Some DNSSEC Measurements

Geoff Huston AM

Chief Scientist, APNIC

Measuring DNSSEC Validation

- Clients who are located behind DNS Recursive Resolvers that perform DNSSEC validation
    - Using ECDSA-P-256 as the crypto algorithm

- We are NOT measuring individual recursive resolvers, nor performing a census of DNSSEC-signed names

Measuring DNSSEC Validation

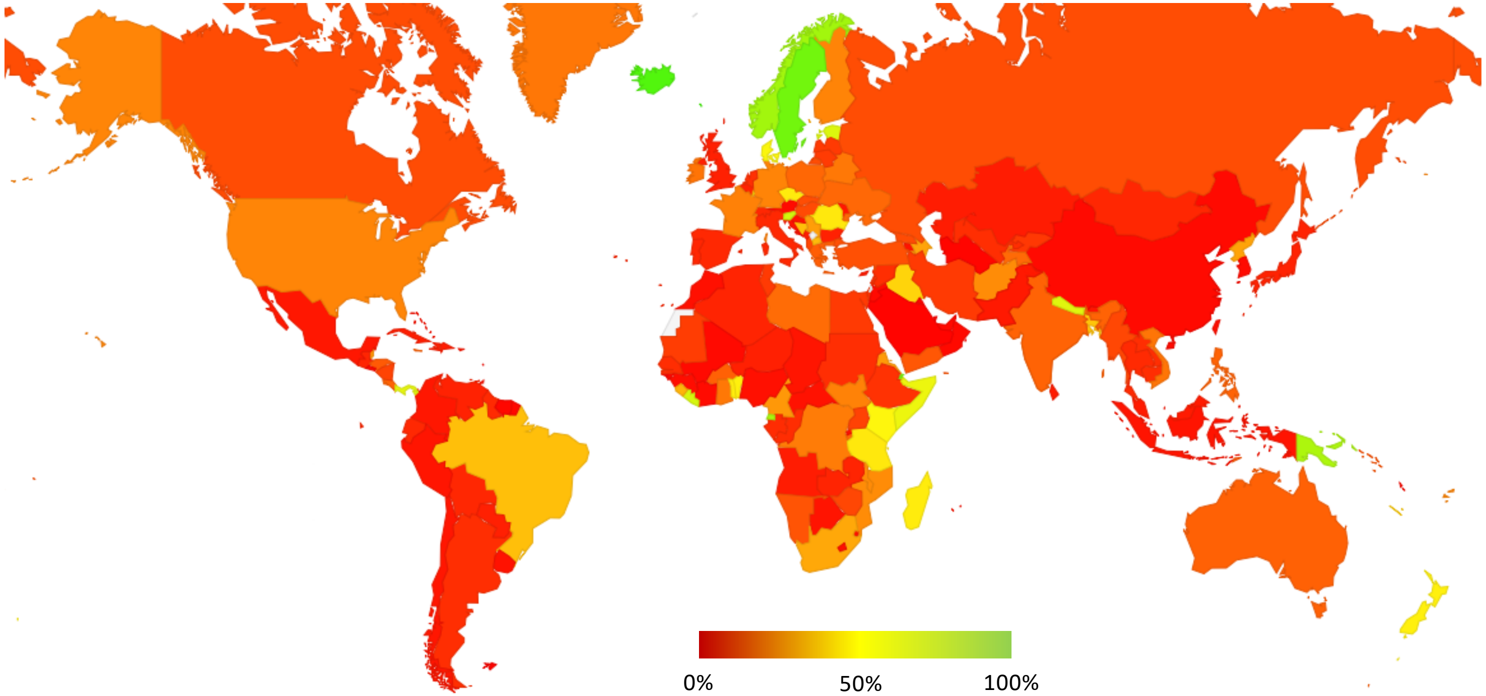
We are NOT measuring individual recursive resolvers:

- It’s quite a challenge to isolate the DNSSEC validation behaviour of a recursive resolver from authoritative server’s query logs.
- If the aim is to measure the user impact here, then it makes more sense to measure the number of users who use DNSSEC validating resolvers rather than the resolvers themselves

We are NOT performing a census of DNSSEC-signed names:

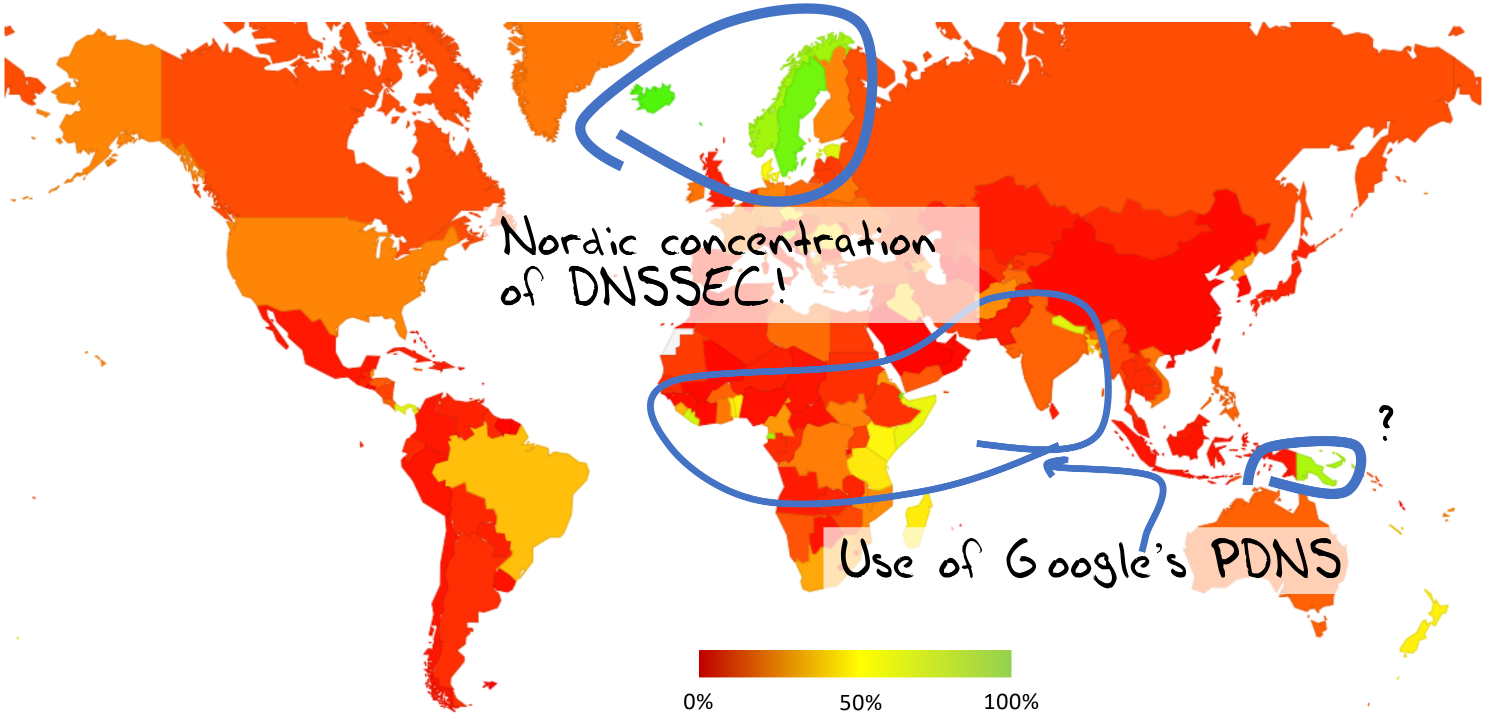
- This has its own challenges relating to zone enumeration in the DNS, and we are not undertaking that exercise here!

The Global Validation Picture in 2016



http://stats.labs.apnic.net/dnssec

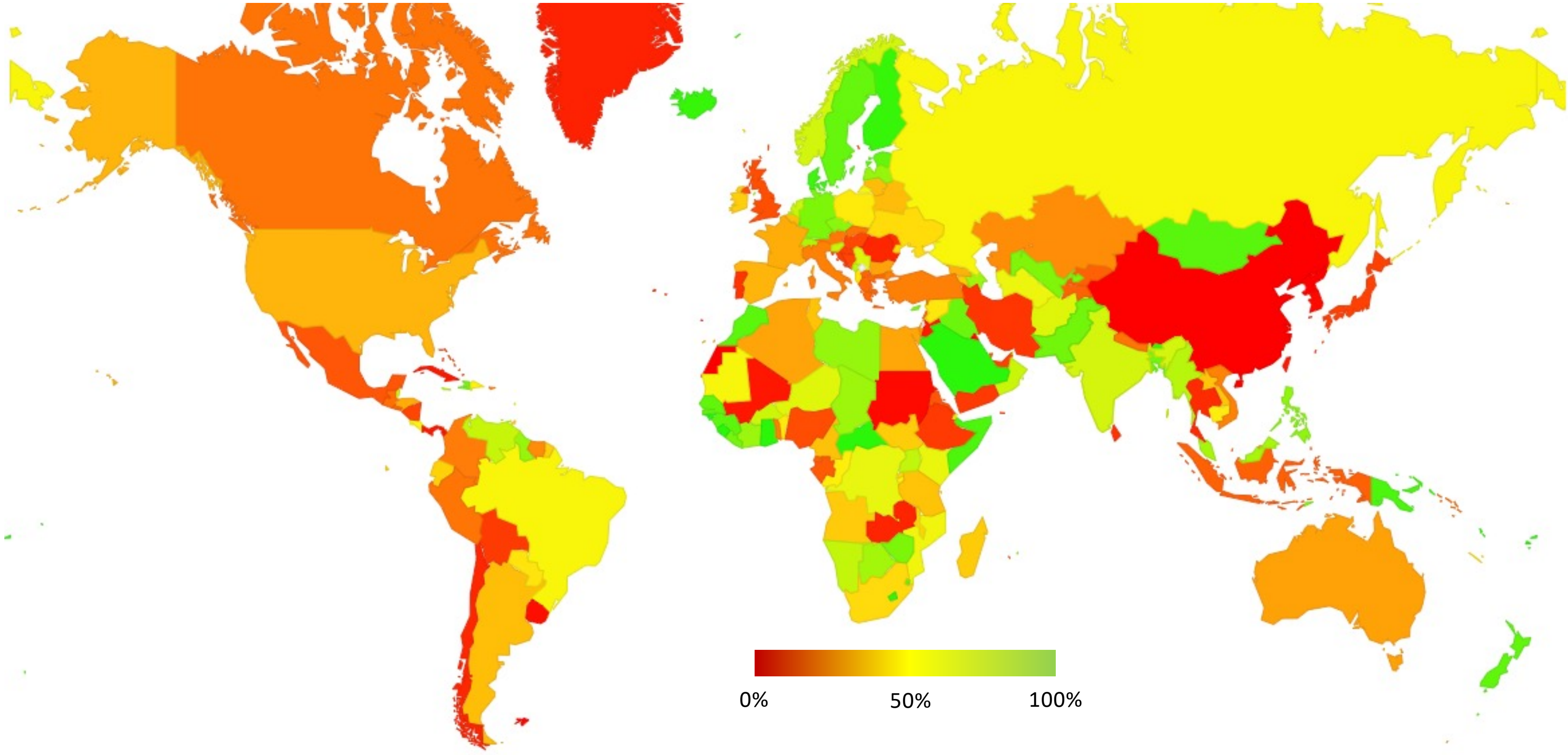
The Global Validation Picture in 2016



÷ of users in a country that use DNSSEC validating resolvers

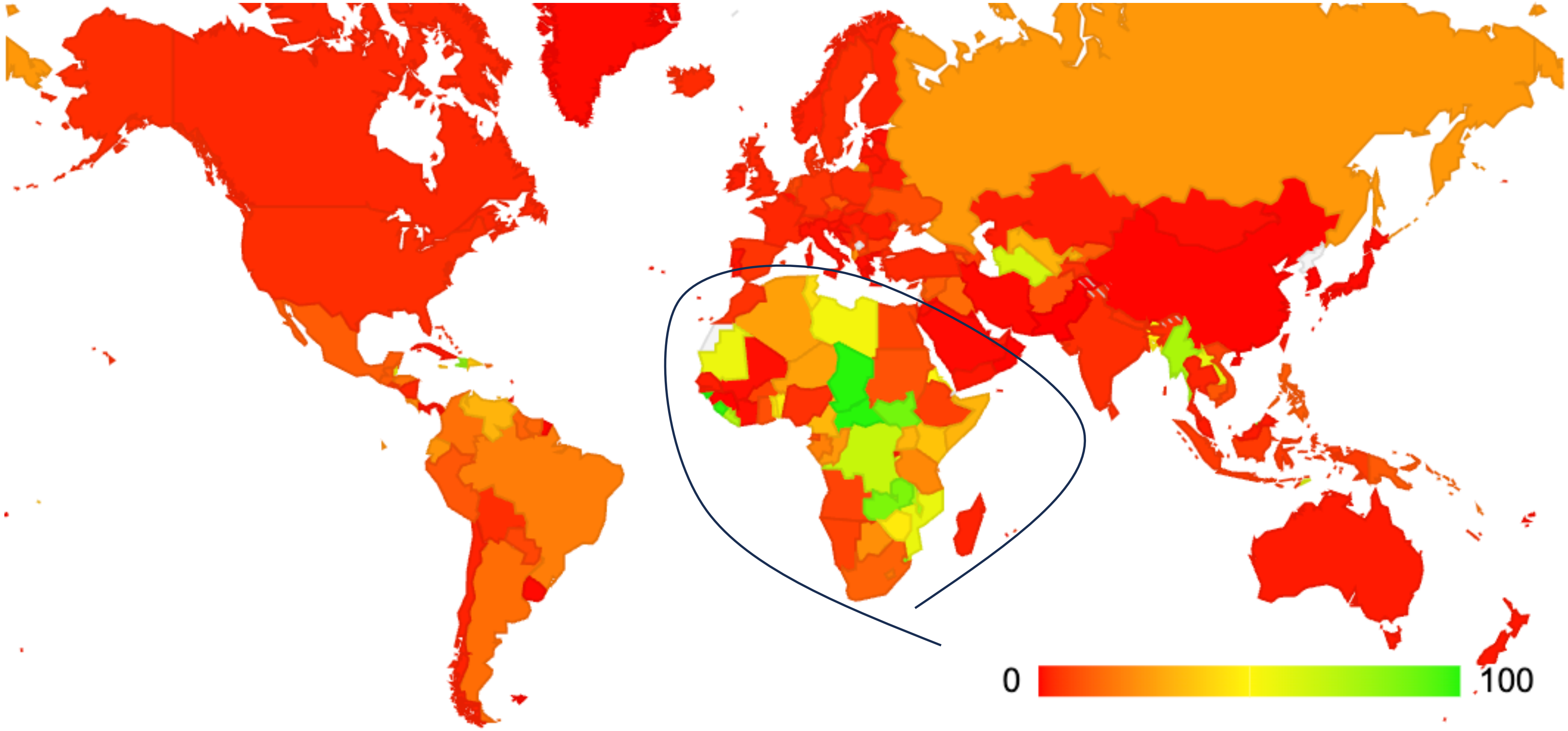
http://stats.labs.apnic.net/dnssec

DNSSEC Validation in 2025



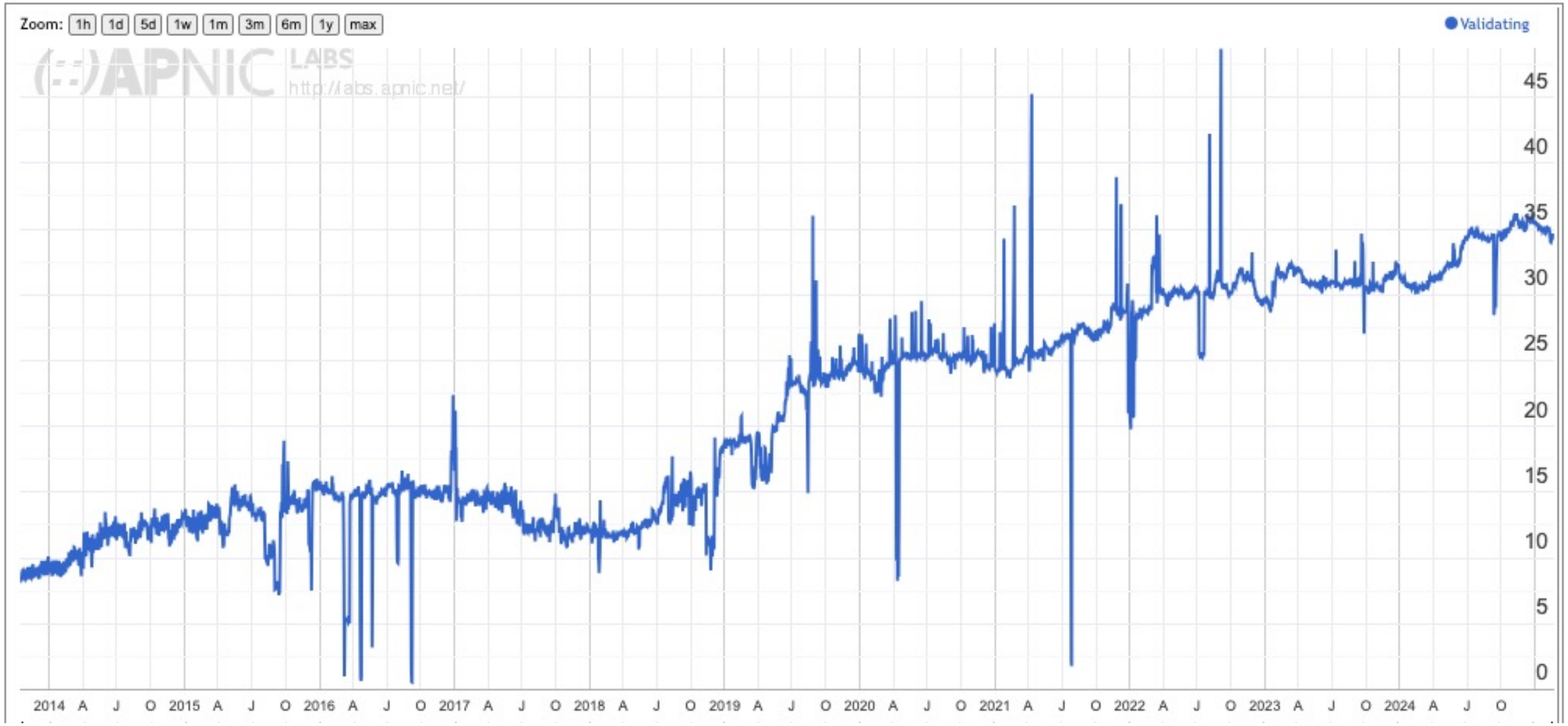
Is Google's 8.8.8.8 important?

Use of googlepdns Resolvers within each Economy



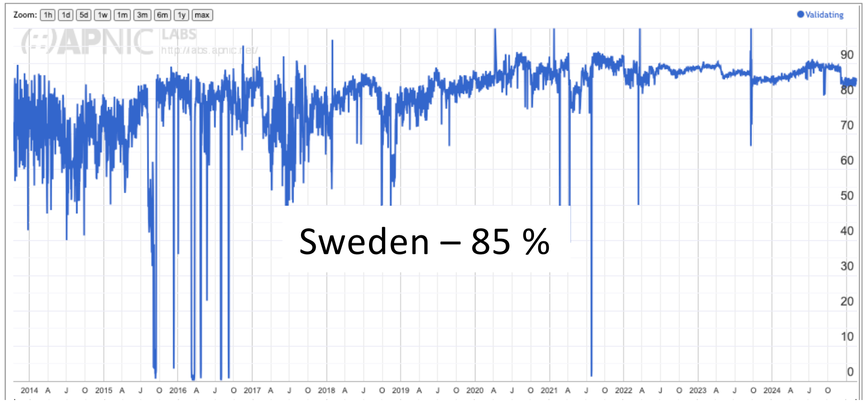
The Global Picture

Use of DNSSEC Validation for World (XA)



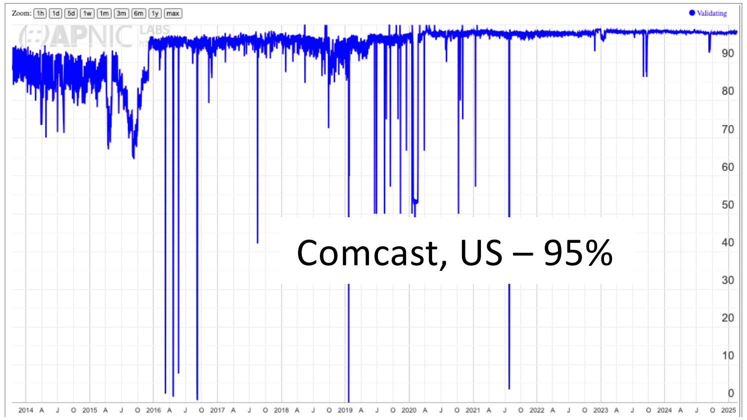
2014 **2018** **2022**

Some have been Validating for many years



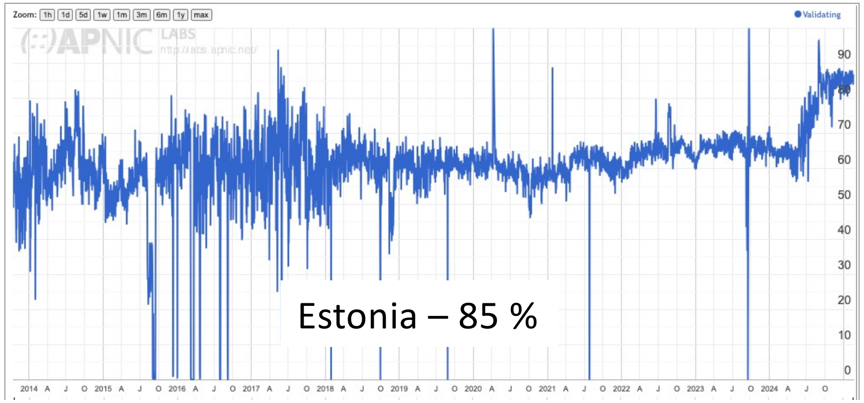
Sweden – 85 %

DNSSEC Per-Country Deployment for AS7922: COMCAST-7922, United States of America (US)

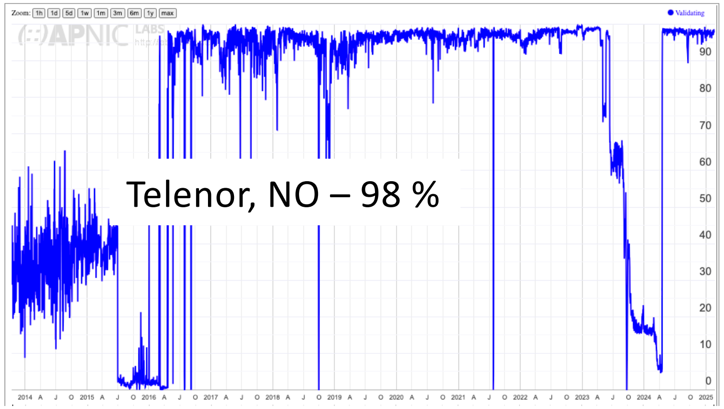


Comcast, US – 95%

Use of DNSSEC Validation for Estonia (EE)



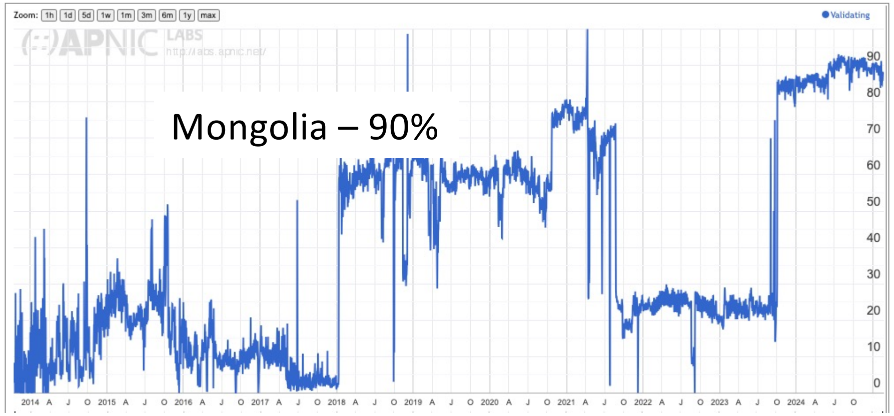
Estonia – 85 %



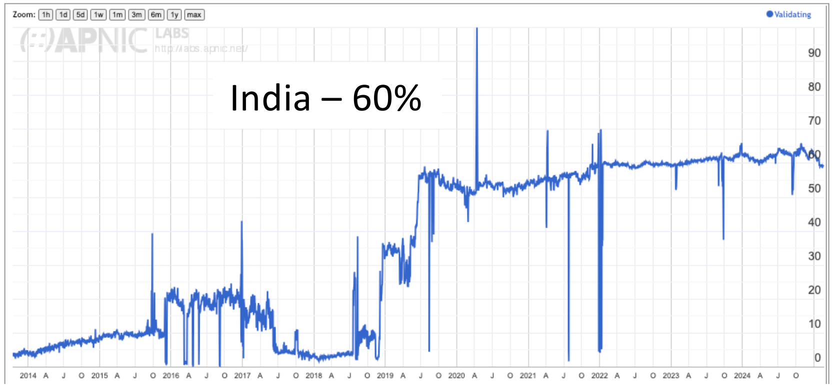
Telenor, NO – 98 %

Turning it ON

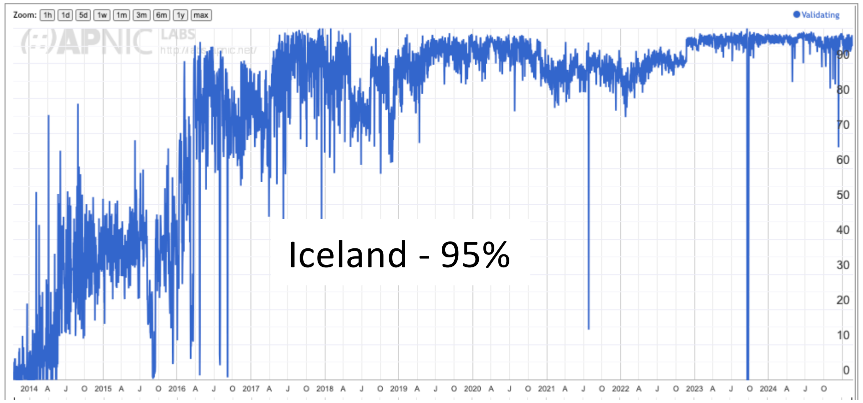
Use of DNSSEC Validation for Mongolia (MN)


Mongolia – 90%

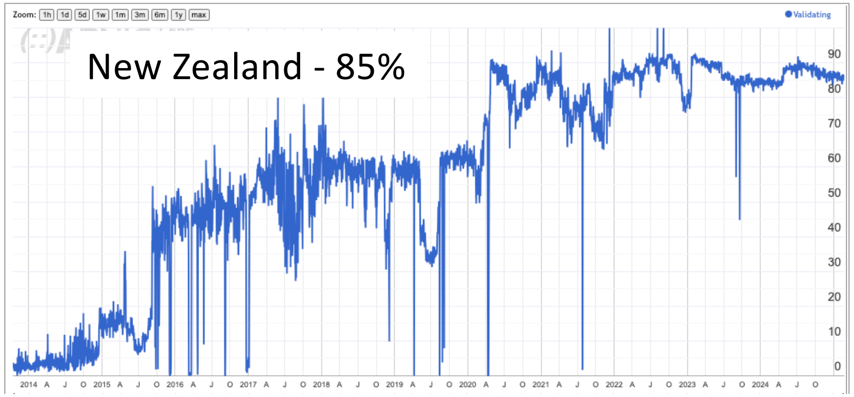
Use of DNSSEC Validation for India (IN)


India – 60%

Use of DNSSEC Validation for Iceland (IS)

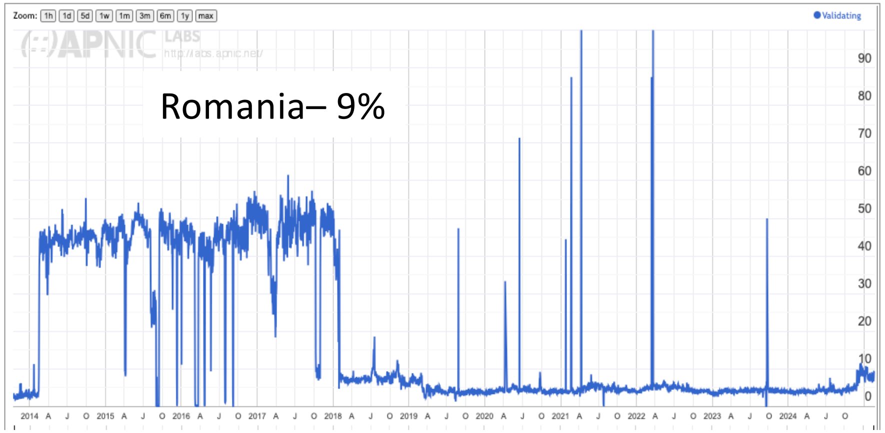

Iceland - 95%

Use of DNSSEC Validation for New Zealand (NZ)


New Zealand - 85%

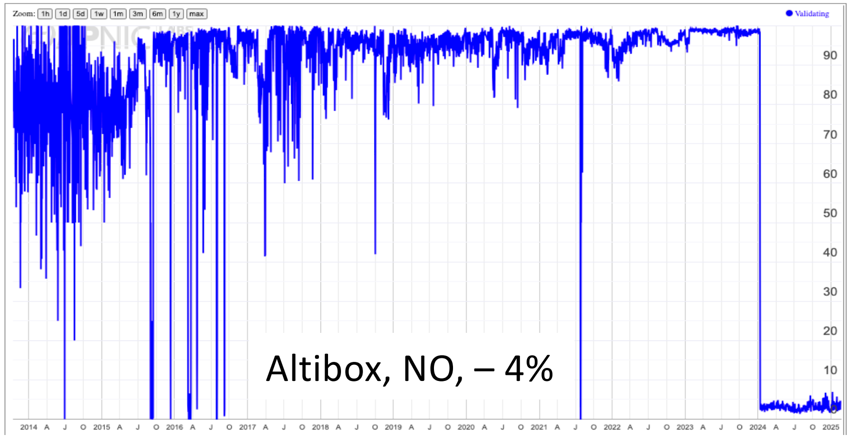
Turning it OFF

Use of DNSSEC Validation for Romania (RO)



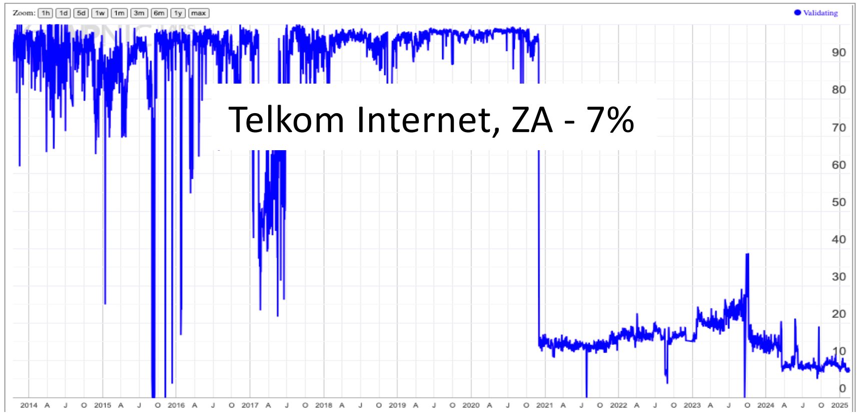
Romania– 9%

DNSSEC Per-Country Deployment for AS29695: ALTIBOX_AS Norway, Norway (NO)



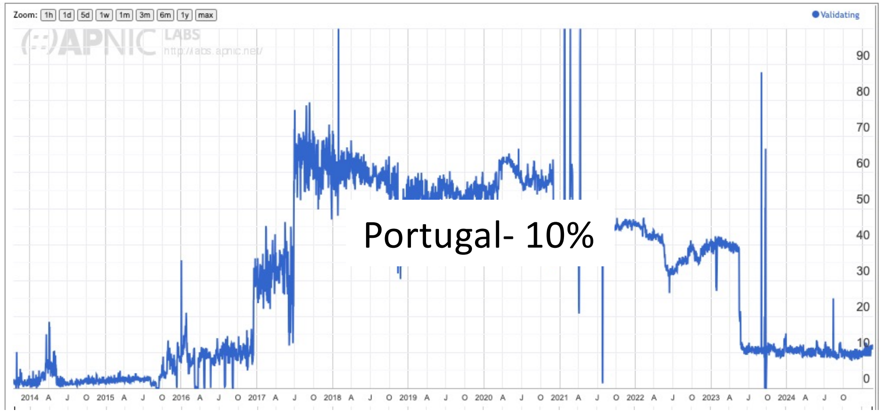
Altibox, NO, – 4%

DNSSEC Per-Country Deployment for AS37457: Telkom-Internet, South Africa (ZA)



Telkom Internet, ZA - 7%

Use of DNSSEC Validation for Portugal (PT)



Portugal- 10%

It's a mixed picture

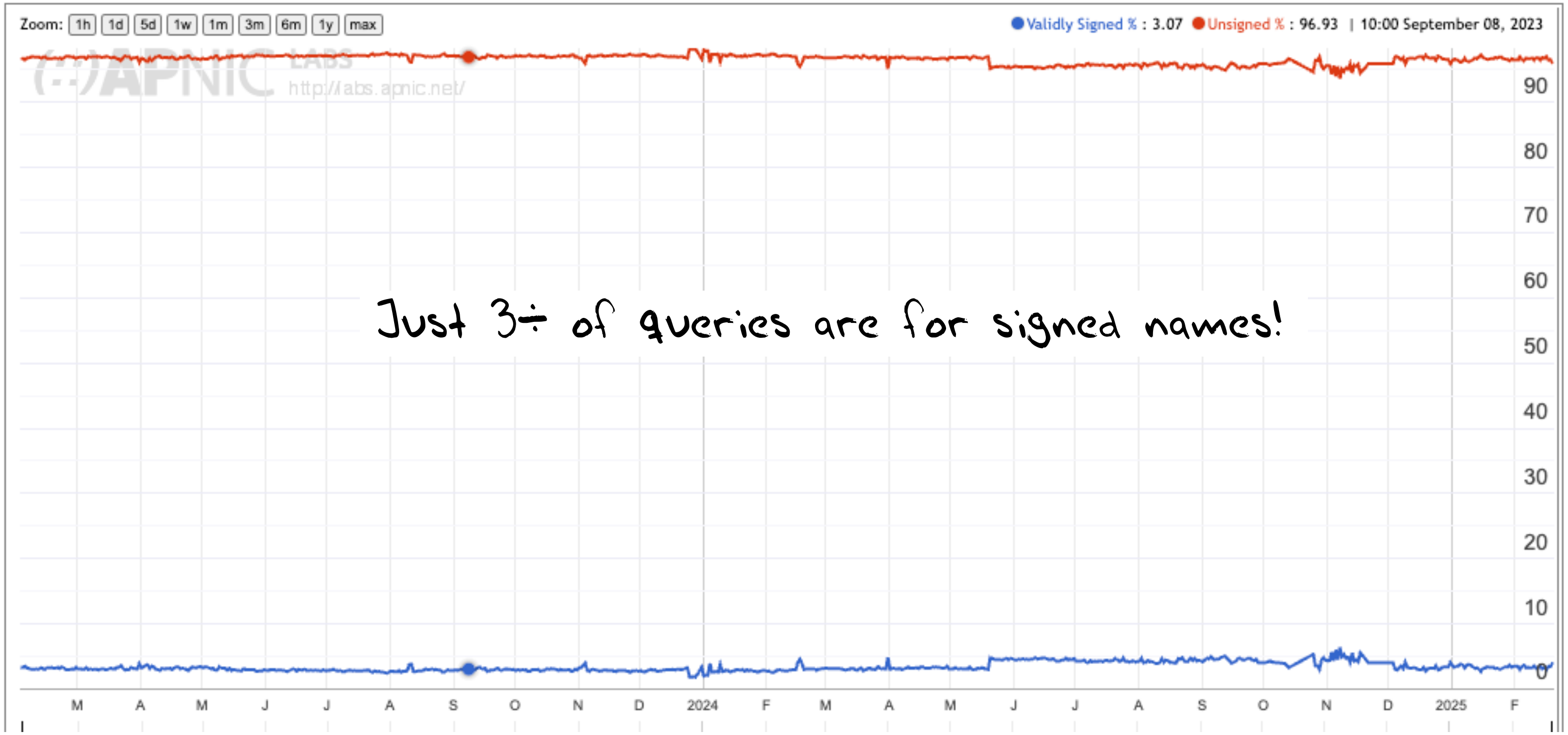
- Some ISPs have had DNSSEC validation enabled for more than a decade
- Some are still turning DNSSEC validation on
- While others are turning it off!
- The case to support DNSSEC validation in recursive resolvers is unclear for some ISPs

What about Measuring DNSSEC-signed Domains?

- It’s challenging to assemble a census of all domain names
- But there are other measurements that make sense from a user’s perspective
- One is the query-weighted view of domain-signing:
  - **What proportion of DNS queries are for domain names that are DNSSEC-signed?**

  - At APNIC we can answer this using the query data from Cloudflare’s 1.1.1.1 recursive resolution service

What about Measuring DNSSEC-signed Domains?



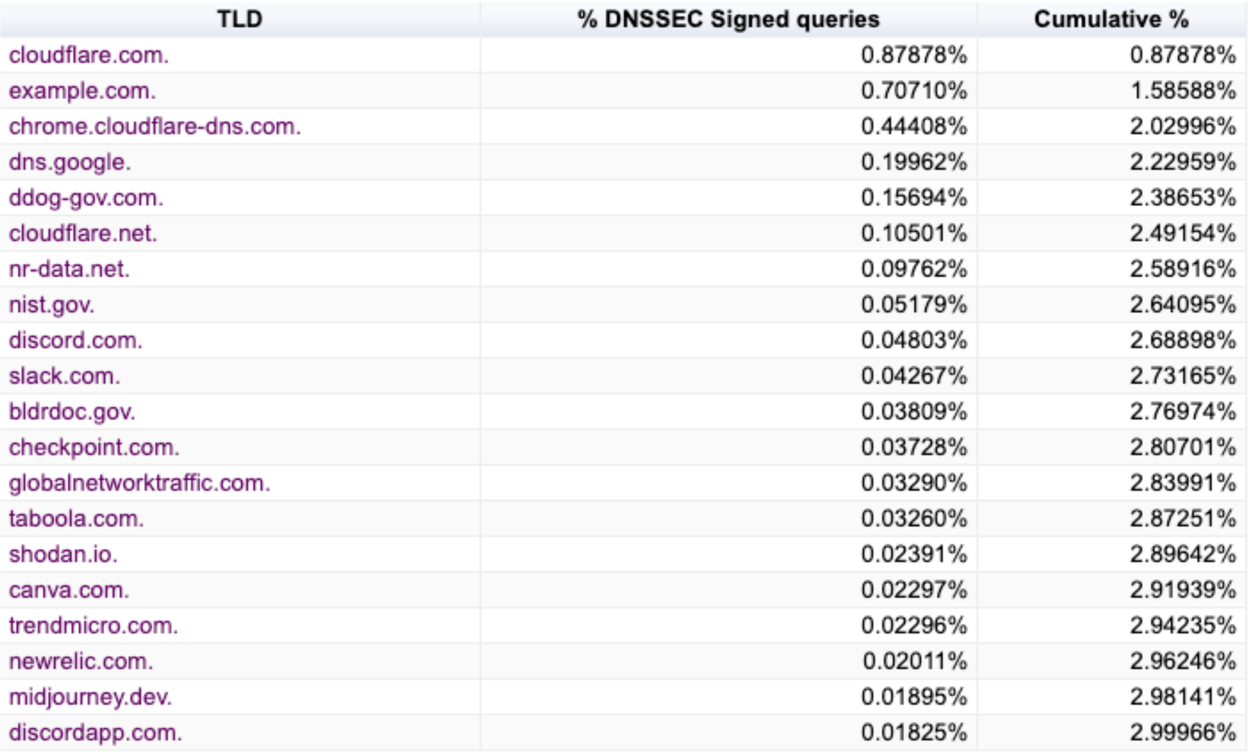
Just 3% of queries are for signed names!

Non-DNSSEC-signed names

% of queries

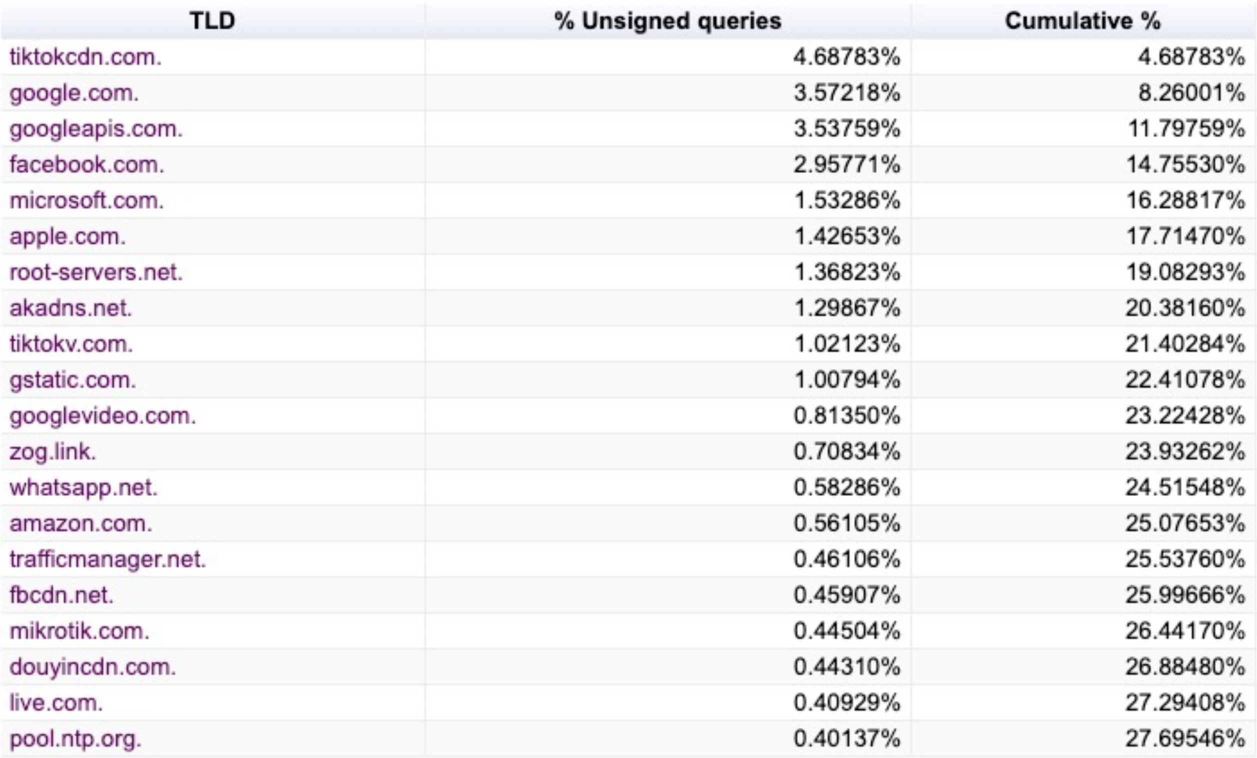
DNSSEC-signed names

Signed Domains



TLD	% DNSSEC Signed queries	Cumulative %
cloudflare.com.	0.87878%	0.87878%
example.com.	0.70710%	1.58588%
chrome.cloudflare-dns.com.	0.44408%	2.02996%
dns.google.	0.19962%	2.22959%
ddog-gov.com.	0.15694%	2.38653%
cloudflare.net.	0.10501%	2.49154%
nr-data.net.	0.09762%	2.58916%
nist.gov.	0.05179%	2.64095%
discord.com.	0.04803%	2.68898%
slack.com.	0.04267%	2.73165%
bldrdoc.gov.	0.03809%	2.76974%
checkpoint.com.	0.03728%	2.80701%
globalnetworktraffic.com.	0.03290%	2.83991%
taboola.com.	0.03260%	2.87251%
shodan.io.	0.02391%	2.89642%
canva.com.	0.02297%	2.91939%
trendmicro.com.	0.02296%	2.94235%
newrelic.com.	0.02011%	2.96246%
midjourney.dev.	0.01895%	2.98141%
discordapp.com.	0.01825%	2.99966%

Unsigned Domains



TLD	% Unsigned queries	Cumulative %
tiktokcdn.com.	4.68783%	4.68783%
google.com.	3.57218%	8.26001%
googleapis.com.	3.53759%	11.79759%
facebook.com.	2.95771%	14.75530%
microsoft.com.	1.53286%	16.28817%
apple.com.	1.42653%	17.71470%
root-servers.net.	1.36823%	19.08293%
akadns.net.	1.29867%	20.38160%
tiktokv.com.	1.02123%	21.40284%
gstatic.com.	1.00794%	22.41078%
googlevideo.com.	0.81350%	23.22428%
zog.link.	0.70834%	23.93262%
whatsapp.net.	0.58286%	24.51548%
amazon.com.	0.56105%	25.07653%
trafficmanager.net.	0.46106%	25.53760%
fbcdn.net.	0.45907%	25.99666%
mikrotik.com.	0.44504%	26.44170%
douyincdn.com.	0.44310%	26.88480%
live.com.	0.40929%	27.29408%
pool.ntp.org.	0.40137%	27.69546%

What's this saying?

- Very popular DNS names are, on the whole, unsigned
- The risks of DNSSEC-related service outage appear to weigh more heavily in the mind of the operators of these heavily used names than the risks of attacks on the DNS resolution of these names
- All these names have X.509 domain name certificates in any case, which is a significant barrier to service impersonation attacks – it is often challenging to identify the incremental benefit that DNSSEC-signing enables as a consequence

Thanks !