DNSSEC: worth adding to your cybersecurity strategy

THNIC DNSSEC Seminar
**21 November 2024 – Bangkok - Thailand**

Champika Wijayatunga
Technical Engagement Sr. Manager (APAC)

ICANN

# DNS contains a wealth of data about your systems

- Your organization's domain names – **xyz.th**
- Your organization's individual host names – **host.xyz.th**
- IP addresses
- Mail server data (MX records) – **mail.xyz.th**
- Database locations – **db0.xyz.th**
- etc

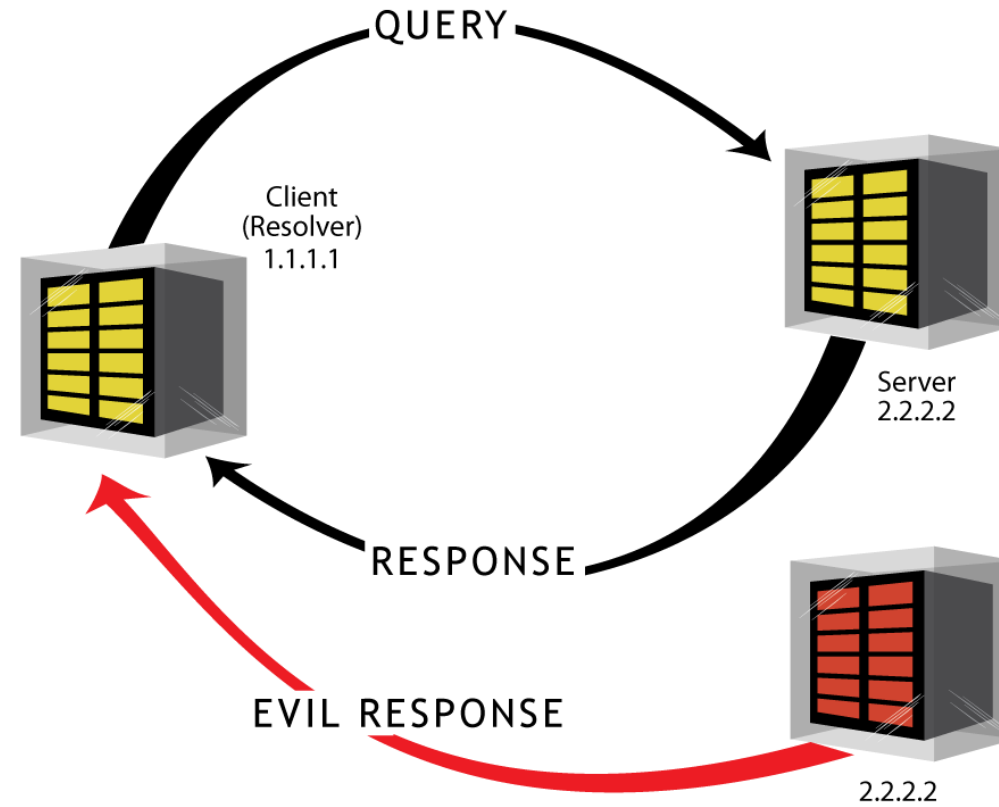**Protecting DNS is extremely important**

DNS Components at a Glance
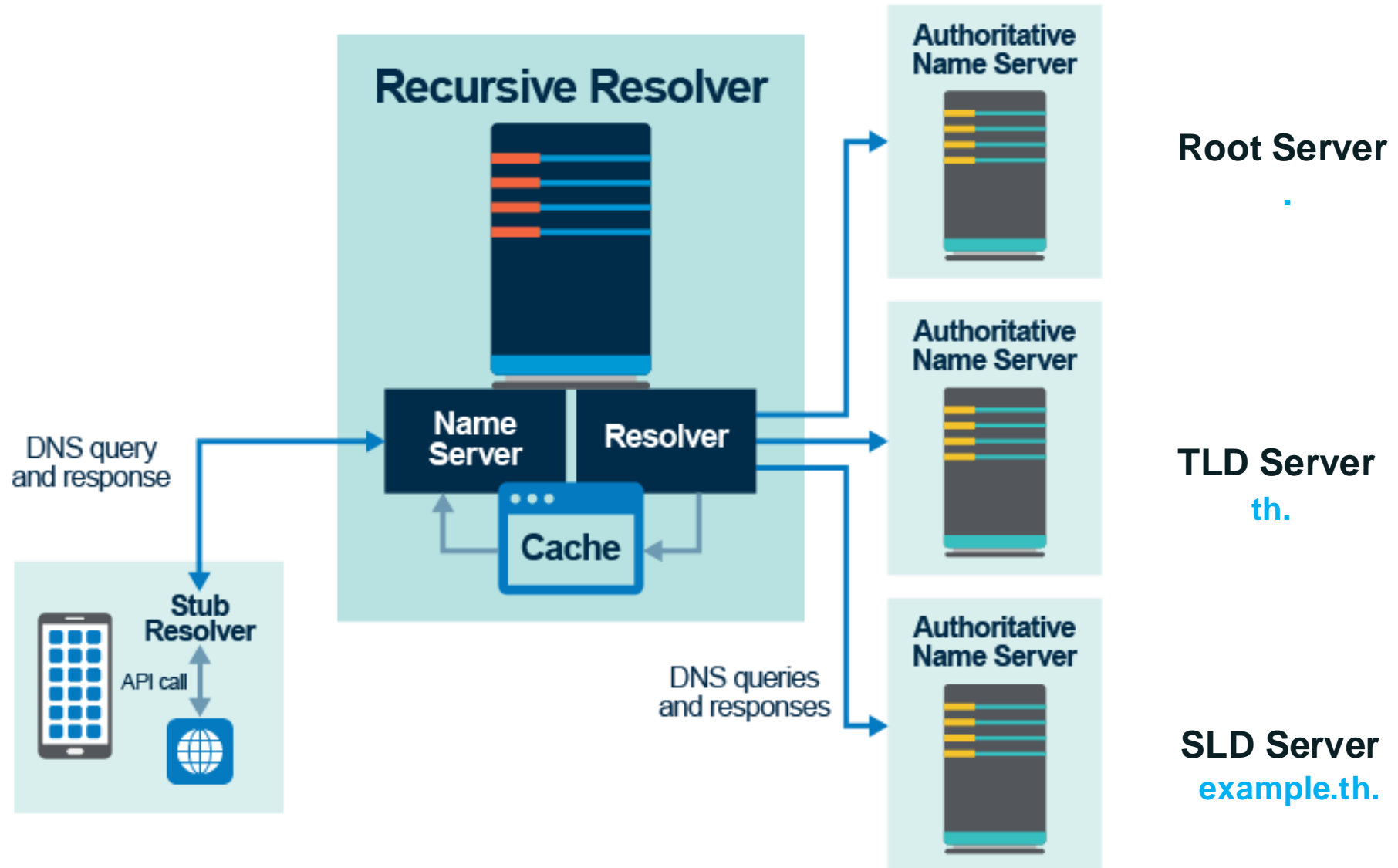
DNS and Lack of Security

DNS and Lack of Security

QUERY

Client
(Resolver)
1.1.1.1

Server
2.2.2.2

RESPONSE
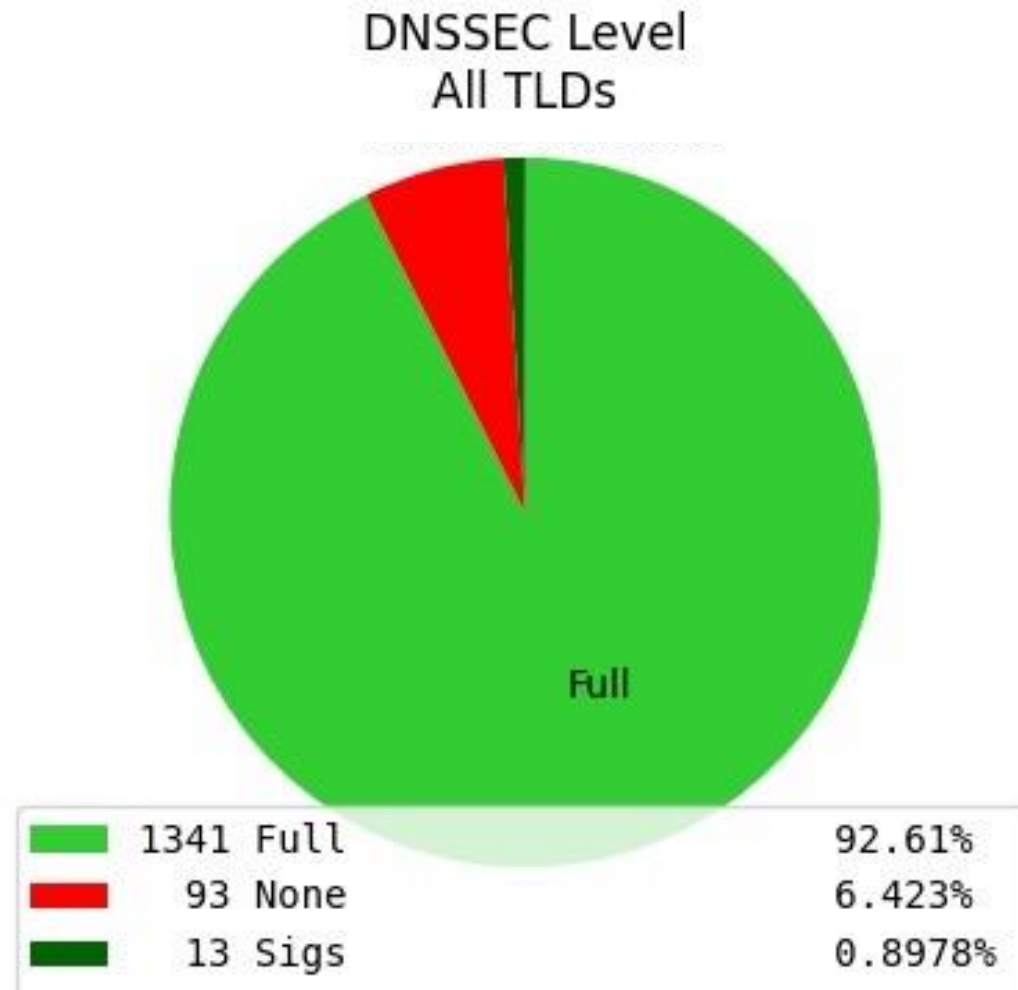
EVIL RESPONSE

2.2.2.2
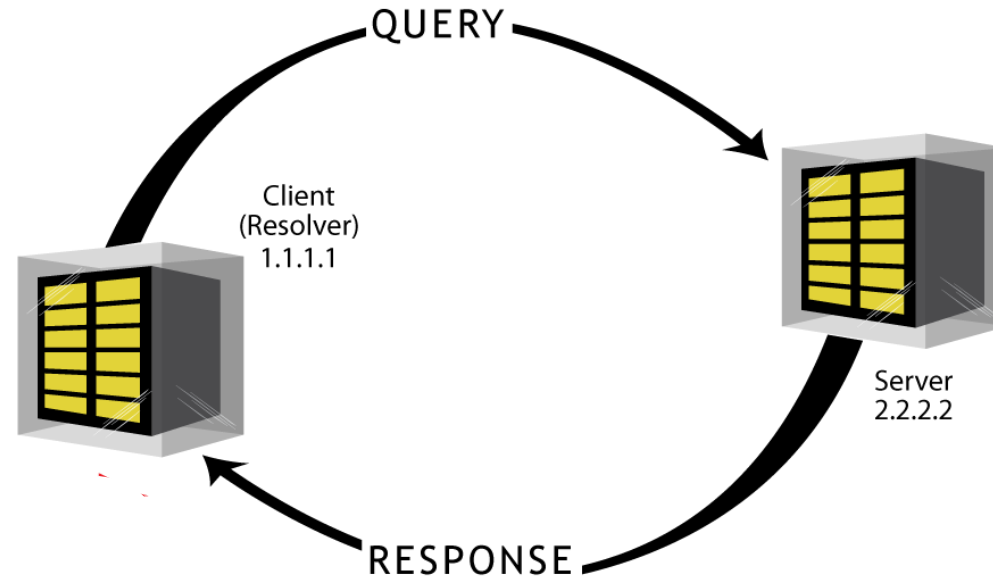
DNSSEC

What DNSSEC Does Vs what it doesn't do

- DNSSEC uses public-key cryptography and digital signatures to provide:
  - **Data Origin Authenticity :** "Did this response really come from the *example.in* zone?"
  - **Data Integrity:** "Did an attacker (e.g., a man in the middle) modify the data in this response since the data was originally signed?"

- DNSSEC offers **protection against spoofing** of DNS data

- DNSSEC **does not provide** any confidentiality for DNS data:
  - no encryption
  - Man in the middle-attack
  - DNS over HTTPS (DoH- RFC 8484) and DNS over TLS (DoT – RFC 7858) – more suited

- DNSSEC **does not address** attacks against DNS software: DDoS; BCP38

DNSSEC – Chain of Keys and Propagation of Trust

Request comes in for "WWW.EXAMPLE.COM"

End User

DNSSEC

192.0.2.103
"WWW.EXAMPLE.COM"

Recursive Name Server

One of Root Servers

One of .COM's Name Servers

One of EXAMPLE.COM's Name Servers

DNSSEC Deployment - All TLDs

DNSSEC Level
All TLDs

Full

🟩	1341 Full	92.61%
🟥	93 None	6.423%
🟩	13 Sigs	0.8978%

Source: ICANN OCTO

DNSSEC Deployment - gTLDs

Number of gTLDs by DNSSEC status

Green: DNSSEC operational (DNSKEY in TLD zone + DS in root zone)

Yellow: Partial signed (DNSKEY in TLD zone without DS in root zone)

Other: No DNSSEC (No DNSKEY in TLD zone)

Number of involved gTLDs in the chart center

1,138

active
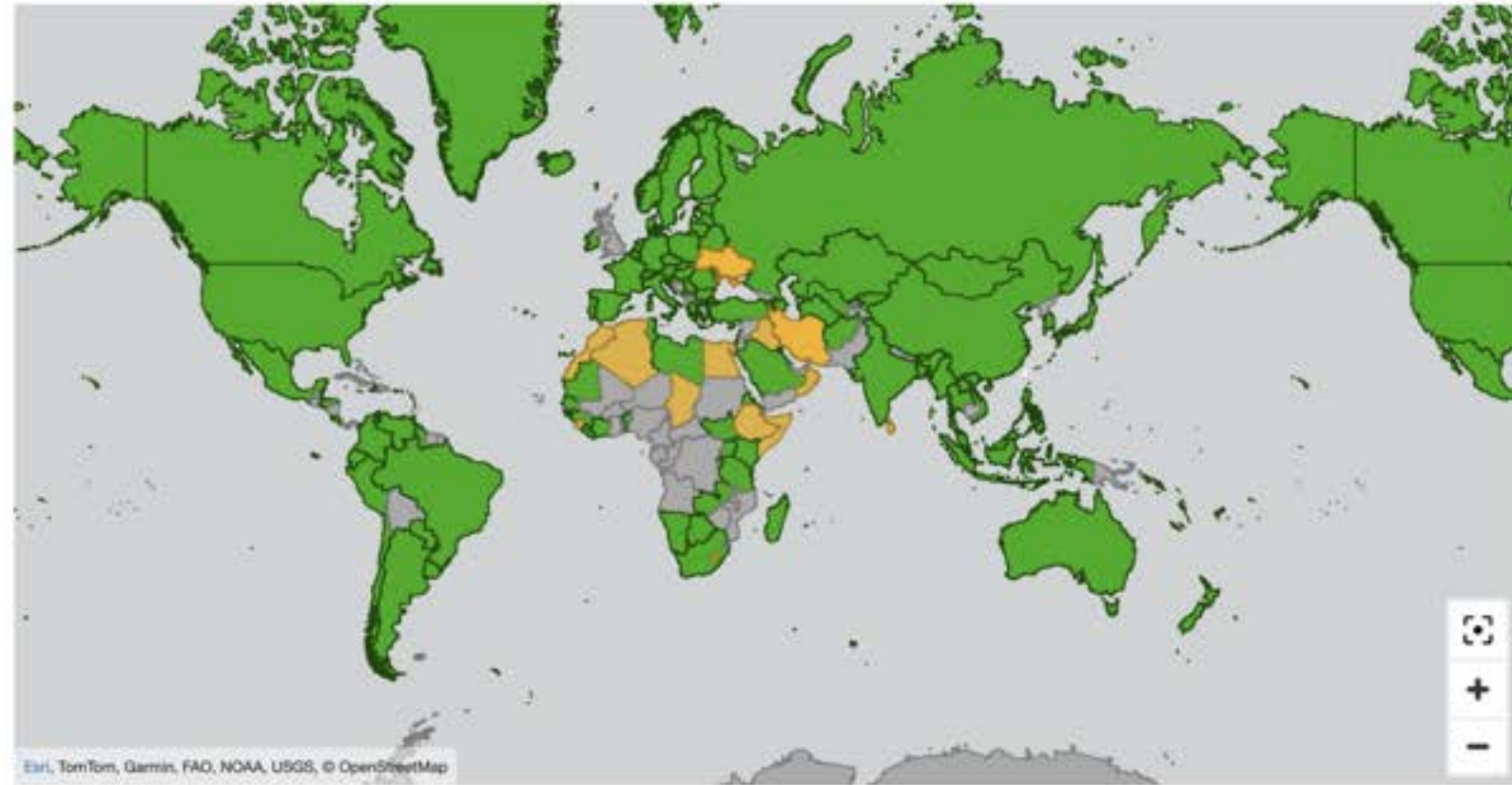1,138 (100%)

Source: ICANN OCTO

DNSSEC Deployment – ccTLDs (including IDNs)

DNSSEC status (world map) of selected ccTLDs

Green: DNSSEC operational (DNSKEY in TLD zone + DS in root zone)
Yellow: Partial signed (DNSKEY in TLD zone without DS in root zone)
Grey: No DNSSEC (No DNSKEY in TLD zone)

Esri, TomTom, Garmin, FAO, NOAA, USGS, © OpenStreetMap

DNSSEC status distribution for selected ccTLDs

Green: DNSSEC operational (DNSKEY in TLD zone + DS in root zone)
Yellow: Partial signed (DNSKEY in TLD zone without DS in root zone)
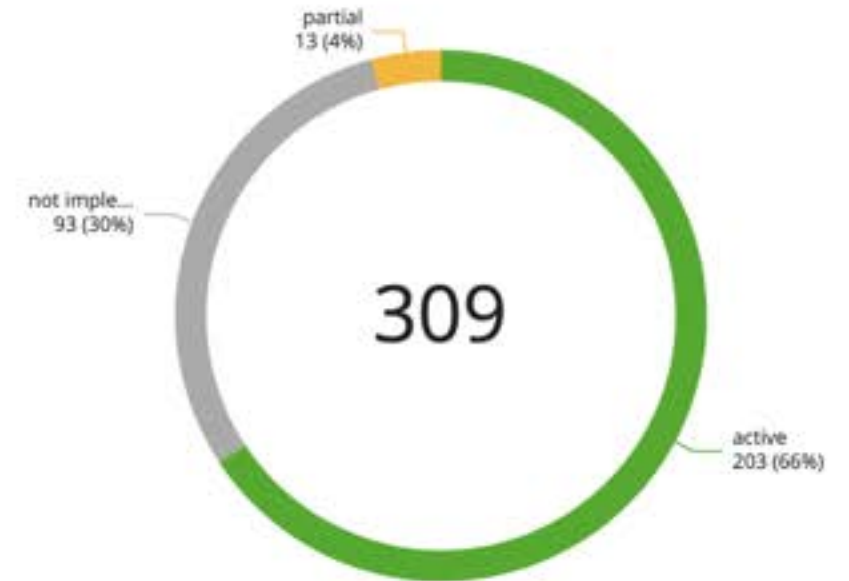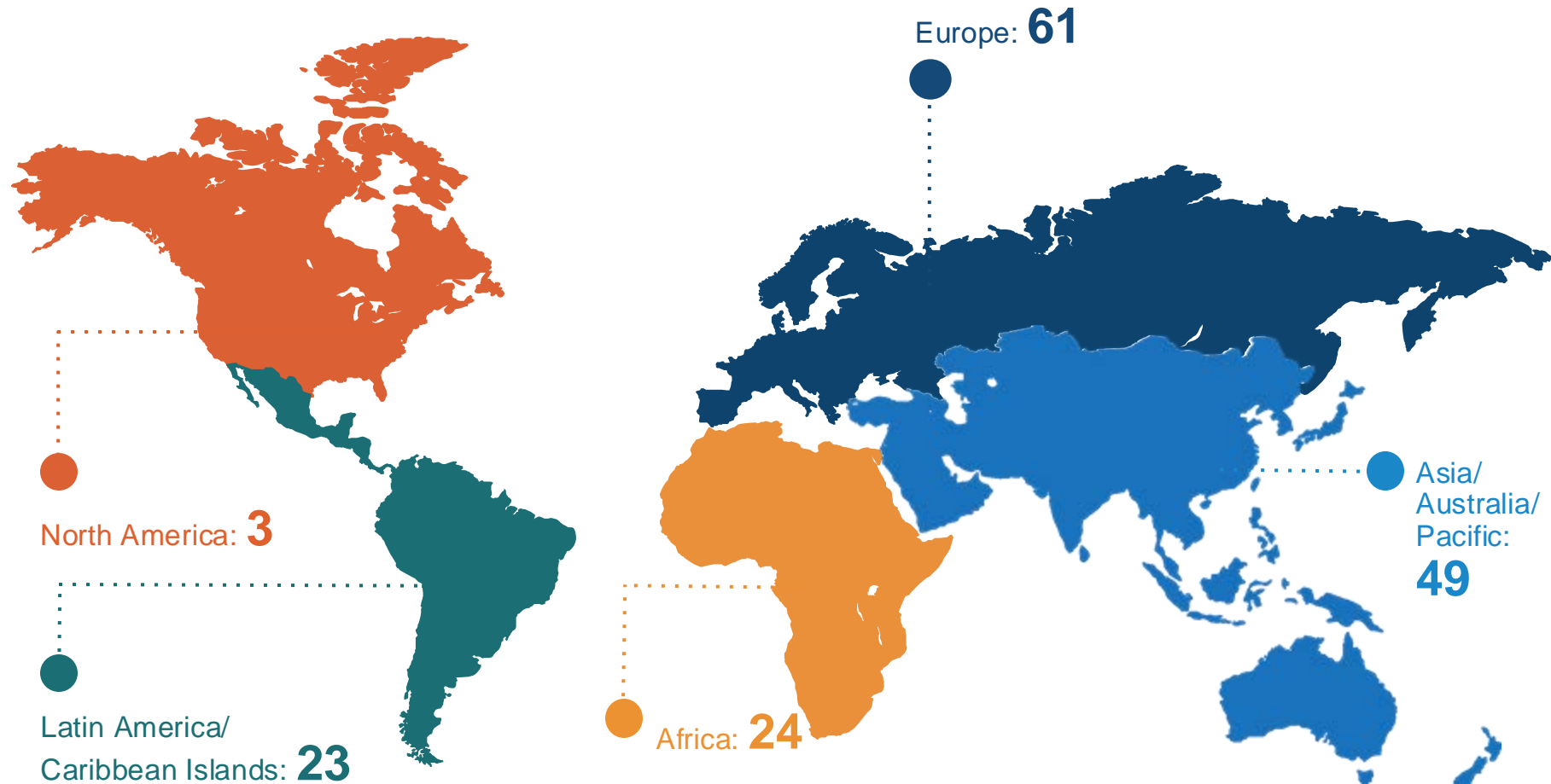**Grey**: No DNSSEC (No DNSKEY in TLD zone)
Number of involved ccTLDs in the chart center

partial
13 (4%)

not imple...
93 (30%)

309

active
203 (66%)

Source: ICANN OCTO

DNSSEC Deployment – ccTLDs based on regions

Europe: **61**

North America: **3**

Latin America/
Caribbean Islands: **23**

Africa: **24**

Asia/
Australia/
Pacific:
49

Based on ICANN Geographic Regions: https://meetings.icann.org/en/regions

DNSSEC Deployment – Thailand (ccTLD including IDNs)

DNSSEC status distribution for selected ccTLDs

Green: DNSSEC operational (DNSKEY in TLD zone + DS in root zone)

Yellow: Partial signed (DNSKEY in TLD zone without DS in root zone)

Grey: No DNSSEC (No DNSKEY in TLD zone)
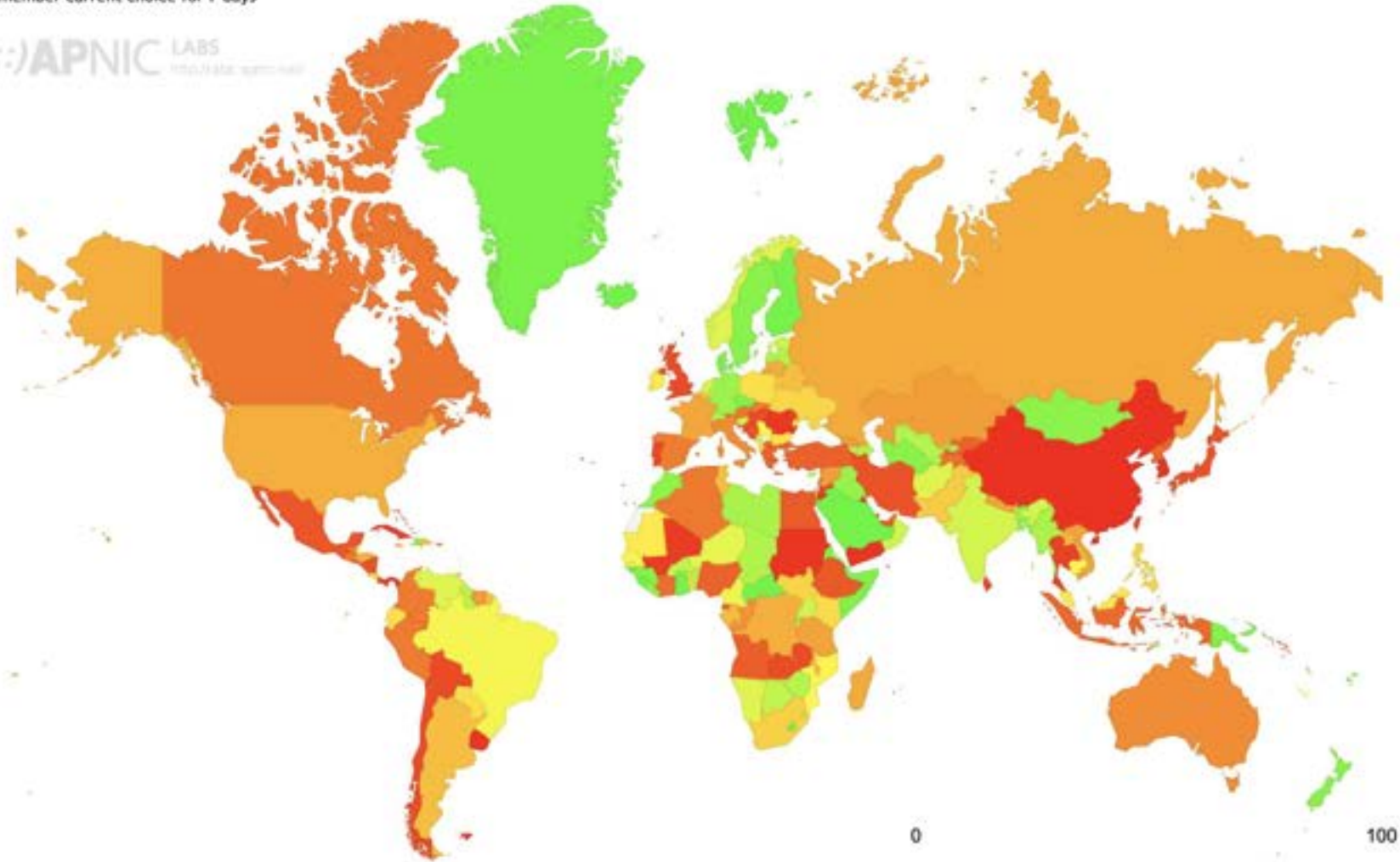
Number of involved ccTLDs in the chart center

2

active
2 (100%)

State of DNSSEC Validation - Global

DNSSEC Validation Rate by country (%)

Click here for a zoomable map
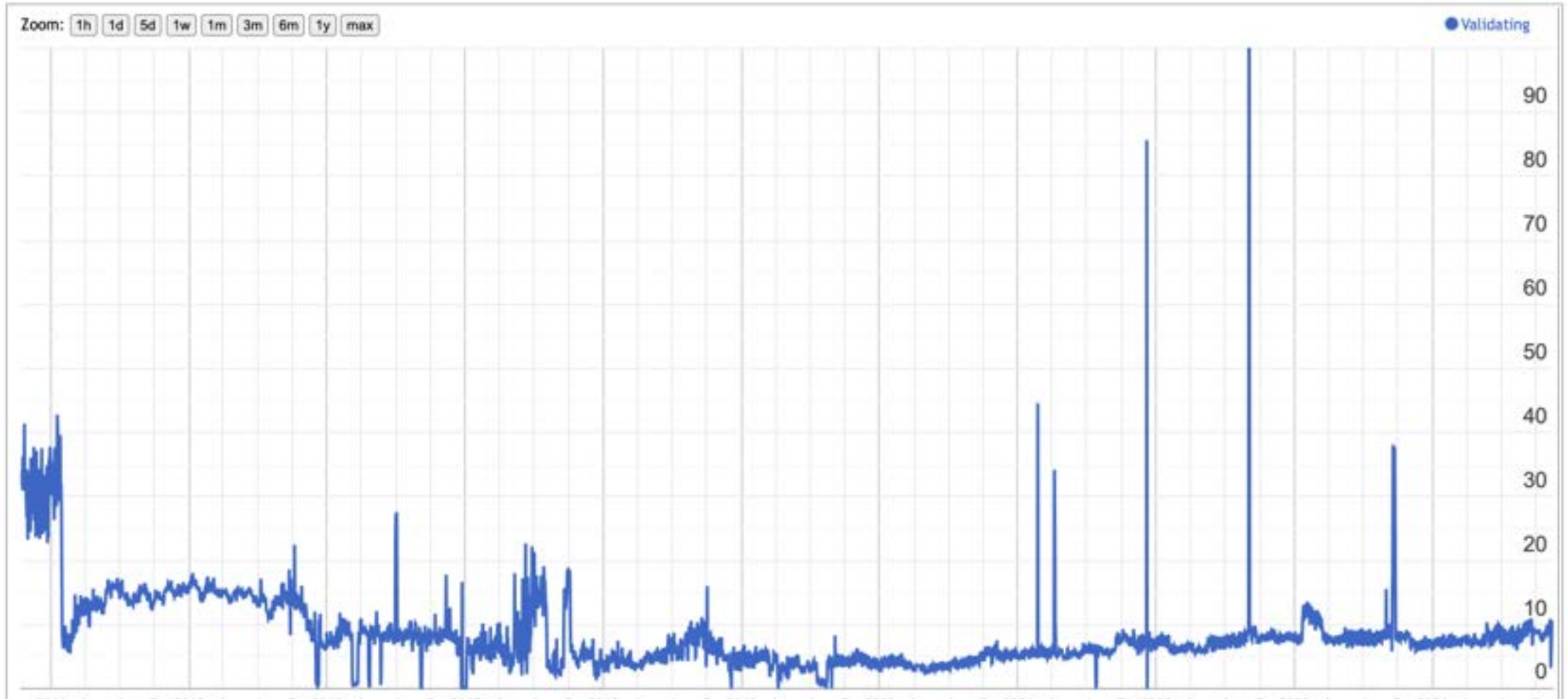☐ Remember current choice for 7 days

APNIC LABS

0   100

Source: APNIC Labs

State of DNSSEC Validation

Region	DNSSEC Validates
World	34.97%
Oceania	44.97%
Europe	44.36%
Africa	40.99%
Americas	35.98%
Asia	31.40%
Thailand	8.98%

Source: APNIC Labs

State of DNSSEC Validation - Thailand

Source: APNIC Labs

What you can do

- **Registries/Registrars/DNS Operators**
  - Offer DNSSEC services to registrants
- **For Companies, Financial Institutions etc.**
  - Sign your corporate domain names
  - Enable DNSSEC validation on corporate DNS resolvers
- **Internet Service Providers (ISPs)**
  - Enable DNSSEC validation on ISP resolvers
- **Governments, Policy makers**
  - Encourage DNSSEC compliance
- **For Users**
  - Request ISP to turn on validation on their DNS resolvers
- **For All**
  - Awareness about DNSSEC, training and education

Engage with ICANN – Thank You and Questions

One World, One Internet

ICANN

Visit us at **icann.org**   Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann