Quality of DNS and DNSSEC in the .se Zone

Patrik Wallström

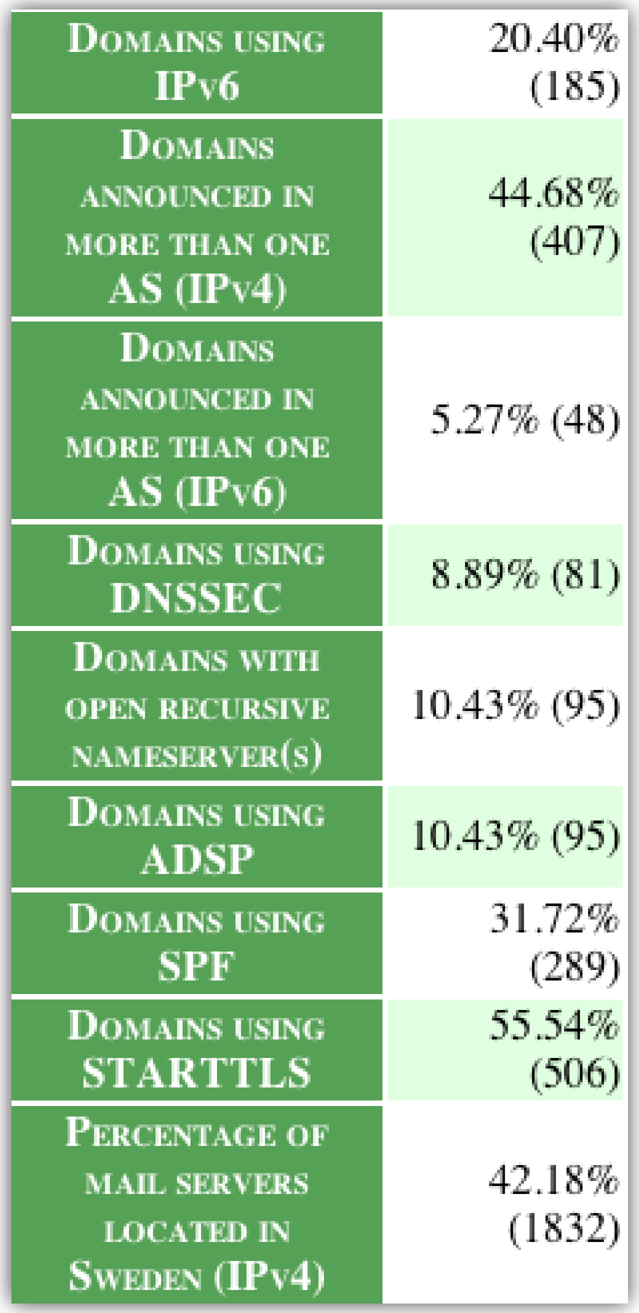
pawal@iis.se

The Yearly Healthcheck Surveys

- Analyze the quality and reachability of DNS in .se
  - key functions for .se registered domains
  - through a selection of domains that considered important
  - random selection of a percentage of all .se domains
- Primarily aimed at IT strategists and IT managers
  - Also intended for persons responsible for the operation
- Part of larger focus area “Health status of the Internet in Sweden”

The Healthcheck System

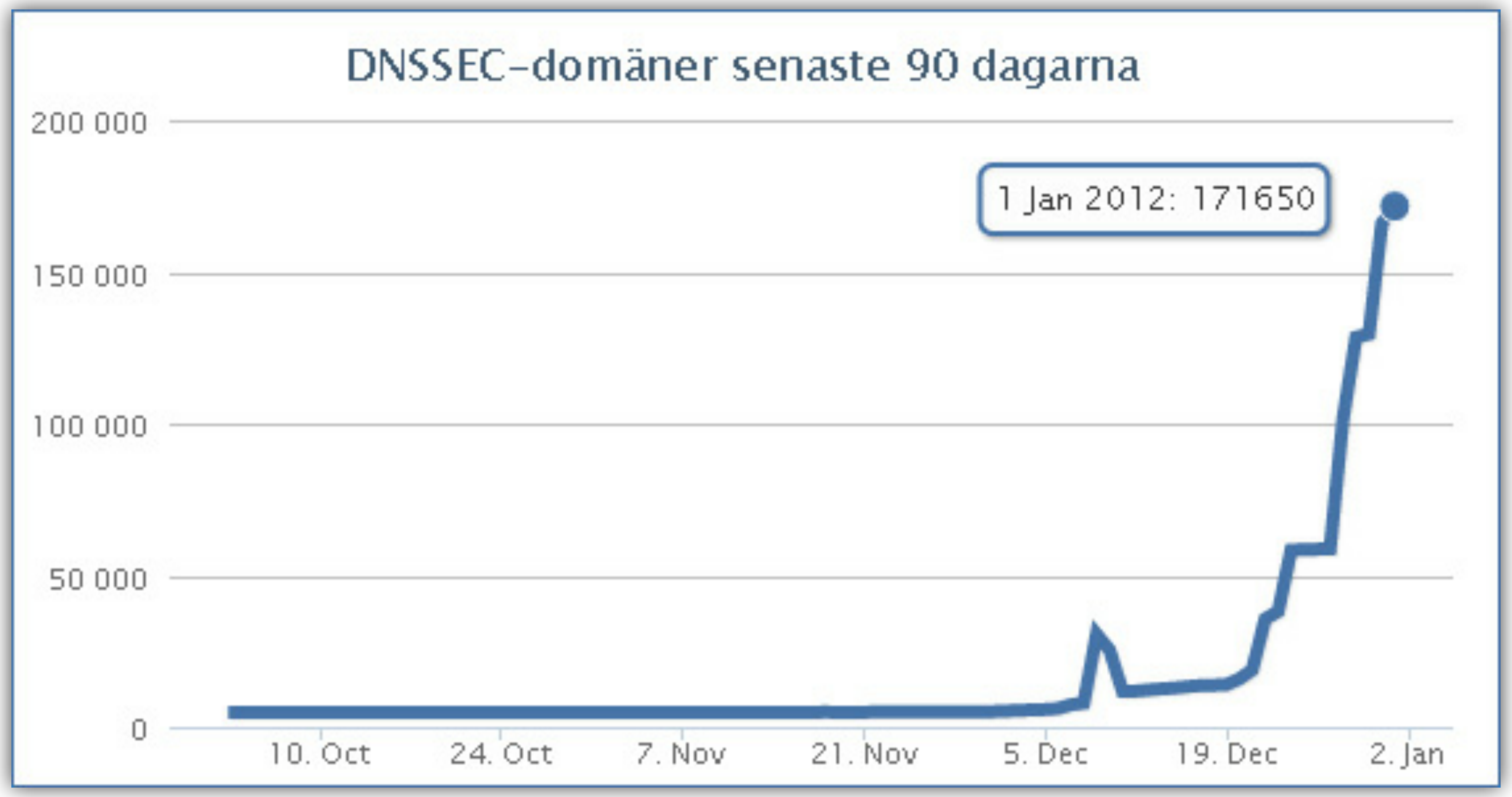
- Based on .SE:s DNSCheck
- Collects data from the a set of domains
  - DNS quality
  - Web pages (Page Analyzer for speed, and WhatWeb for content)
  - AS (web and DNS services)
  - Some e-mail related info (SPF, StartSSL...)
- Presents analysis



Domains using IPv6	20.40% (185)
Domains announced in more than one AS (IPv4)	44.68% (407)
Domains announced in more than one AS (IPv6)	5.27% (48)
Domains using DNSSEC	8.89% (81)
Domains with open recursive nameserver(s)	10.43% (95)
Domains using ADSP	10.43% (95)
Domains using SPF	31.72% (289)
Domains using STARTTLS	55.54% (506)
Percentage of mail servers located in Sweden (IPv4)	42.18% (1832)

.SE:s DNSSEC campaign

- To reach our goal on at least 50000 signed zones...
- Part of a larger campaign
  - Subsidy of 10 SEK per new DNSSEC domain
  - Yet another 4 SEK per DNSSEC domain at end of year



.SE Market Situation

- **Registrars:** .SE’s three largest account for 50 percent of the market. Seven largest commands 75 percent

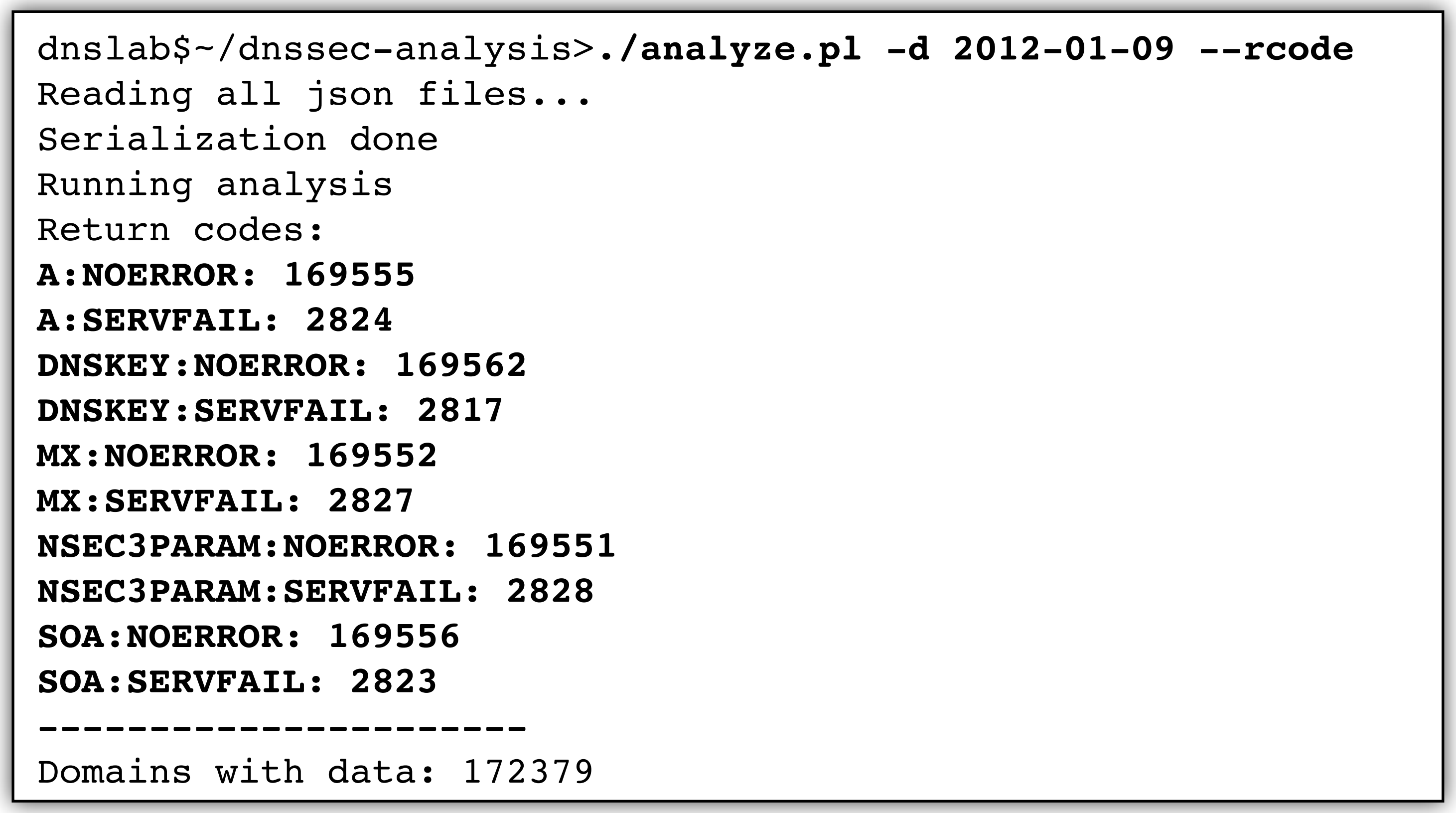
- **Name server operators:** Two largest have 36 percent, five largest commands 50 percent. Long tail with very small players

Most DNS-operators are DNSSEC newbies

- We decided to help them
  - By checking their zones
  - Regular report on DNS errors (after changes, opt-in)
  - Special DNSSEC error reports to Registrar Customer Support
- .SE Internal monitoring tools
  - Summary of the above
- A report on DNS with DNSSEC
  - Explaining all the DNSSEC parameters

A tool for analyzing DNSSEC quality

- “dnssec-analysis”
  - collect.pl: Quickly gather DNSSEC info on a list of domains
  - analyze.pl: Analyzes the data depending on interest
- https://github.com/pawal/dnssec-analysis



```
dnslab$~/dnssec-analysis>./analyze.pl -d 2012-01-09 --rcode
Reading all json files...
Serialization done
Running analysis
Return codes:
A:NOERROR: 169555
A:SERVFAIL: 2824
DNSKEY:NOERROR: 169562
DNSKEY:SERVFAIL: 2817
MX:NOERROR: 169552
MX:SERVFAIL: 2827
NSEC3PARAM:NOERROR: 169551
NSEC3PARAM:SERVFAIL: 2828
SOA:NOERROR: 169556
SOA:SERVFAIL: 2823
----------------------
Domains with data: 172379
```

.se

analyze.pl

```
Usage:
    analyze -d directory
    Required argument(s):
        --directory directory    A directory with WhatWeb JSON files

Optional arguments:
        --limit value            When generating lists, limit the length to this value
        --recache                Recreate our serialized cache (TODO)
        --fake-date YY-MM-DD     Make this the current date for signature lifetime comparisons
        --rcode                  Analyze RCODEs
        --servfail               Toplist of name servers with SERVFAIL
        --servfaillist ns        Get all domains that SERVFAIL on this name server
        --dsduplicates           Toplist of the number of domains that has the same DS record
        --keyduplicates          Toplist of the number of domains that has the same DNSKEY
        --working-ns             Toplist of name servers not NO ERROR on all queries
        --all-ns                 List all name servers in descending order # of associated zones
        --siglife                Analyze RRSIG lifetimes
        --extreme-sigs           List extreme RRSIG lifetimes (inception and expiration larger than 100 days)
        --expiration             Correlate SOA expiration value with lowest RRSIG lifetime
        --algorithms             Analyze DNSSEC algorithms and keylengths
        --nsec3                  Analyze NSEC3 (salt, iterations)
        --keytags                Analyze distribution of DNSKEY keytags
        --keytaglist n           List zones which contain the specified keytag
```

- A new specialized report on DNS and DNSSEC quality
- Focus on DNSSEC
- Explaining the issues...

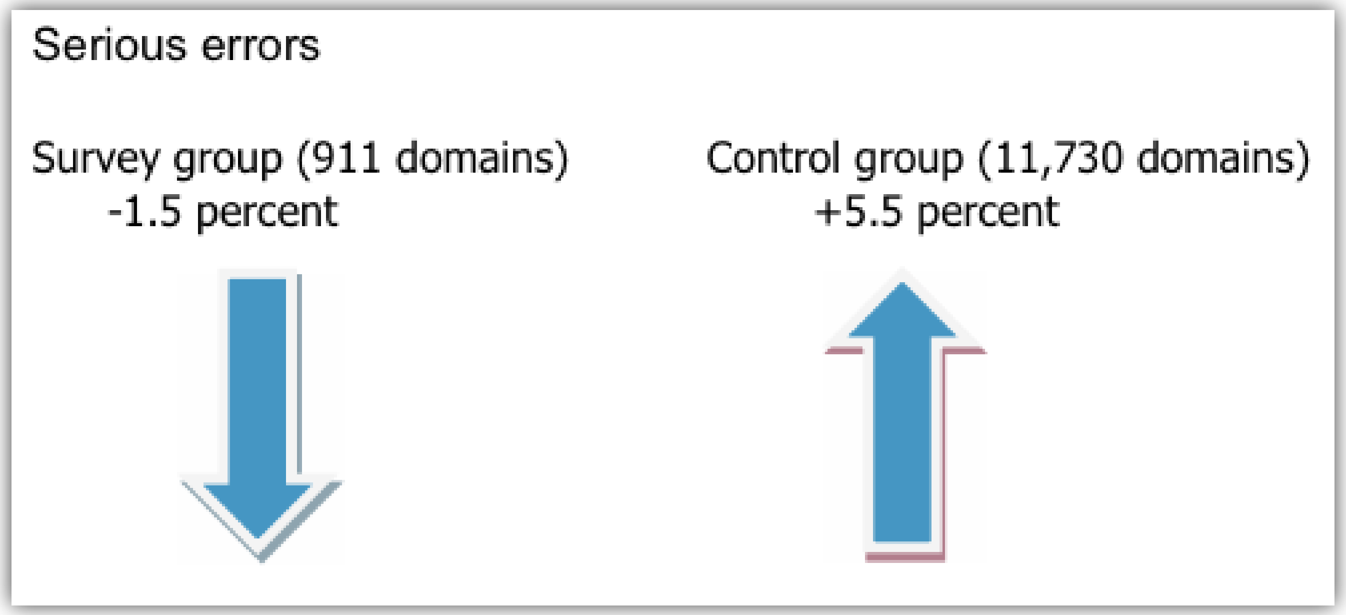
.se | .se Health Status

– DNS and DNSSEC

Results from the report

- Report was released 2012-03-21
- Measurements and analysis during February 2012
- 174,487 signed zones out of a total of 1,195,719
- 163,700 actually worked (no SERVFAIL)

“Normal” DNS →

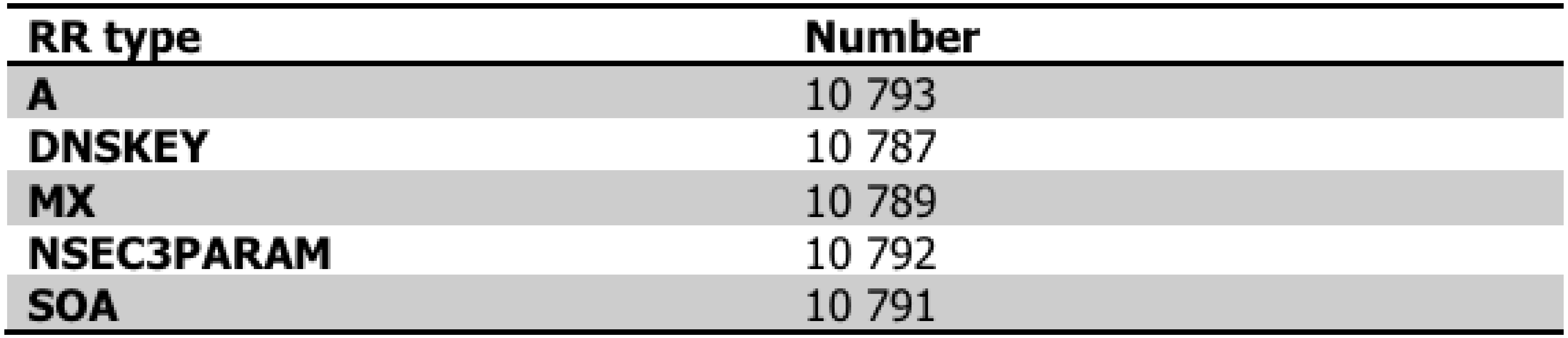


Serious errors

Survey group (911 domains)
-1.5 percent

Control group (11,730 domains)
+5.5 percent

SERVFAILs

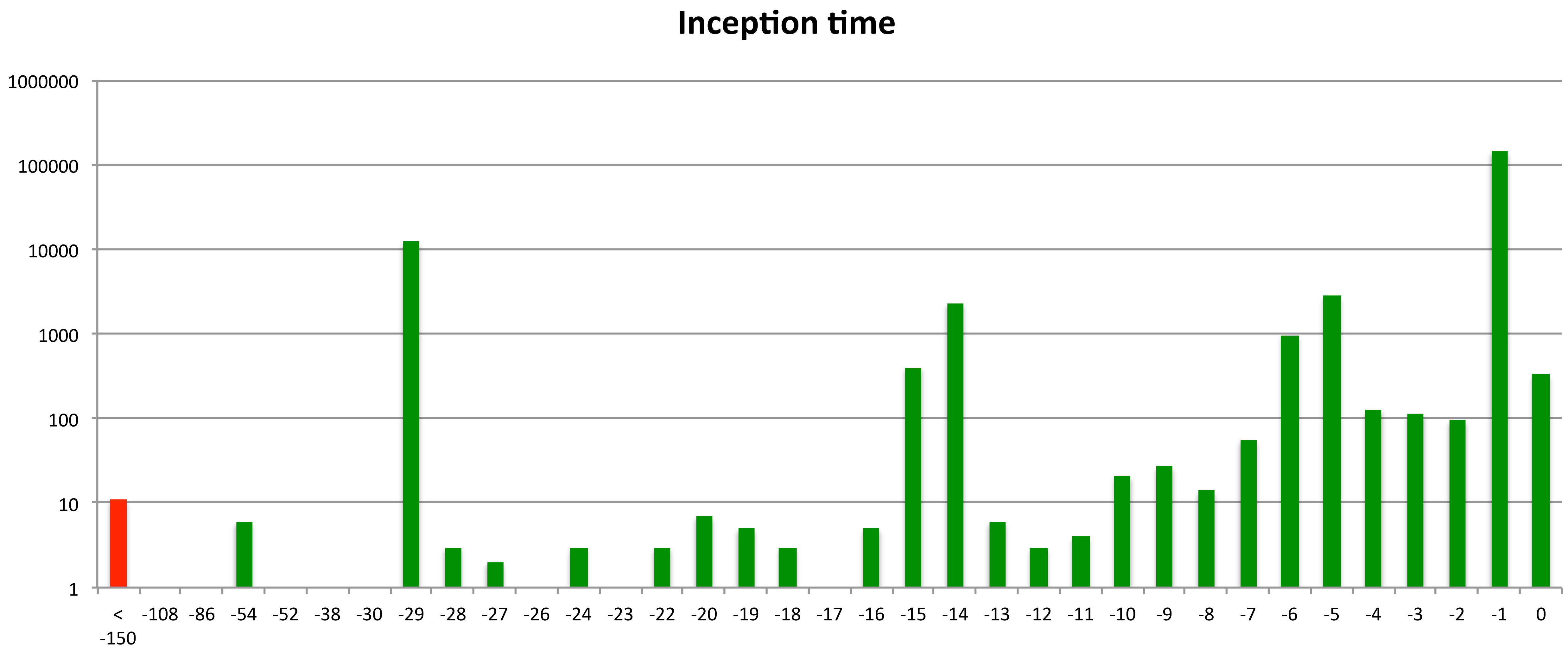


RR type	Number
A	10 793
DNSKEY	10 787
MX	10 789
NSEC3PARAM	10 792
SOA	10 791

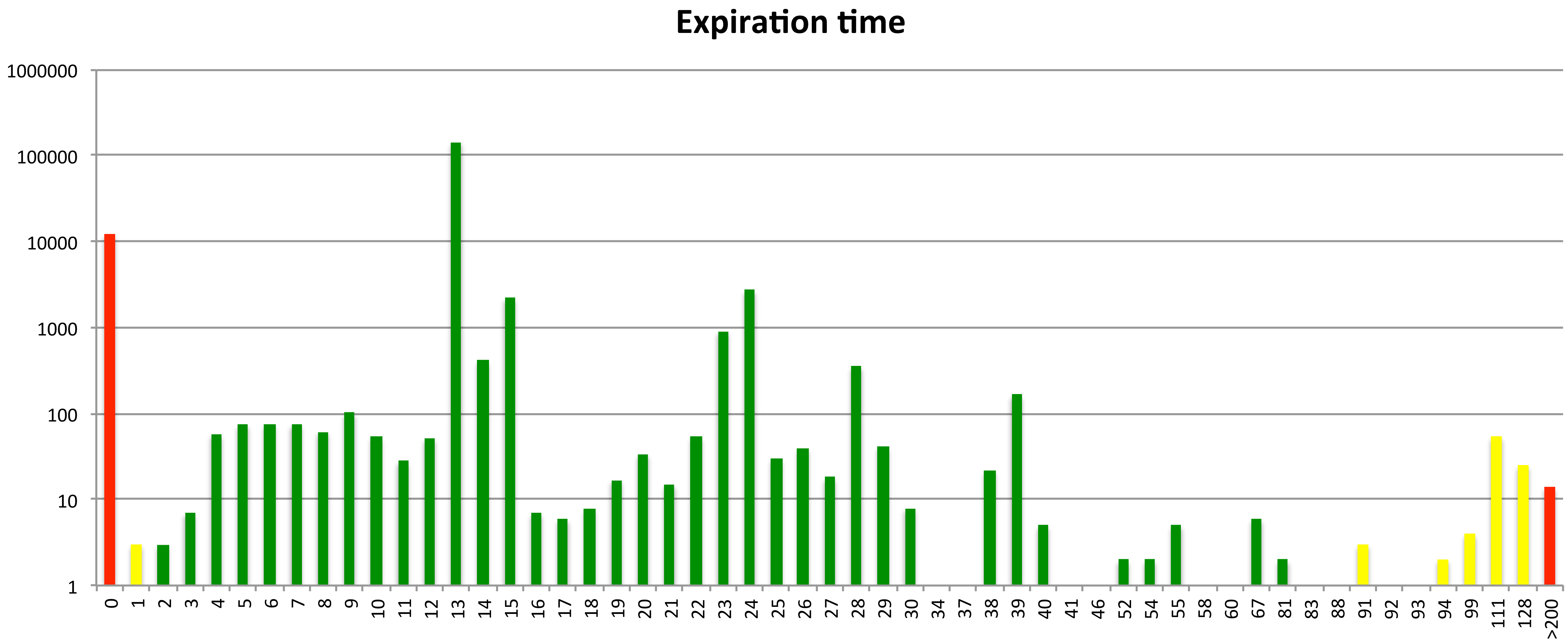
The tool queries for these RR types through local recursors:

A	Authoritative
DNSKEY	Authoritative
MX	Authoritative
NSEC3PARAM	Authoritative
SOA	Authoritative
DS	Parent (no DNSSEC validation)
NS	Parent (no DNSSEC validation)

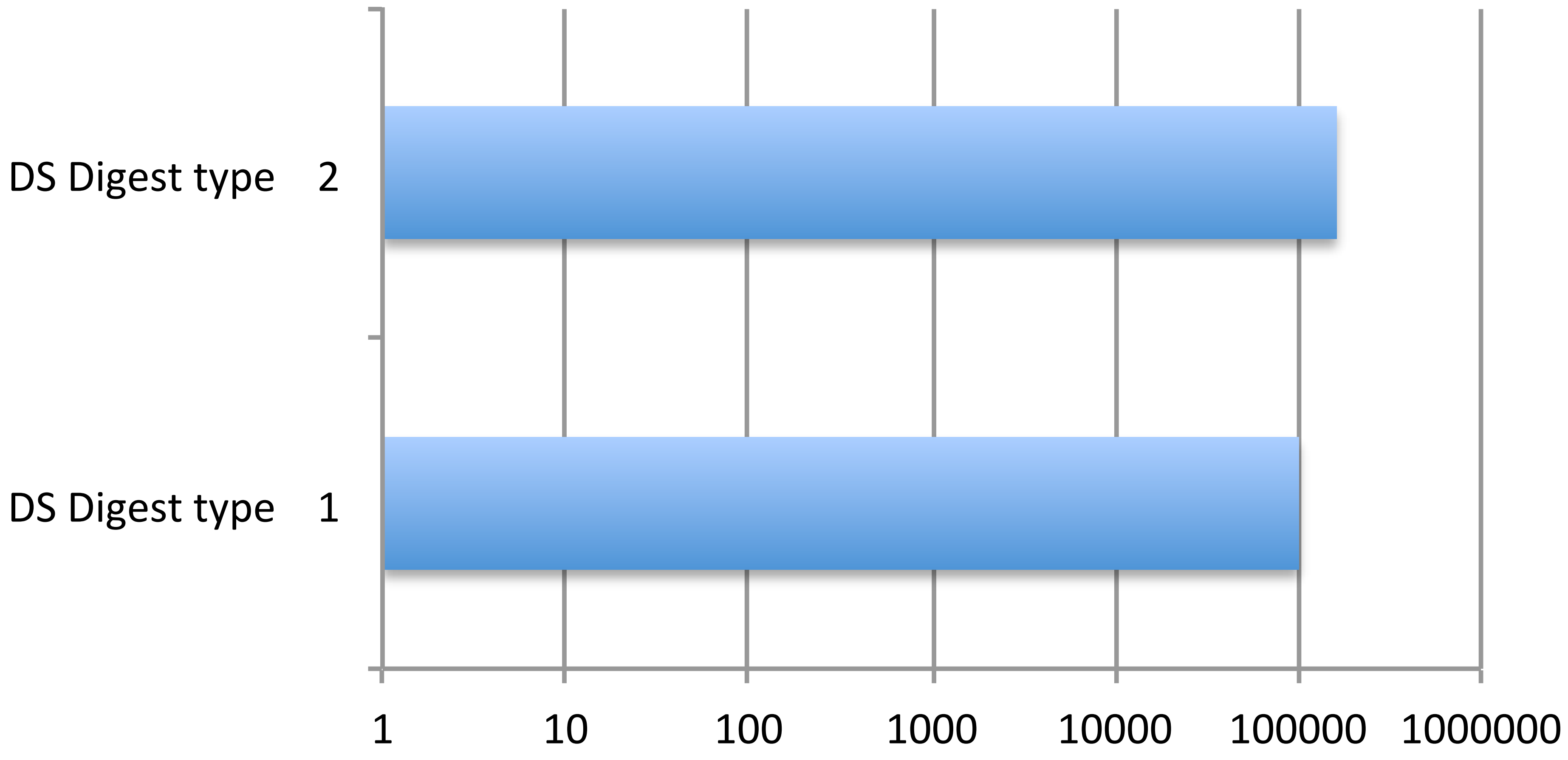
Signature Lifetimes



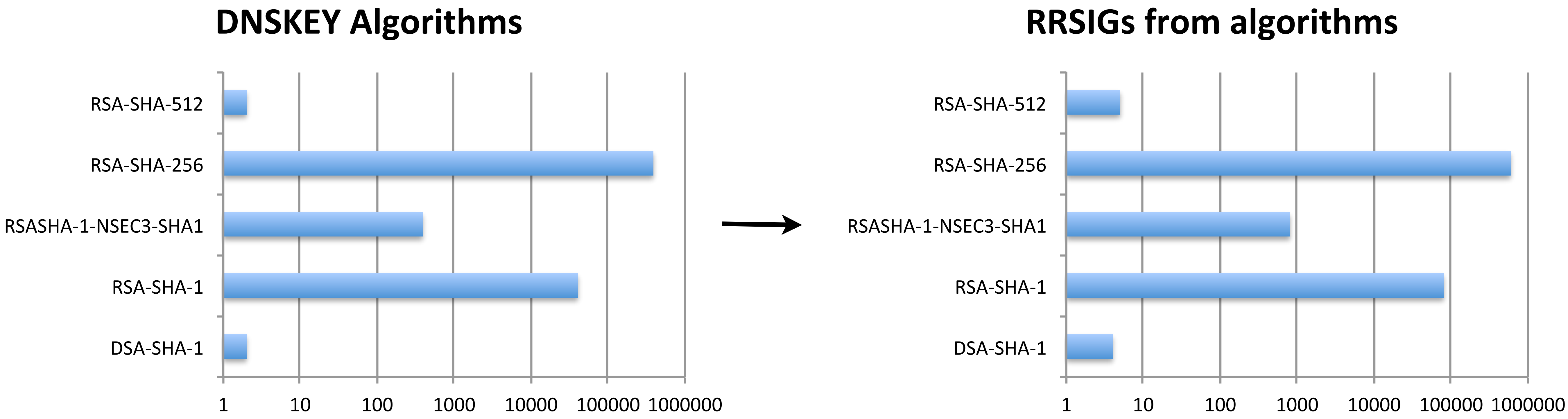
Signature Lifetimes



DS Digest types

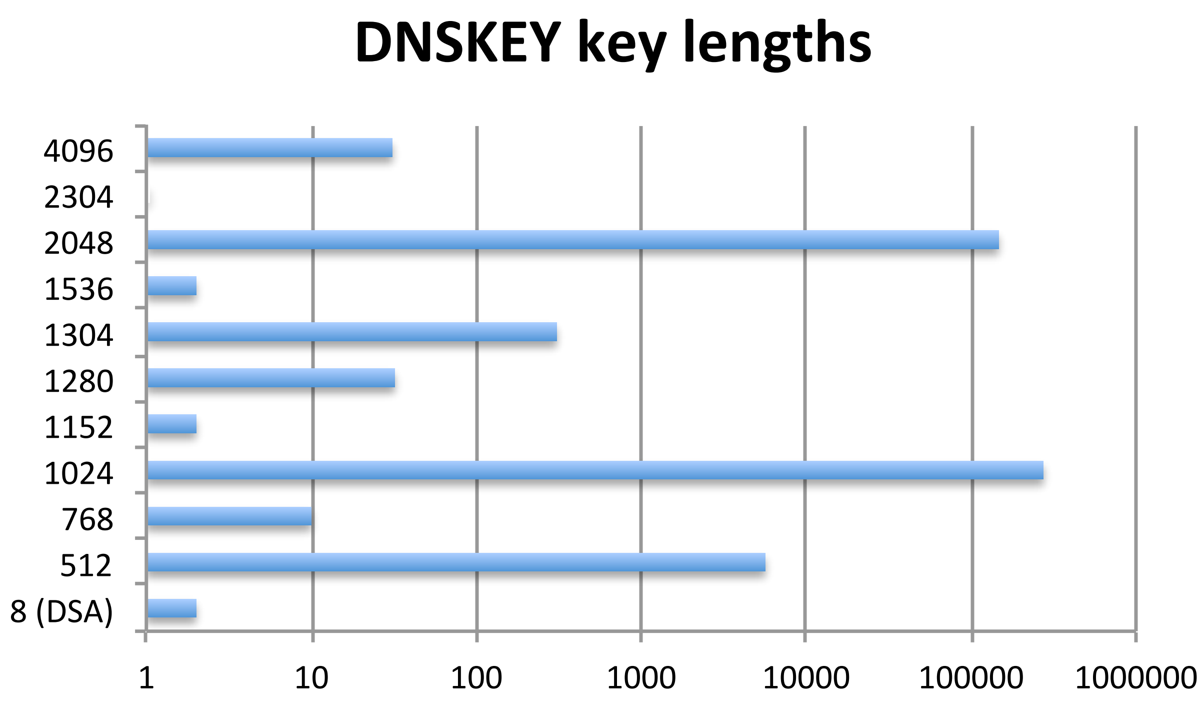


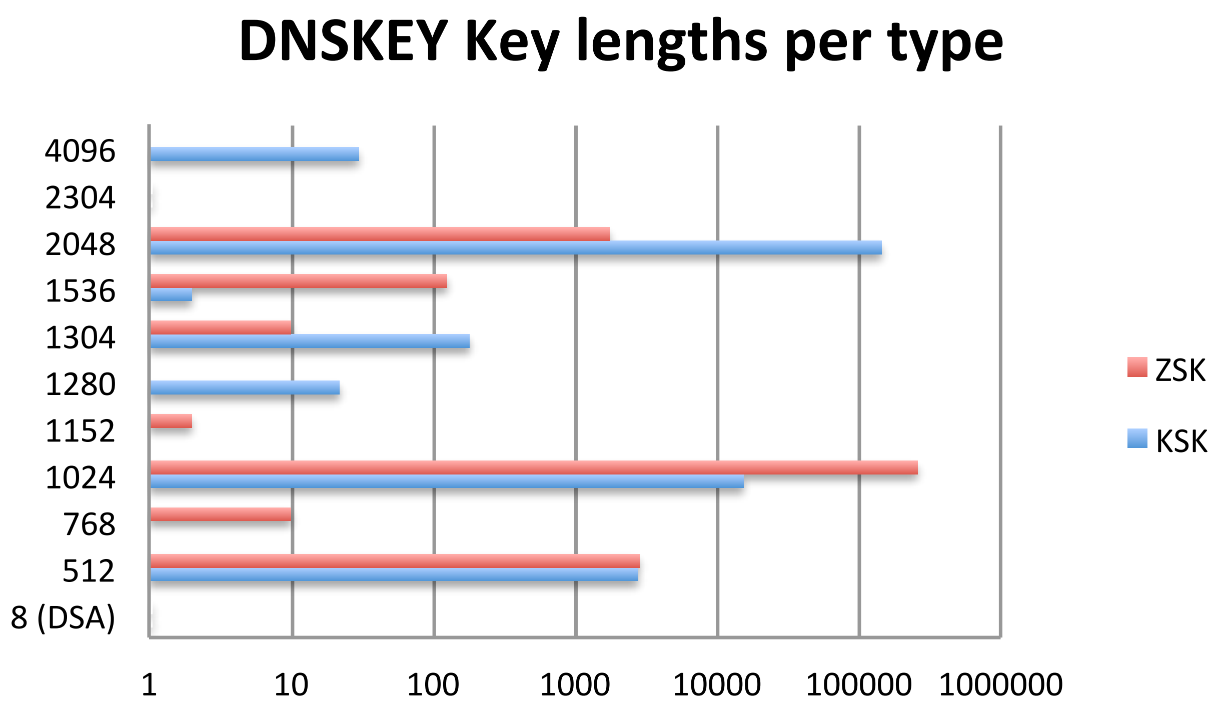
Algorithms



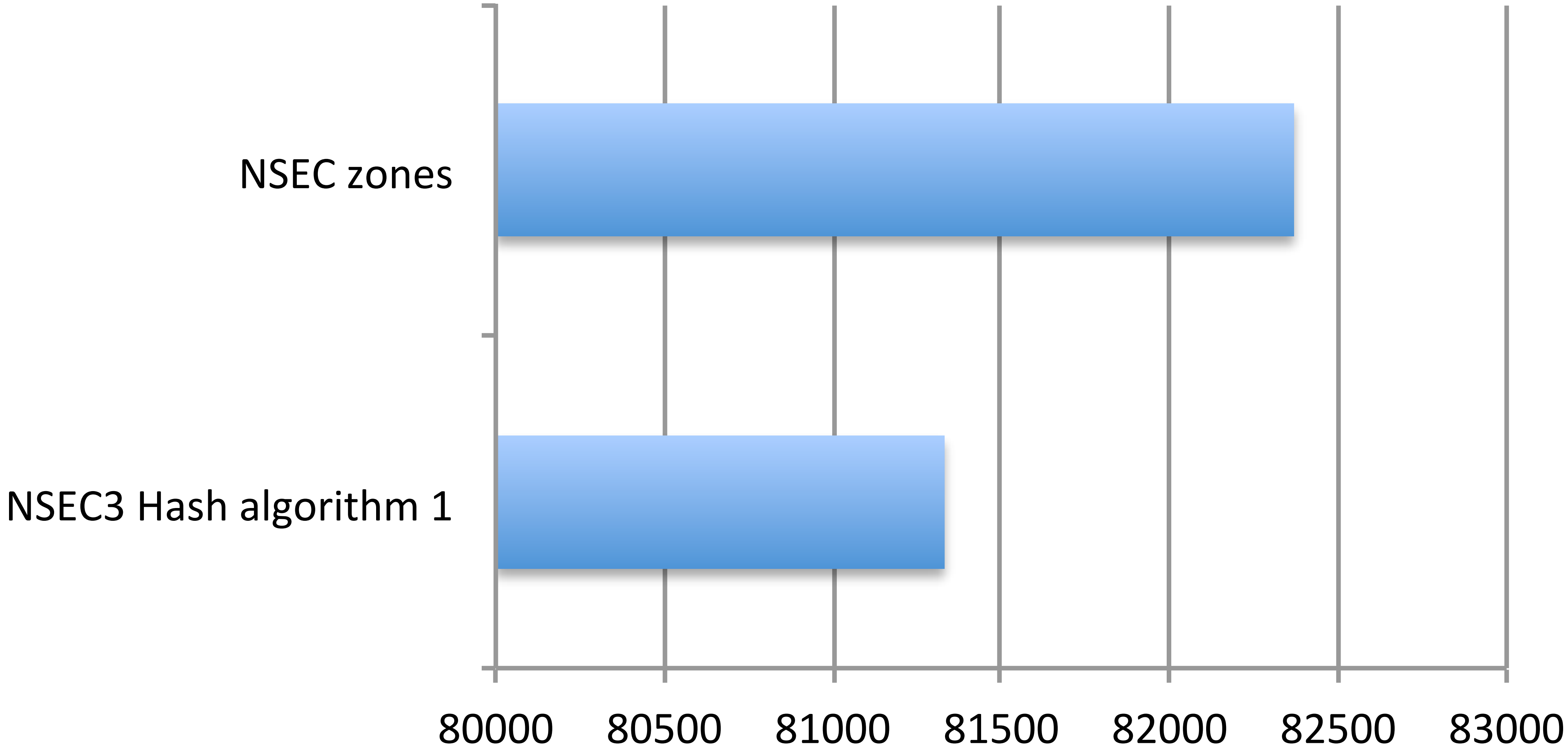
DNSKEY Algorithms
RSA-SHA-512
RSA-SHA-256
RSASHA-1-NSEC3-SHA1
RSA-SHA-1
DSA-SHA-1
1
10
100
1000
10000
100000
1000000
RRSIGs from algorithms
RSA-SHA-512
RSA-SHA-256
RSASHA-1-NSEC3-SHA1
RSA-SHA-1
DSA-SHA-1
1
10
100
1000
10000
100000
1000000

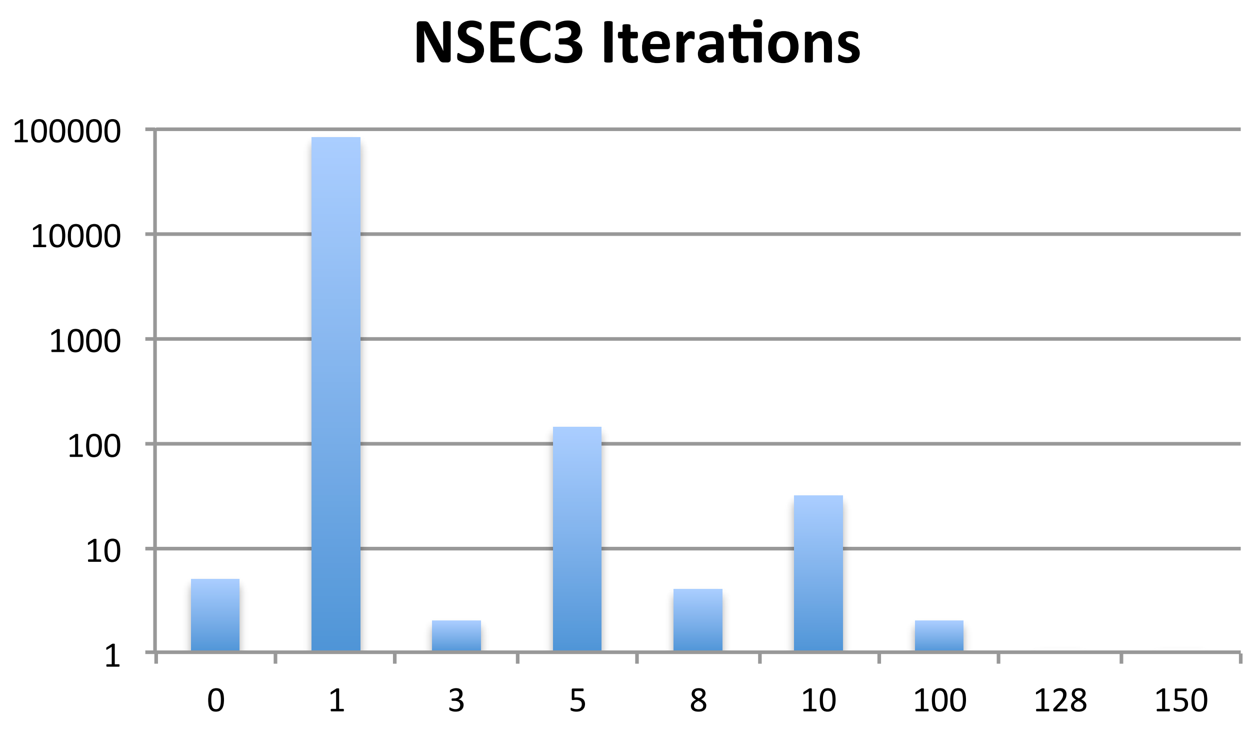
Key Lengths

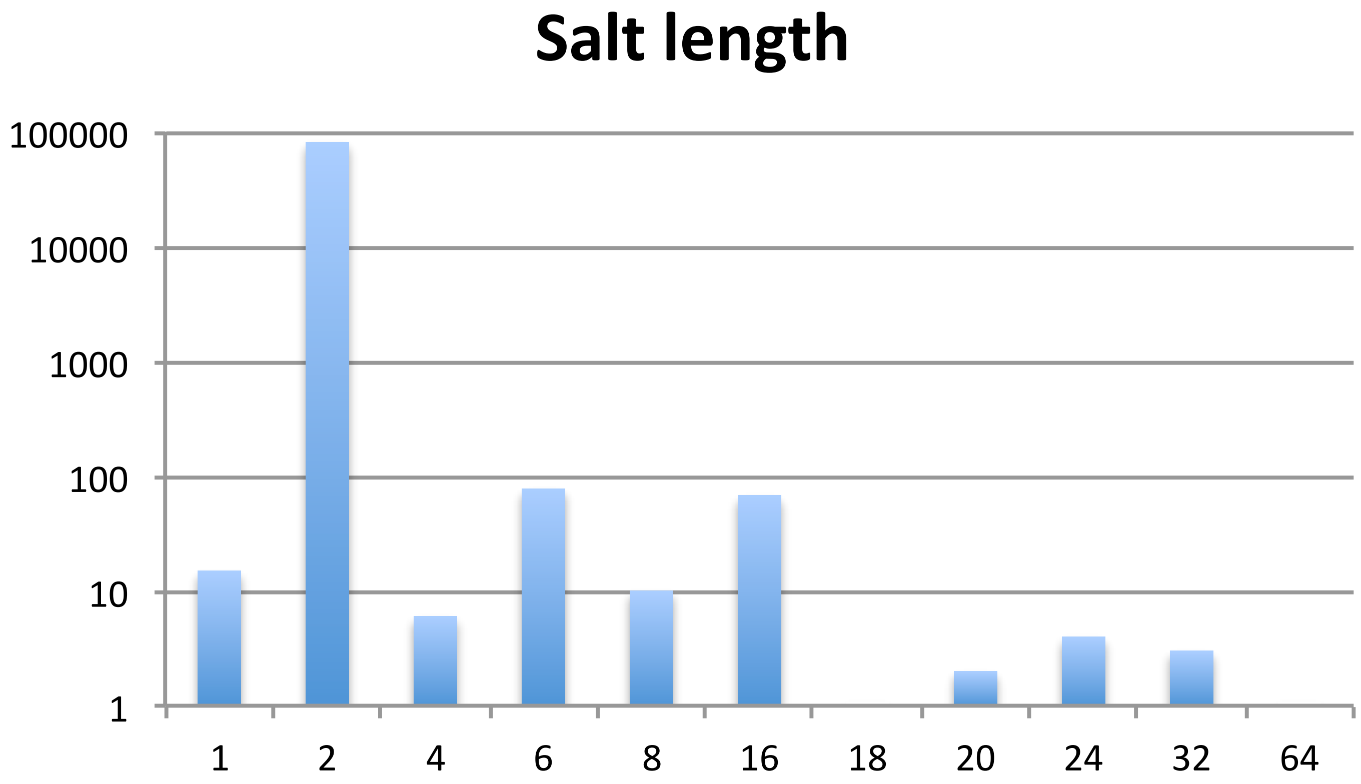

DNSKEY key lengths
4096
2304
2048
1536
1304
1280
1152
1024
768
512
8 (DSA)
1
10
100
1000
10000
100000
1000000


DNSKEY Key lengths per type
4096
2304
2048
1536
1304
1280
1152
1024
768
512
8 (DSA)
1
10
100
1000
10000
100000
1000000
ZSK
KSK

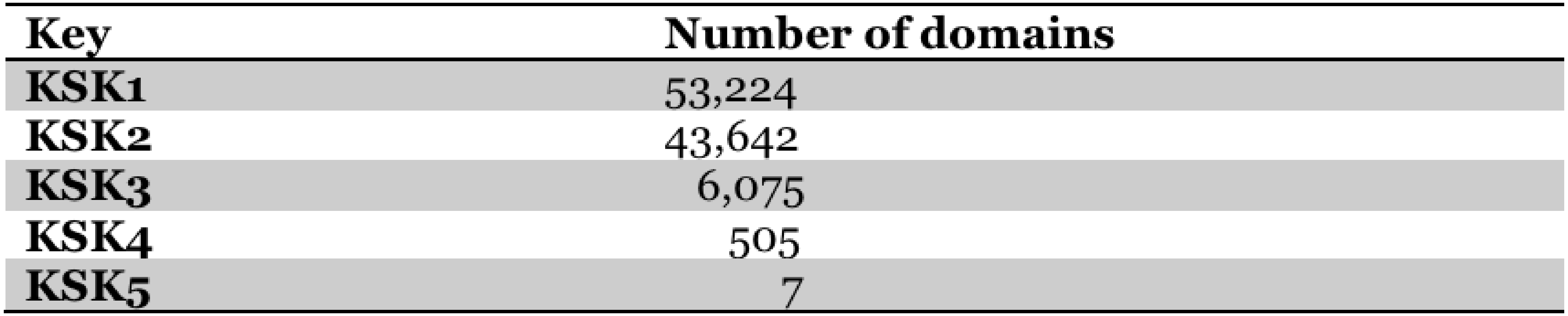
NSEC vs NSEC3




NSEC3 Iterations
100000
10000
1000
100
10
1
0
1
3
5
8
10
100
128
150


Salt length
100000
10000
1000
100
10
1
1
2
4
6
8
16
18
20
24
32
64

Shared Keys

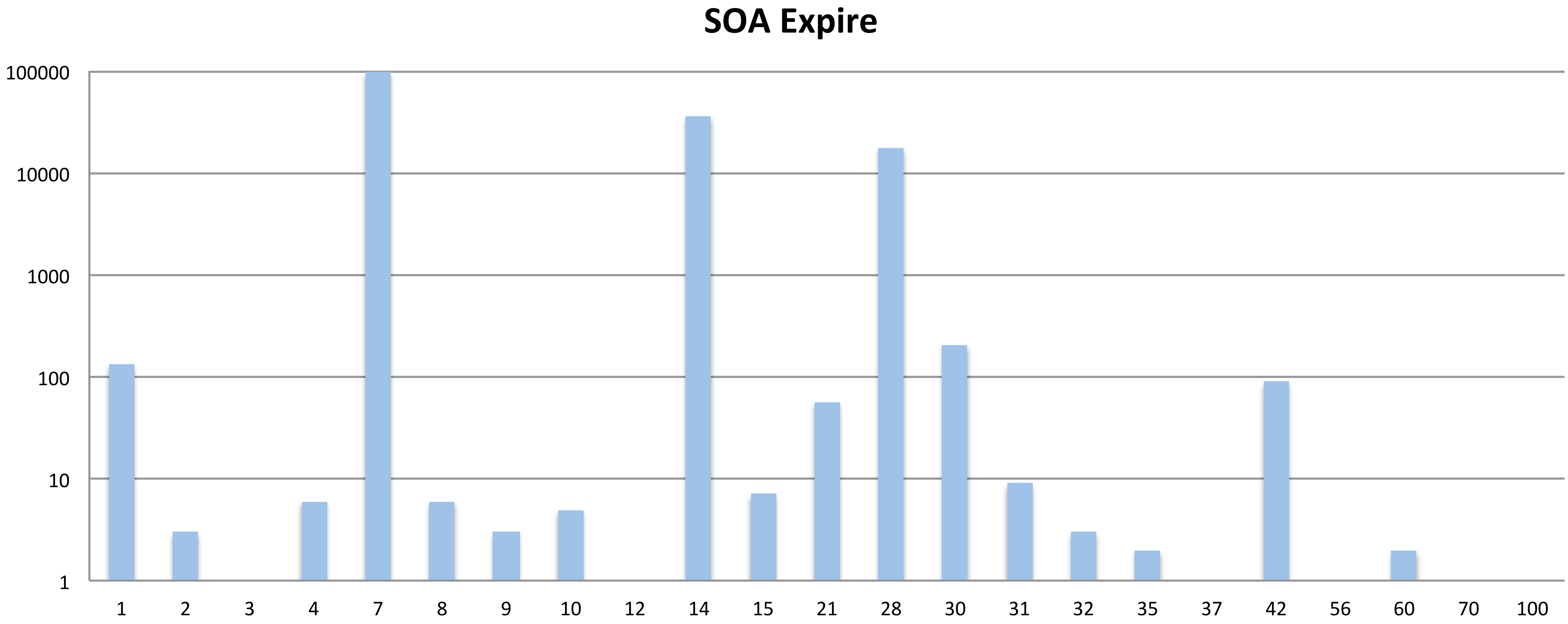


Key	Number of domains
KSK1	53,224
KSK2	43,642
KSK3	6,075
KSK4	505
KSK5	7

Key Averages...

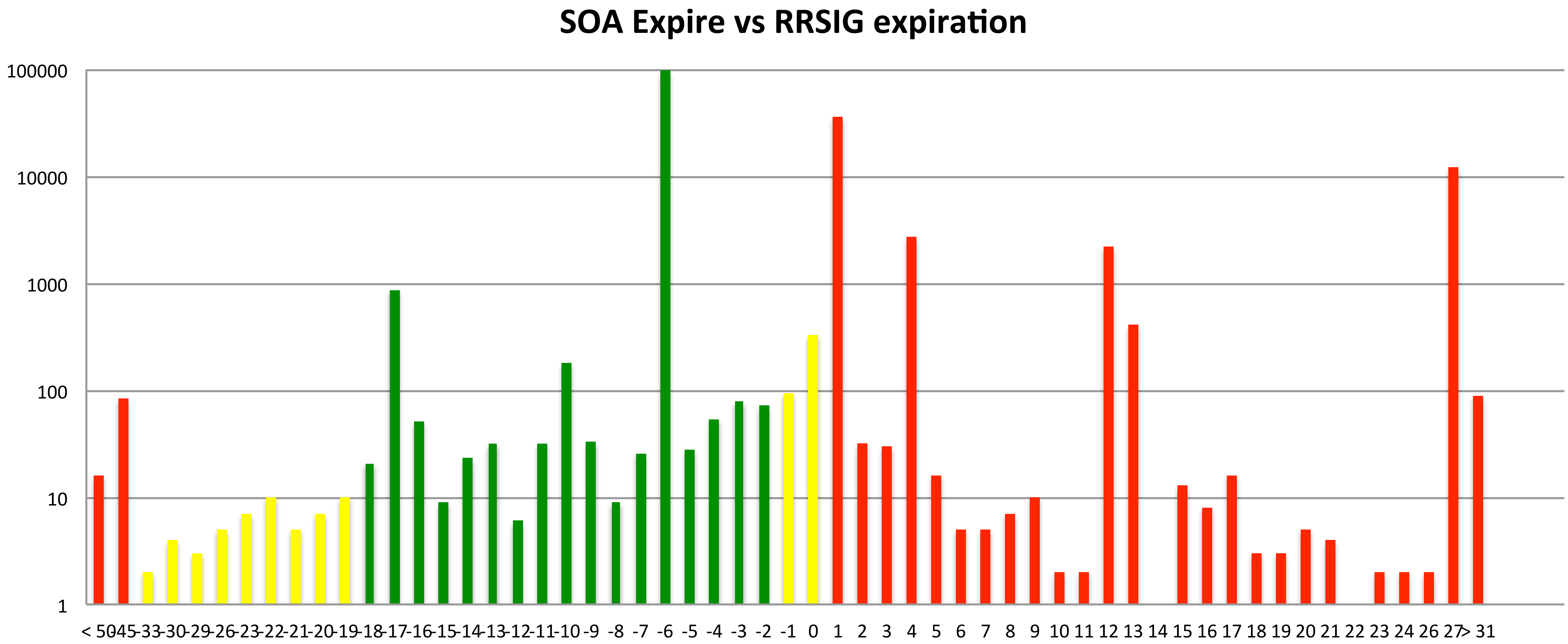
DS per domain	1.614838119
KSK per domain	1.000207697
ZSK per domain	1.612724496
DNSKEY per domain	2.612932193

SOA Expire vs RRSIG Expiration



RIPE recommendation is 1000 (41 days) for SOA Expire, RIPE-203

SOA Expire vs RRSIG Expiration



RFC4641bis says that RRSIG expiration should be 2/3 of SOA Expire

Summary of DNSSEC analysis

- Signature lengths found that are too short, or unexpectedly long
- Use of NSEC3 is essentially adequate
- Most domains use RSA keys, 2,048 bit KSK and 1,024 ZSK
- A few too many domains are using 512 bit keys ... in 2012
- We can begin to discontinue the double publication of DS types 1 and 2, as the publication of type 2 is sufficient today.
- All too often, SOA Expire lacks a connection to RRSIG expiration time, these parameters should definitely be reviewed.

.se

Future work

- Frequent measurements over time to see ...
  - Key rollovers
  - Signature refresh intervals
  - Number of domains that regularly fails
  - Salt replacements
- Long term measurements to see ...
  - Introduction rate of new algorithms
  - New operational methods (shared keys, CSK etc)
- TTLs

- RIPE DNSSEC recommendations document?

Thank you!

Code:

https://github.com/pawal/dnssec-analysis

Report:

https://www.iis.se/docs/Health-Status-DNS-and-DNSSEC-20120321.pdf

.se