DNSSEC Validation

And why it matters…

Yazid Akanho

A presentation to Somalia NOG

28 Oct. 2021

ICANN

Agenda

- Introduction to DNSSEC
- DNSSEC validation - Intro
- State of DNSSEC Deployment
- Enabling DNSSEC Validation

Introduction to DNSSEC

What Is DNSSEC?

DNSSEC stands for **Domain Name System (DNS) Security Extensions.**

- DNSSEC is a protocol that is currently being deployed to secure the DNS.
- DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names.
- DNSSEC is the result of over two decade of community-based, open standards development.
- Specified in RFCs 4033, 4034, 4035 and 5155

DNSSEC in summary

- To achieve Authenticity and Integrity of DNS data
- Allows domain name registrants to cryptographically **SIGN** their DNS data
- Allows DNS operators to **VALIDATE** all DNS data passing through DNS resolvers
- Provide assurances to users that the DNS data they are seeing is valid and true
- Helps prevent DNS threats and abuses

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.com* 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

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

DNSSEC Validation

DNSSEC Enabled - Resolvers in action

DNSSEC Validation

- DNSSEC validation is the process of **checking the signatures** on DNSSEC data
- Validation can occur in applications, stub resolvers or recursive resolvers
- Most validation today occurs in recursive resolvers
- Trust Anchor: To perform DNSSEC validation, you have to trust somebody (some zone's key). **Root Zone KSK is the most important trust Anchor on the Internet.**
- What happens when validation fails?

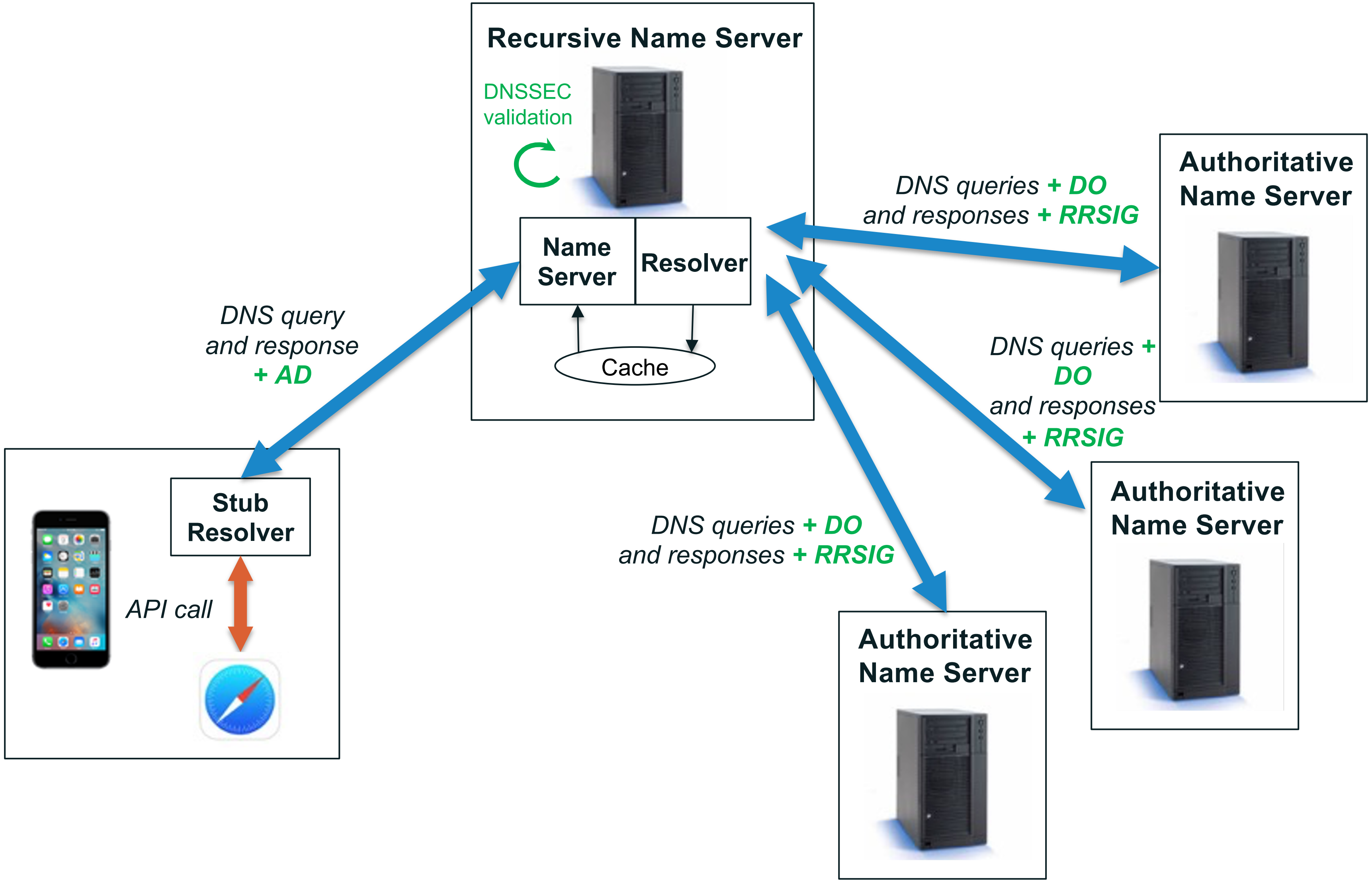
  Overloaded signaling mechanism from recursive resolver to stub resolvers

  - SERVFAIL error, which has other meanings

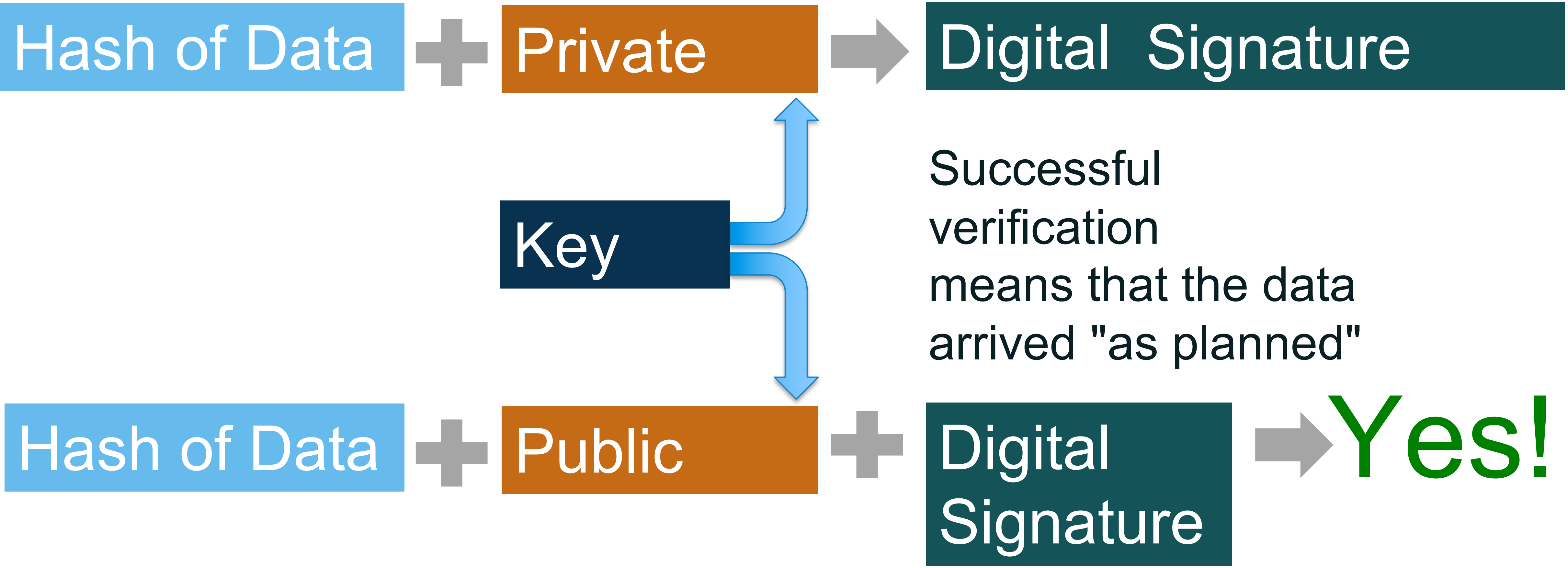
  No signaling mechanism from stub resolver to application

  - Most resolver APIs not rich enough to pass validation status

DNS resolution process with DNSSEC


Recursive Name Server
DNSSEC validation
Name Server
Resolver
Cache
DNS query and response + AD
Stub Resolver
API call
DNS queries + DO and responses + RRSIG
Authoritative Name Server
DNS queries + DO and responses + RRSIG
Authoritative Name Server
DNS queries + DO and responses + RRSIG
Authoritative Name Server

Digital Signatures - Verification



Hash of Data + Private → Digital Signature

Key

Hash of Data + Public + Digital Signature → Yes!

Successful verification means that the data arrived "as planned"

Chain of Trust

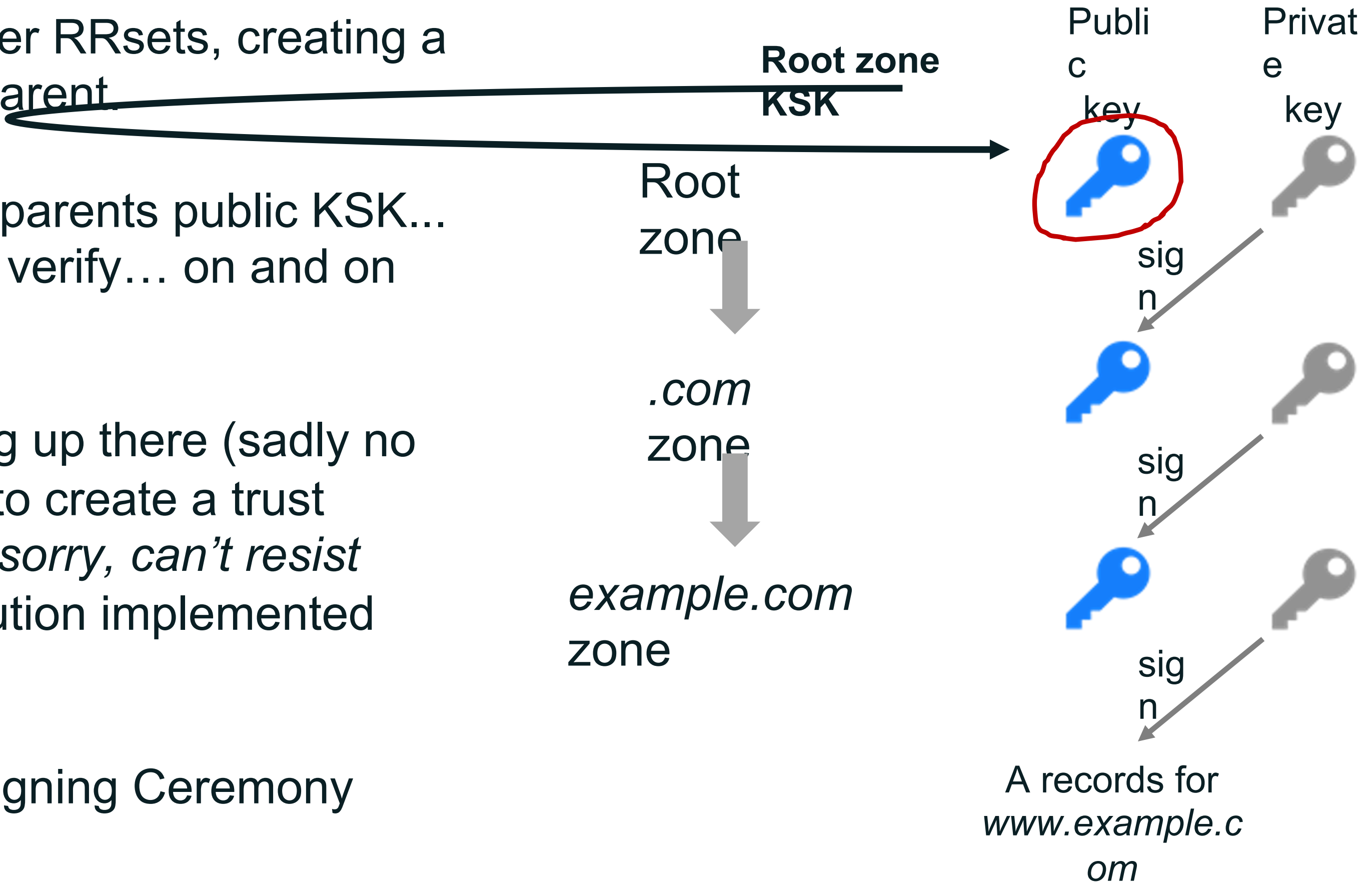
Finally, how do we trust DS record?

Well, we just sign DS record like we did with other RRsets, creating a corresponding RRSIG for the DS record in the parent.

We repeat the validation process and get to the parents public KSK... And again must go to that parent's DS record to verify… on and on up to the DNS root.

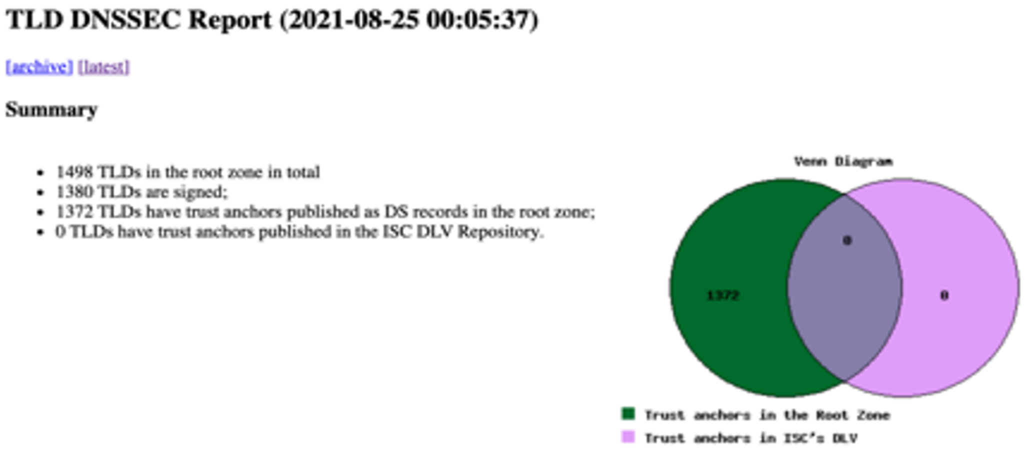
Eventually, we get to the root and there's nothing up there (sadly no parent)… and so we must come with a solution to create a trust anchor for the root, a "one key to rule them all" (*sorry, can't resist quoting LOTR again*)… and here it comes a solution implemented since 2010 called:

The Root Signing Ceremony



State of DNSSEC Deployment

State of DNSSEC deployment



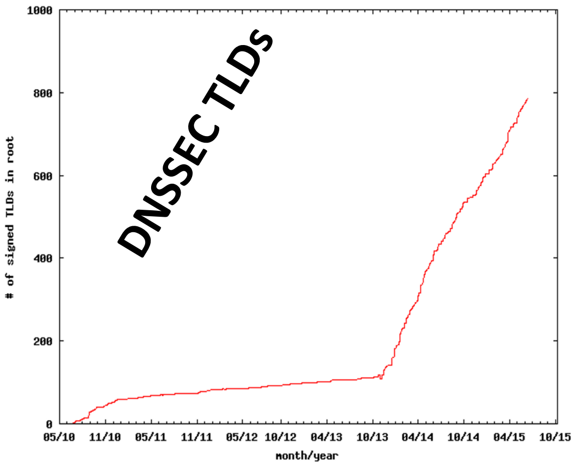
TLD DNSSEC Report (2021-08-25 00:05:37)

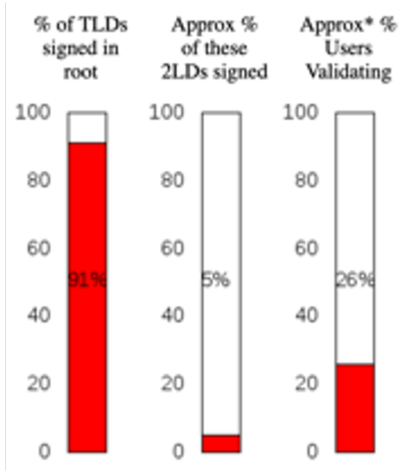
[archive] [latest]

Summary

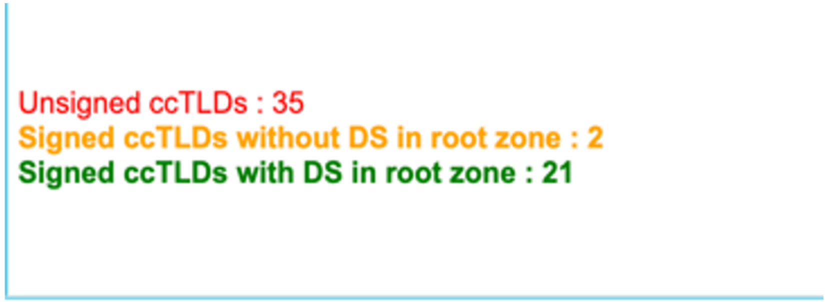
- 1498 TLDs in the root zone in total
- 1380 TLDs are signed;
- 1372 TLDs have trust anchors published as DS records in the root zone;
- 0 TLDs have trust anchors published in the ISC DLV Repository.

http://stats.research.icann.org/dns/tld_report/





http://rick.eng.br/dnssecstat/



Unsigned ccTLDs : 35

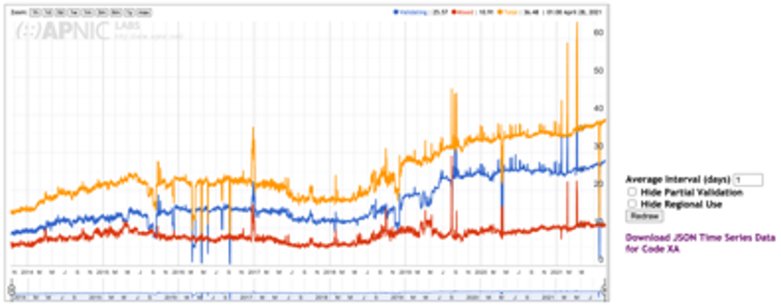
Signed ccTLDs without DS in root zone : 2

Signed ccTLDs with DS in root zone : 21

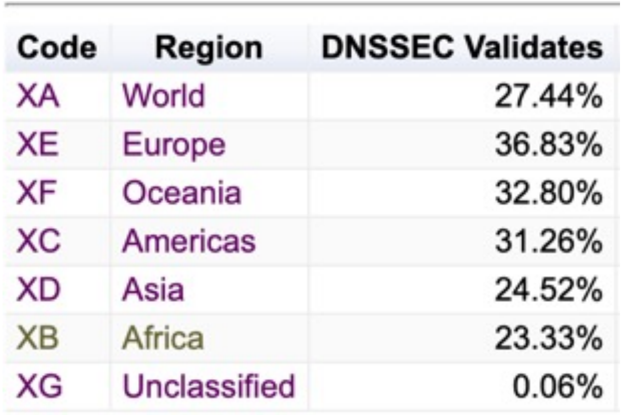
DNSSEC signing in Africa ccTLDs, Oct. 2021

https://dnssec-africa.org/index.html

Use of DNSSEC Validation for World (XA)



https://stats.labs.apnic.net/dnssec/XA



Code	Region	DNSSEC Validates
XA	World	27.44%
XE	Europe	36.83%
XF	Oceania	32.80%
XC	Americas	31.26%
XD	Asia	24.52%
XB	Africa	23.33%
XG	Unclassified	0.06%

State of DNSSEC Validation

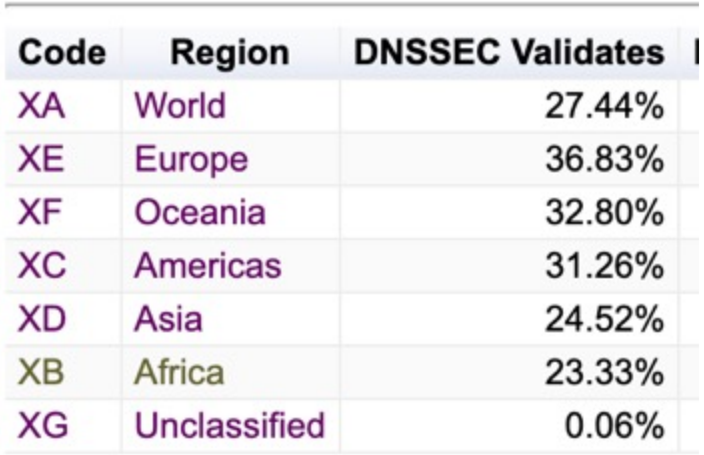
- Most validation today occurs in recursive resolvers
- **Bad News:**

  27% of DNS responses are validated according to APNIC Labs*

  Too many resolvers do not validate DNS answers

  . . And not enough domains are signed
- ICANN has a mandate in our strategic plan for 2021-2025 to significantly increase DNSSEC adoption, including convincing DNS resolver vendors to ship their software with DNSSEC validation turned-on by default

State of DNSSEC Validation– (Oct 2021)

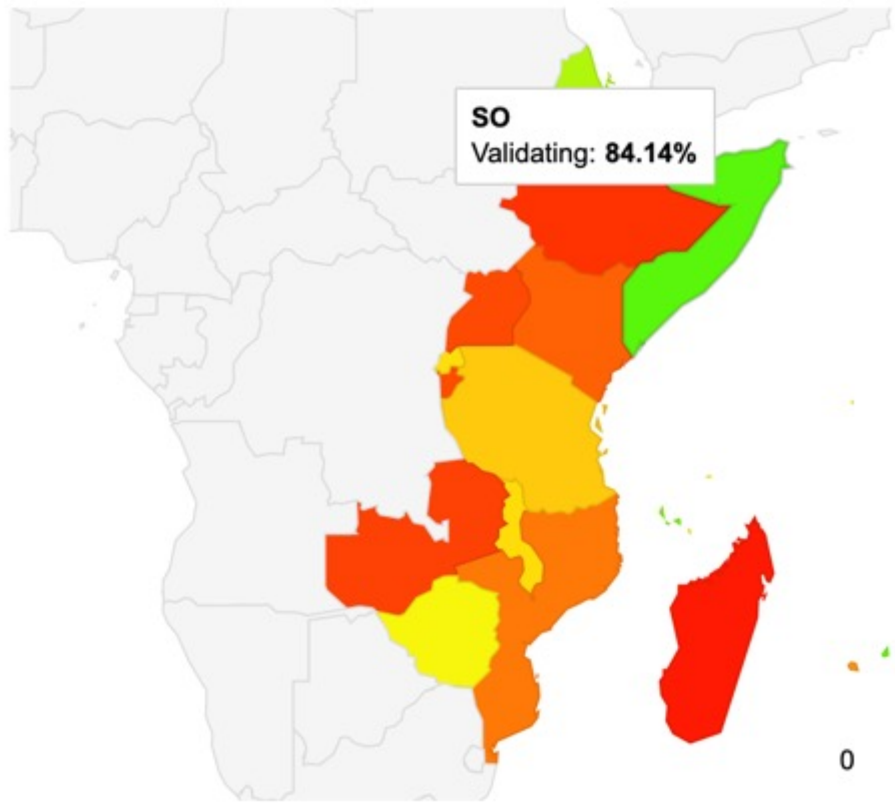


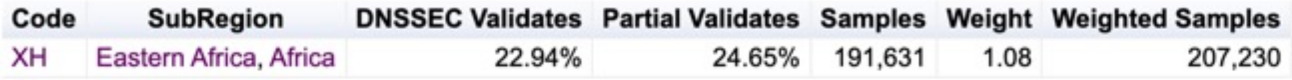
Code	Region	DNSSEC Validates
XA	World	27.44%
XE	Europe	36.83%
XF	Oceania	32.80%
XC	Americas	31.26%
XD	Asia	24.52%
XB	Africa	23.33%
XG	Unclassified	0.06%

Source: APNIC Labs: https://stats.labs.apnic.net/dnssec/XA

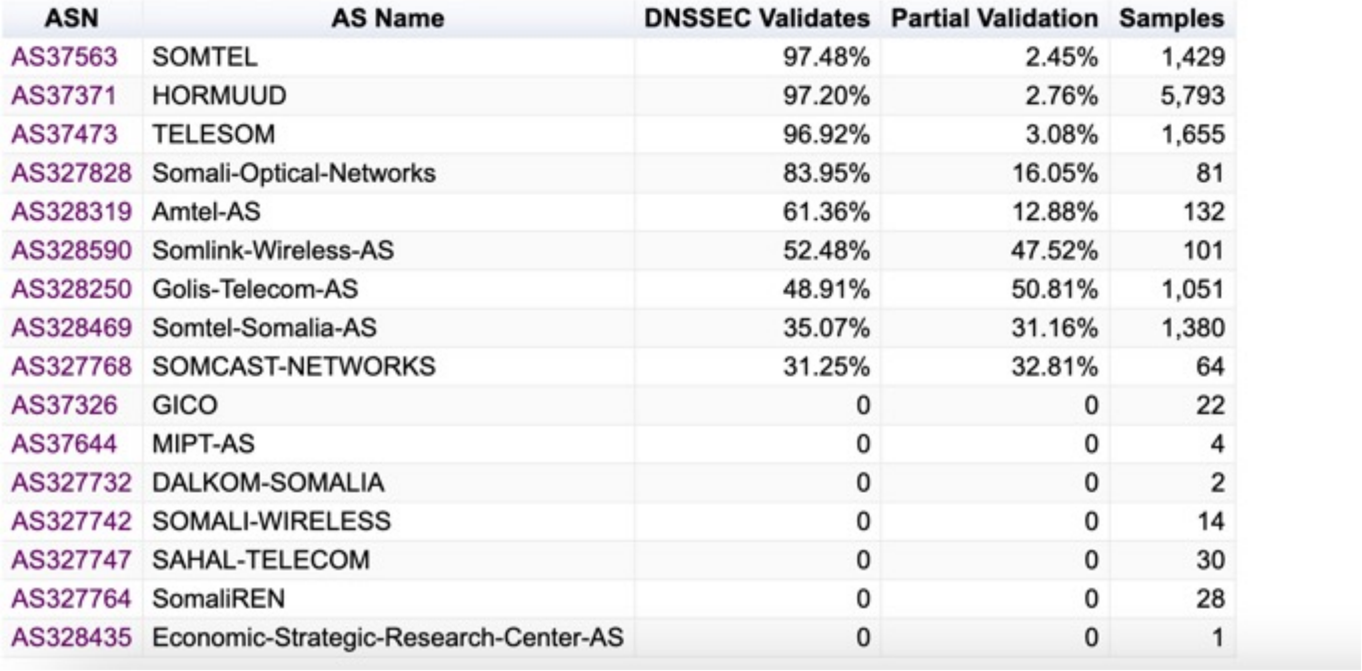
State of DNSSEC Validation – Somalia

Region Map for Eastern Africa (014)





Code	SubRegion	DNSSEC Validates	Partial Validates	Samples	Weight	Weighted Samples
XH	Eastern Africa, Africa	22.94%	24.65%	191,631	1.08	207,230



ASN	AS Name	DNSSEC Validates	Partial Validation	Samples
AS37563	SOMTEL	97.48%	2.45%	1,429
AS37371	HORMUUD	97.20%	2.76%	5,793
AS37473	TELESOM	96.92%	3.08%	1,655
AS327828	Somali-Optical-Networks	83.95%	16.05%	81
AS328319	Amtel-AS	61.36%	12.88%	132
AS328590	Somlink-Wireless-AS	52.48%	47.52%	101
AS328250	Golis-Telecom-AS	48.91%	50.81%	1,051
AS328469	Somtel-Somalia-AS	35.07%	31.16%	1,380
AS327768	SOMCAST-NETWORKS	31.25%	32.81%	64
AS37326	GICO	0	0	22
AS37644	MIPT-AS	0	0	4
AS327732	DALKOM-SOMALIA	0	0	2
AS327742	SOMALI-WIRELESS	0	0	14
AS327747	SAHAL-TELECOM	0	0	30
AS327764	SomaliREN	0	0	28
AS328435	Economic-Strategic-Research-Center-AS	0	0	1

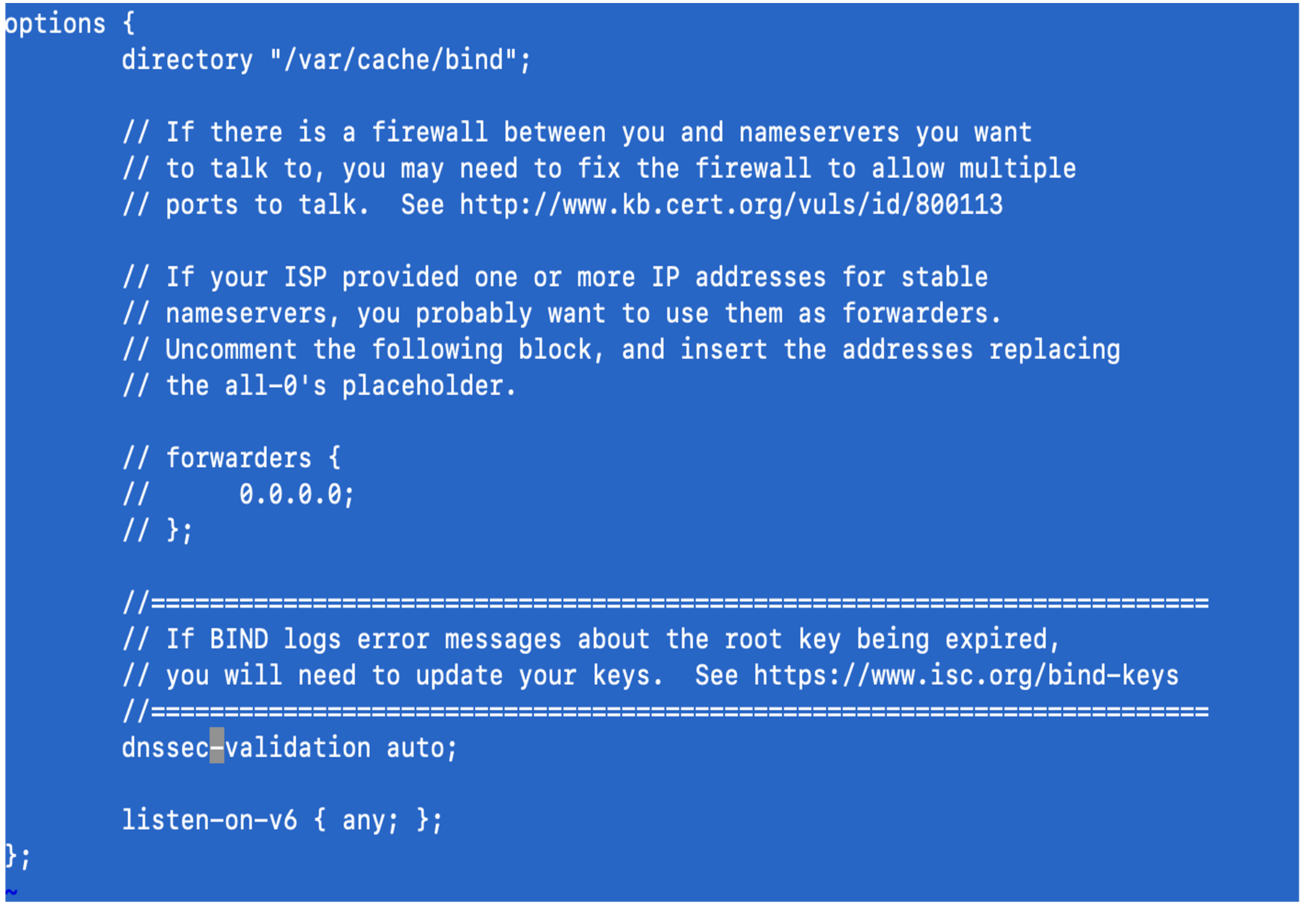
Source: APNIC Labs: https://stats.labs.apnic.net/dnssec/SO

Enabling DNSSEC Validation

DNSSEC Validation in BIND 9.11+

- On /etc/bind/named.conf.options :

dnssec-validation auto



```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
~
```

DNSSEC Validation in Unbound 1.7+

1) Download root-key trust anchor:

```
unbound-anchor
```

2) On /etc/unbound/unbound.conf.d/root-auto-trust-anchor-file.conf :

Uncomment the line:

```
# auto-trust-anchor-file: "/var/lib/unbound/root.key"
```

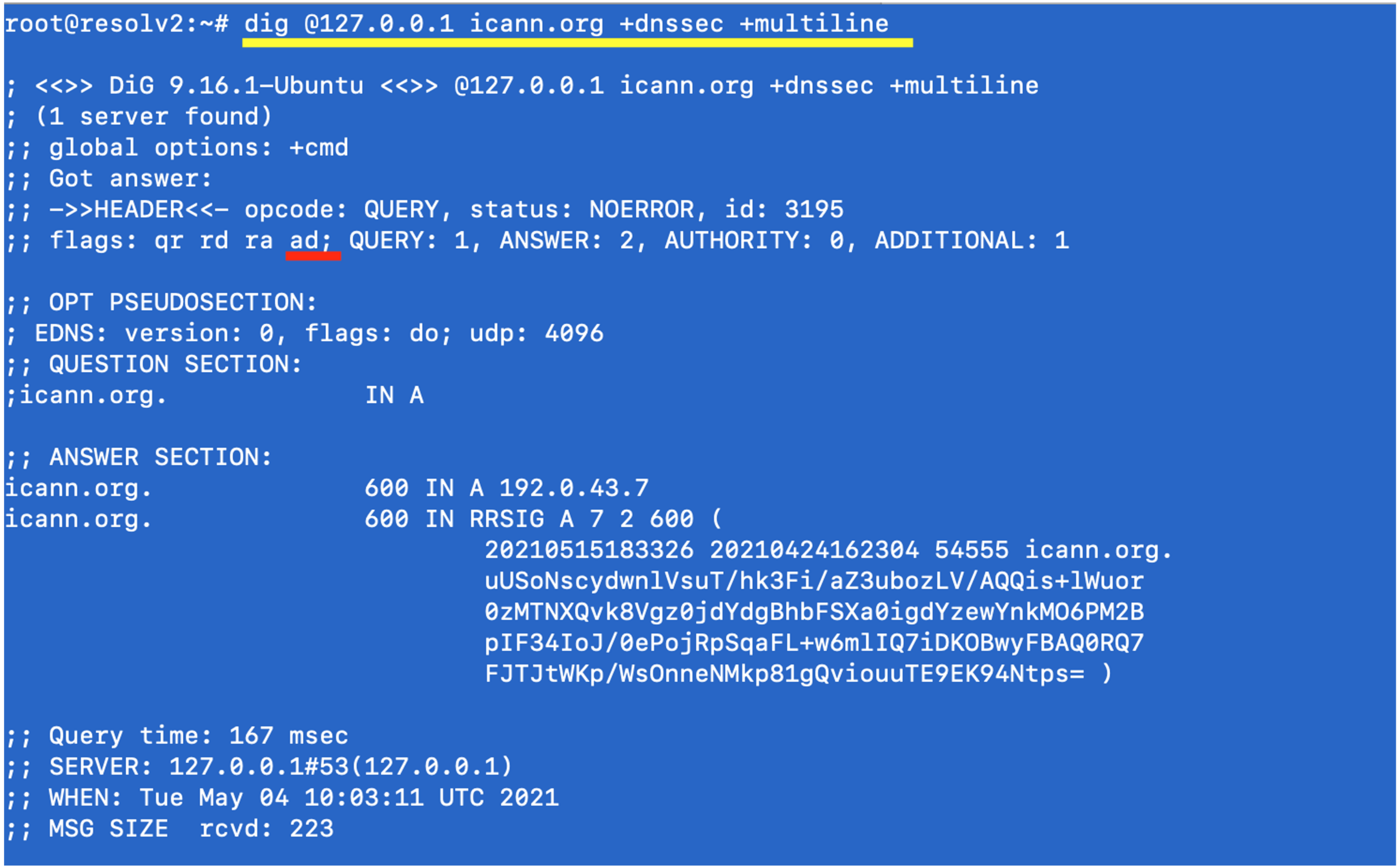
To:

```
auto-trust-anchor-file: "/var/lib/unbound/root.key”
```

3) Restart Unbound

Test your Resolver is Validating

- Do you get the **ad** bit?



```
root@resolv2:~# dig @127.0.0.1 icann.org +dnssec +multiline

; <<>> DiG 9.16.1-Ubuntu <<>> @127.0.0.1 icann.org +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3195
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;icann.org.             IN A

;; ANSWER SECTION:
icann.org.              600 IN A 192.0.43.7
icann.org.              600 IN RRSIG A 7 2 600 (
                                20210515183326 20210424162304 54555 icann.org.
                                uUSoNscydwnlVsuT/hk3Fi/aZ3ubozLV/AQQis+lWuor
                                0zMTNXQvk8Vgz0jdYdgBhbFSXa0igdYzewYnkMO6PM2B
                                pIF34IoJ/0ePojRpSqaFL+w6mlIQ7iDKOBwyFBAQ0RQ7
                                FJTJtWKp/WsOnneNMkp81gQviouuTE9EK94Ntps= )

;; Query time: 167 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue May 04 10:03:11 UTC 2021
;; MSG SIZE  rcvd: 223
```

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann