Upcoming Changes to Verisign-Operated Top Level Domains

Duane Wessels

DNS-OARC 26, Amsterdam

October 13, 2018

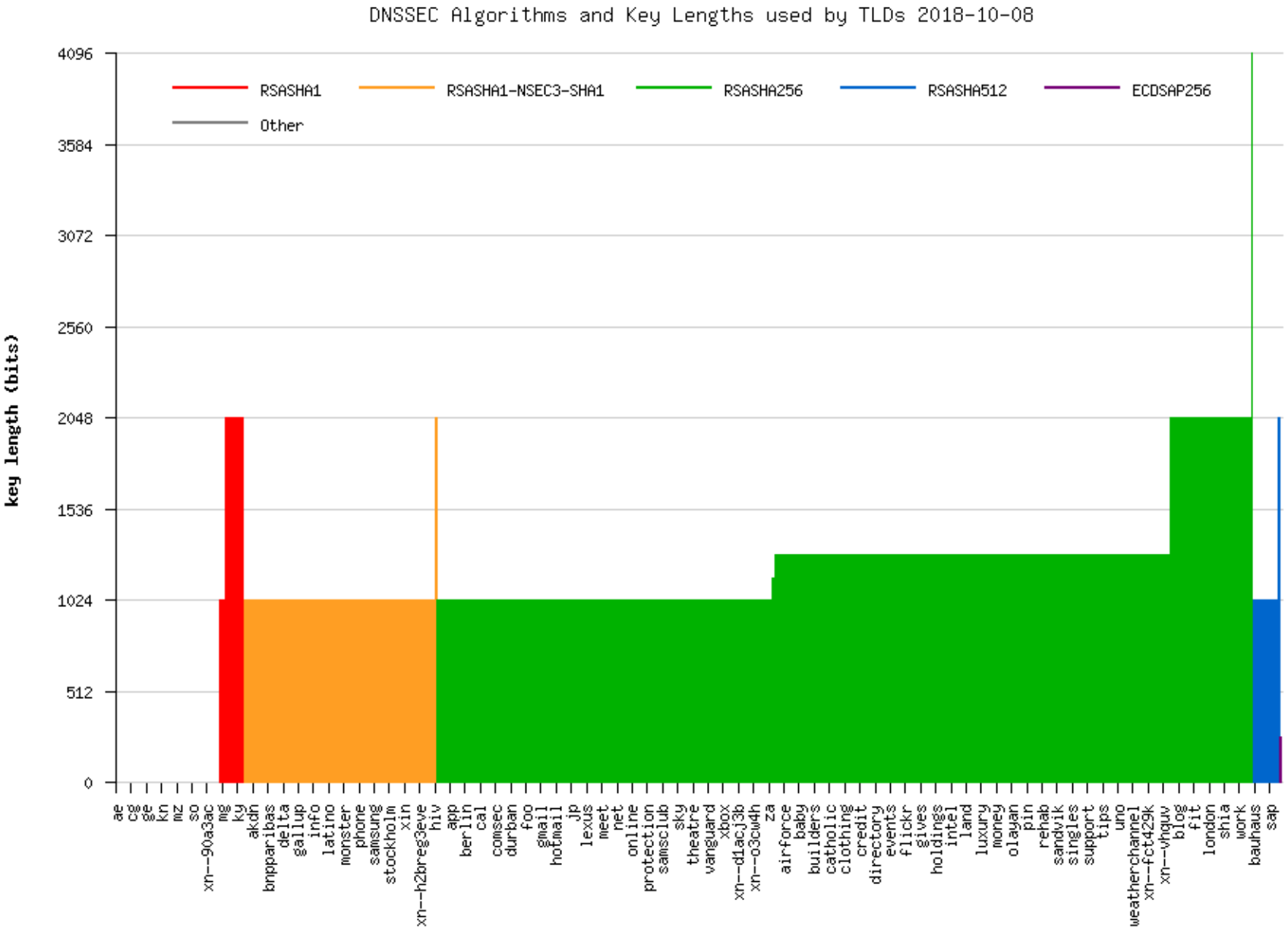
VERISIGN

Outline

Parameters in Verisign-operated TLDs:

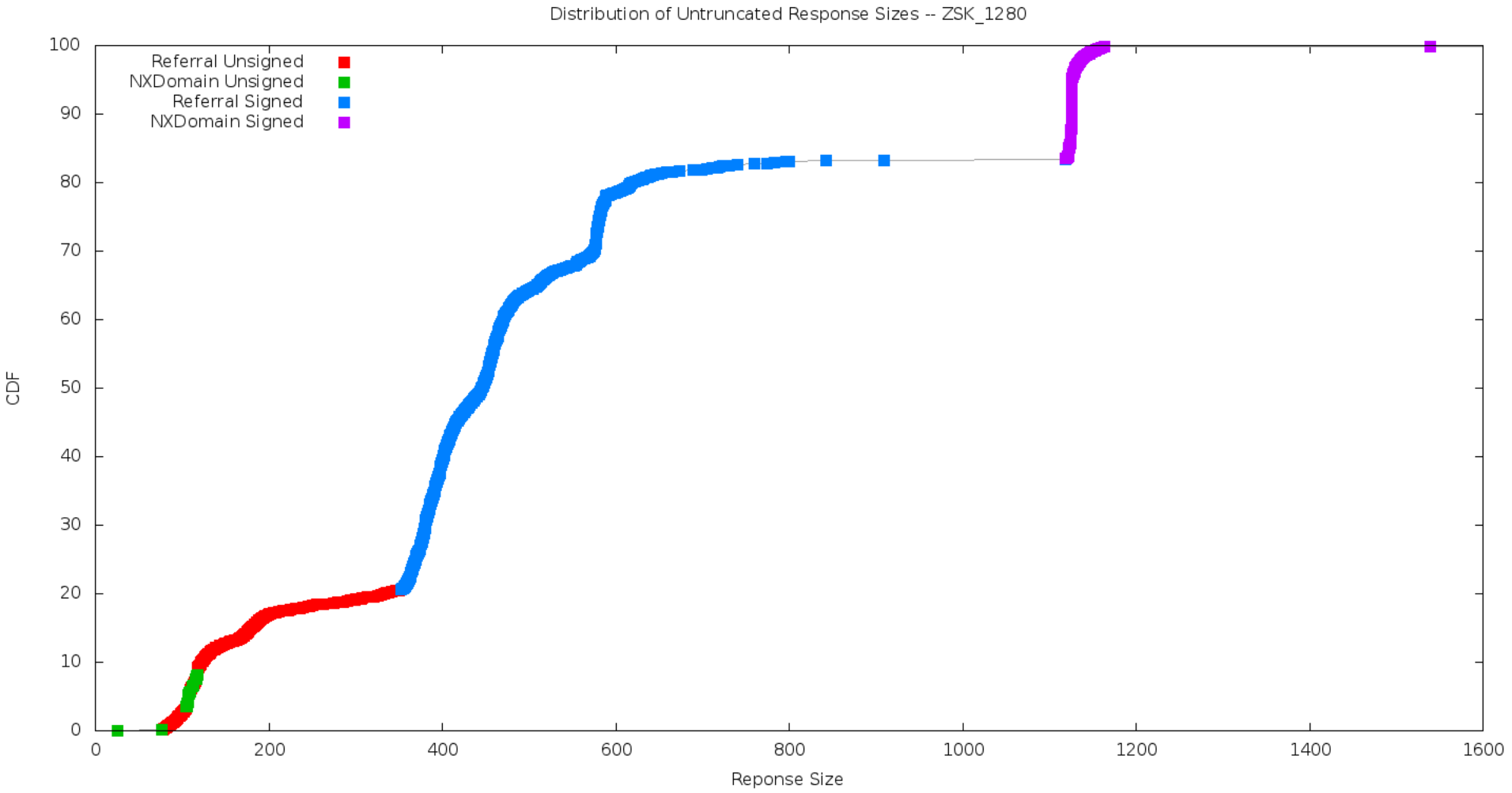
- ZSK Length Increase
- TTLs
- Cross-Zone Glue

ZSK Length Increase


DNSSEC Algorithms and Key Lengths used by TLDs 2018-10-08
key length (bits)
4096
3584
3072
2560
2048
1536
1024
512
0
RSASHA1
RSASHA1-NSEC3-SHA1
RSASHA256
RSASHA512
ECDSAP256
Other
ae
cg
ge
kn
mz
so
xn--90a3ac
mg
ky
akdn
bnpparibas
delta
gallup
info
latino
monster
phone
samsung
stockholm
xin
xn--h2breg3eve
hiv
app
berlin
cal
comsec
durban
foo
gmail
hotmail
jp
lexus
meet
net
online
protection
samsclub
sky
theatre
vanguard
xbox
xn--d1acj3b
xn--o3cw4h
za
airforce
baby
builders
catholic
clothing
credit
directory
events
flickr
gives
holdings
intel
land
luxury
money
olayan
pin
rehab
sandvik
singles
support
tips
uno
weatherchannel
xn--fct429k
xn--vhquv
blog
fit
london
shia
work
bauhaus
sap

ZSK Strength Increase

- Currently, all Verisign-operated TLDs have 1024-bit RSA ZSKs
  - Root has been operating with 2048-bit ZSK since Oct 2016
- TLD ZSKs to be increased to 1280-bit RSA
  - ARPA will be increased to 2048-bit
- Rationale: 1024-bit RSA deprecated for use in DNSSEC
- Gradual rollout per platform
  - Tentatively 2018-Q4 through 2019-Q4
- For NSEC3 zones, 1280-bit keys keep us under fragmentation limits
  - See next slides


Distribution of Untruncated Response Sizes -- ZSK_1280
Referral Unsigned
NXDomain Unsigned
Referral Signed
NXDomain Signed
CDF
Reponse Size
0
10
20
30
40
50
60
70
80
90
100
0
200
400
600
800
1000
1200
1400
1600

Time To Live

Time To Live Values

- Verisign-operated TLDs use 48-hour TTLs on delegation responses
- “’Twas always thus”
- Implemented a feature to change delegation TTL per TLD
- Considering lower TTLs for some low-volume TLDs
- If deployed, TTLs will be changed incrementally

Cross-Zone Glue

Cross-Zone Glue

- Currently a referral for a .COM name includes .NET glue records, and vice-versa
- Most implementations ignore this cross-zone glue
  - Google Public DNS does not
- In the future, .COM and .NET referrals will not include cross-zone glue
- Rationale:
  - Cross-zone glue largely ignored
  - Slightly smaller responses
  - Allows providers to use dynamically addressed name servers in .COM and .NET
- Expected to be deployed 2018-Q4

VERISIGN®