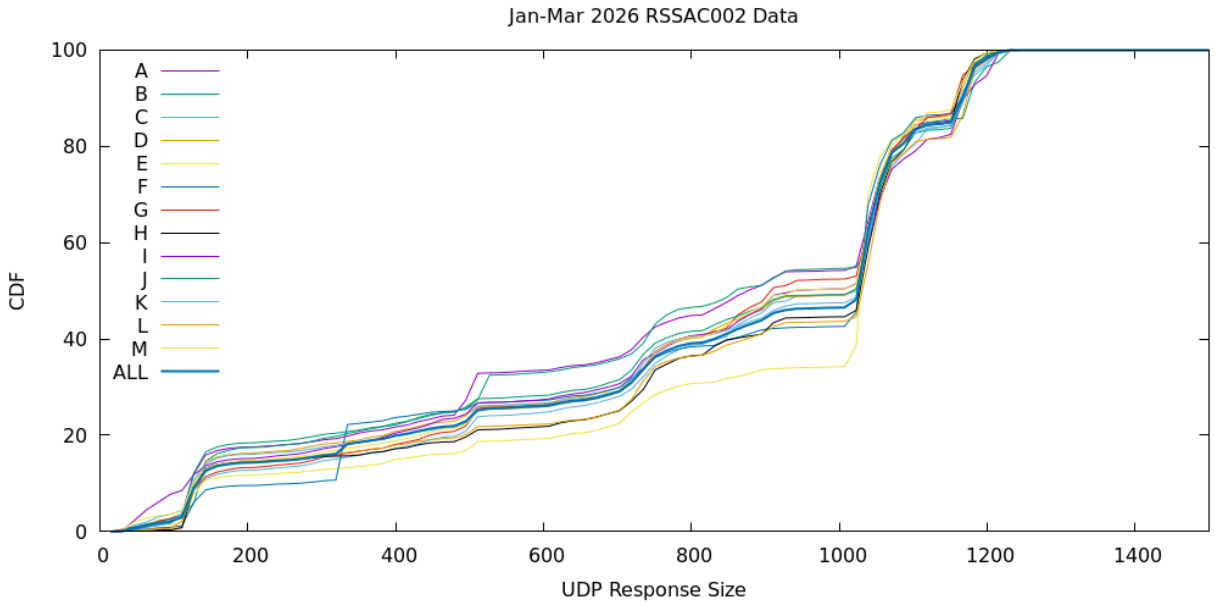
An Analysis of Root Server Response Sizes

April 2026

Duane Wessels, Verisign

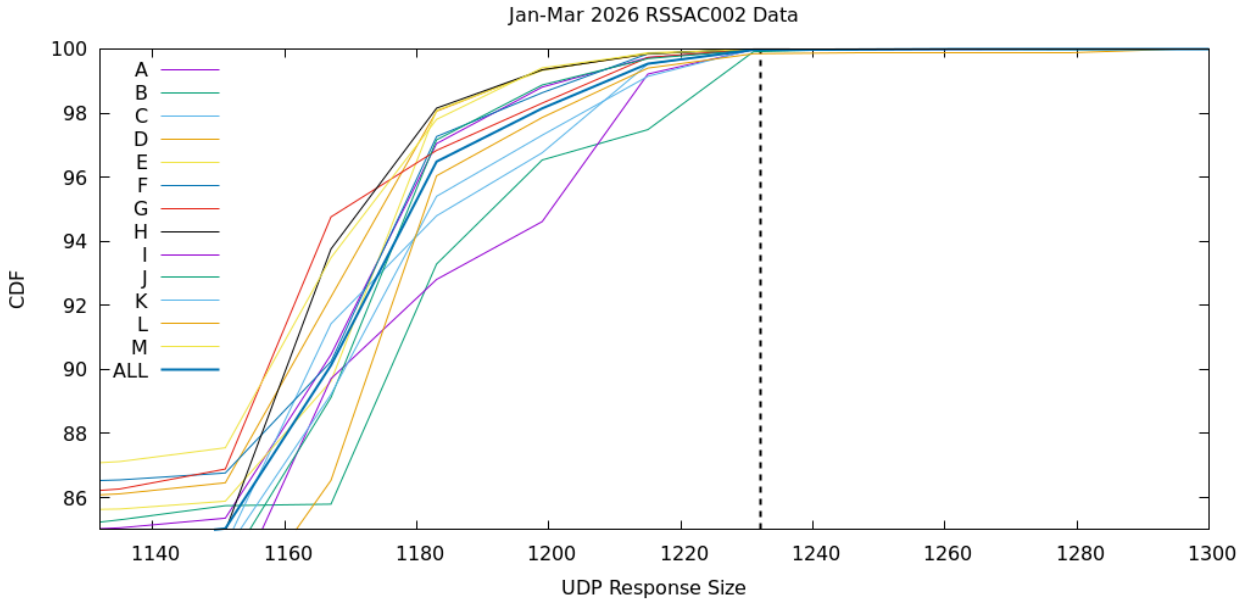
RSSAC-002 Data

RSOs provide daily aggregated measurements of root server response sizes in their RSSAC-002 data (in 16-byte wide buckets). The graph below shows the cumulative distribution percentage of response sizes for RSSAC-002 data from January-March of 2026.



The graph shows that there are very few responses above 1232 bytes. This is because (a) such responses rarely occur naturally, and (b) many RSOs will truncate responses above that size.

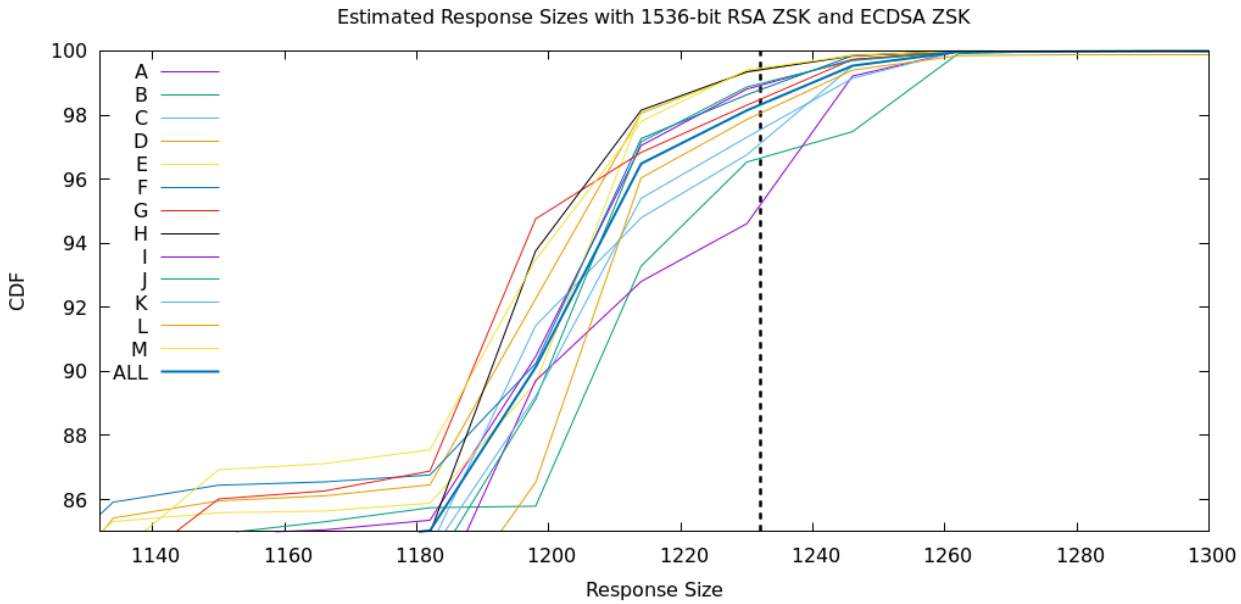
The graph below zooms in to the region of interest around the maximum size limit.



As a reminder, this is from current root server traffic where we have one algorithm (RSA) and the ZSK size is 2048-bits. During the proposed algorithm transition, we would reduce the RSA ZSK size to 1536-bits, which makes responses 64 bytes smaller per signature, and add an ECDSA ZSK, which makes responses 95 bytes larger per signature. Thus, each response becomes 31 bytes larger per signature. Referral responses (about half of root traffic) have just one signature, while NXDomain response (about the other half of traffic) have three signatures.

Referral response sizes are heavily influenced by the number of NS records for a given TLD, and to a lesser extent the number of DS records. Referrals for .com and .net are among the largest since they have 13 NS records (and 13 A+AAAA glue records). NXDomain responses tend to not only depend on the query name length, but also on where the query name falls in relation to existing TLDs. A .com referral today is larger (~1200 bytes) than an NXDomain response (~1100 bytes). Unfortunately, the RSSAC-002 data does not differentiate between response types, which makes modeling changes in response size somewhat difficult.

If we model the reduction in ZSK size to 1536 and addition of ECDSA as a minimum increase of 31 bytes in response size, then the response size distribution looks something like the graph below.



Somewhere between 1-5% of responses would be pushed over the 1232-byte limit.

DNS Cookies

Another factor to consider is the increasing prevalence of DNS Cookies. Most DNS clients already support EDNS0, which adds at least 11 bytes to the response. We're seeing the use of DNS Cookies becoming more common, which adds another 28 bytes.

Other RSA Sizes

Guidance from NIST and other bodies generally only consider specific RSA key sizes (e.g., 1024, 2048, 3072, 7680, 15360). However, the RSA algorithm does not require key size be multiples of 512 or any other value. Verisign, in fact, operated .com and .net with 1280-bit RSA zone signing keys for many years.

Each 16-bit increase in key size results in an extra 2 bytes of DNS response data per signature. Furthermore, each 16-bit increase in key size results in about 0.5 additional bits of security for the range of key RSA key sizes appropriate for DNSSEC. An RSA key of 1600-bits adds 2 bits of security over 1536, makes referrals 8 bytes larger, and NXDomain responses 24 bytes larger.

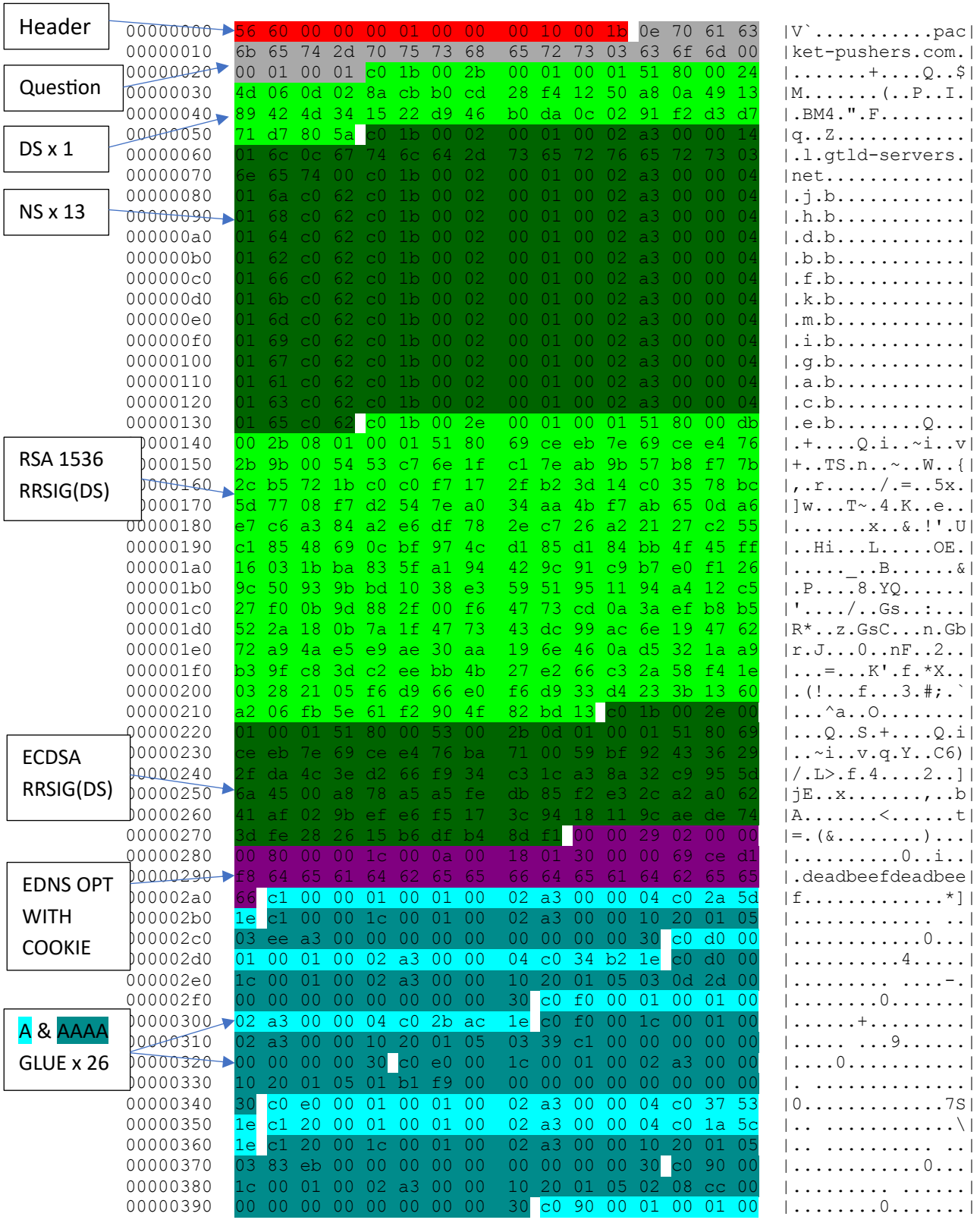
Given that:

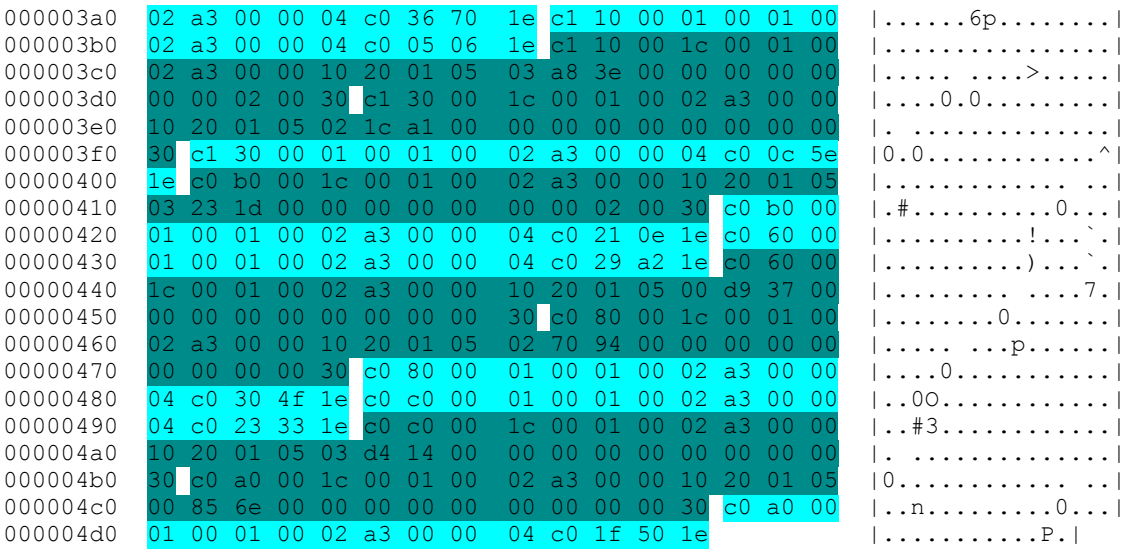
- We know some responses (at least 2-5%) doubly signed by a 1536-bit RSA key and an ECDSA key will exceed 1232 bytes, and
- We expect usage of DNS Cookies to increase over the next few years, and

- More resolver vendors might decide to implement---and more RSOs might decide to deploy---RFC 9471 aka “Glue is not Optional,”

We recommend staying with a 1536-bit RSA zone signing key for the root zone algorithm transition.

Anatomy of a DNS Response Packet





```
000003a0  02 a3 00 00 04 c0 36 70  1e c1 10 00 01 00 01 00  |......6p........|
000003b0  02 a3 00 00 04 c0 05 06  1e c1 10 00 1c 00 01 00  |................|
000003c0  02 a3 00 00 10 20 01 05  03 a8 3e 00 00 00 00 00  |..... ....>.....|
000003d0  00 00 02 00 30 c1 30 00  1c 00 01 00 02 a3 00 00  |....0.0.........|
000003e0  10 20 01 05 02 1c a1 00  00 00 00 00 00 00 00 00  |. ..............|
000003f0  30 c1 30 00 01 00 01 00  02 a3 00 00 04 c0 0c 5e  |0.0............^|
00000400  1e c0 b0 00 1c 00 01 00  02 a3 00 00 10 20 01 05  |............. ..|
00000410  03 23 1d 00 00 00 00 00  00 00 02 00 30 c0 b0 00  |.#..........0...|
00000420  01 00 01 00 02 a3 00 00  04 c0 21 0e 1e c0 60 00  |..........!...`.|
00000430  01 00 01 00 02 a3 00 00  04 c0 29 a2 1e c0 60 00  |..........)...`.|
00000440  1c 00 01 00 02 a3 00 00  10 20 01 05 00 d9 37 00  |......... ....7.|
00000450  00 00 00 00 00 00 00 00  30 c0 80 00 1c 00 01 00  |........0.......|
00000460  02 a3 00 00 10 20 01 05  02 70 94 00 00 00 00 00  |..... ...p......|
00000470  00 00 00 00 30 c0 80 00  01 00 01 00 02 a3 00 00  |....0...........|
00000480  04 c0 30 4f 1e c0 c0 00  01 00 01 00 02 a3 00 00  |..0O............|
00000490  04 c0 23 33 1e c0 c0 00  1c 00 01 00 02 a3 00 00  |..#3............|
000004a0  10 20 01 05 03 d4 14 00  00 00 00 00 00 00 00 00  |. ..............|
000004b0  30 c0 a0 00 1c 00 01 00  02 a3 00 00 10 20 01 05  |0............. ..|
000004c0  00 85 6e 00 00 00 00 00  00 00 00 00 30 c0 a0 00  |..n.........0...|
000004d0  01 00 01 00 02 a3 00 00  04 c0 1f 50 1e           |...........P.|
```

Section	Record Type	Size	Comments
Header		12	
Question		24	Varies on query name length
Authority	DS x 1	48	Varies based on TLD preferences for number of DS records and choice of hash algorithm
	NS x 13	224	Varies, but 13 is worst case (.com/.net)
	RRSIG RSA 1536-bit	231	
	RRSIG ECDSA	95	
Additional	OPT (with COOKIE)	39	Can vary, cookies becoming more common
	A x 13	208	Worst case
	AAAA x 13	364	Worst case
TOTAL		1245	