DNSSEC: worth adding to your cybersecurity strategy

AFRINIC Webinar series

Yazid Akanho
ICANN Office of the CTO

August 2023

ICANN

AFRINIC
The Internet Numbers Registry for Africa

The context

The Domain Name System, well known under the acronym DNS, is a critical service used in every single communication we (people, systems, applications) do on the Internet.

The problem

Akamai researchers have analyzed malicious DNS traffic from millions of devices to determine how corporate and personal devices are interacting with malicious domains, including phishing attacks, malware, ransomware, and command and control (C2).

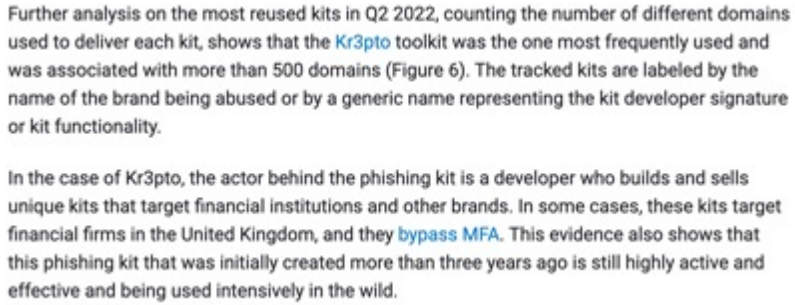
Akamai researchers saw that 12.3% of devices used by home and corporate users communicated at least once to domains associated with malware or ransomware.

63% of those users' devices communicated with malware or ransomware domains, 32% communicated with phishing domains, and 5% communicated with C2 domains.

As many other services, DNS has several vulnerabilities that **bad actors on the Internet use to conduct their attacks**.

Classic firewalls and usual security measures in the network do not protect against those weaknesses.

This is where DNSSEC comes in …



https://www.dnsfilter.com/blog/rsac-2022-the-rise-of-dns-based-attacks
https://www.akamai.com/blog/security-research/q2-dns-akamai-insights
https://www.cloudflare.com/learning/insights-dns-landscape/

DNSSEC: overview and benefits

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

- A protocol being deployed since 2000s to secure the DNS.
- Adds security to the DNS by incorporating public key cryptography.
- Provides assurance to users that the DNS data they get is **valid and true**.
- Helps prevent DNS threats and abuses (cache poisoning, redirection to fake destination, etc.) by verifying and confirming authenticity and integrity of DNS data.
- Protects your digital integrity and your business, protects your customers online.
- Complementary to other technologies like SSL widely used to secure web communications.

How does DNSSEC work ?

Two actions are required :

- Registrants (domain name holder) should **sign their domain**: the domain administrator generates and maintains the cryptographic keys and signatures for the domain.

- DNS operators, ISPs, mobile operators, hosting providers, companies, … should **activate DNSSEC validation** (verifies the authenticity and integrity of DNS responses from signed domains) in their recursive resolvers: system administrators should enter the server configuration and turn on the functionality.

Original
Or
Counterfeit
Banknote ?

Detection mechanisms

Who should implement DNSSEC ?

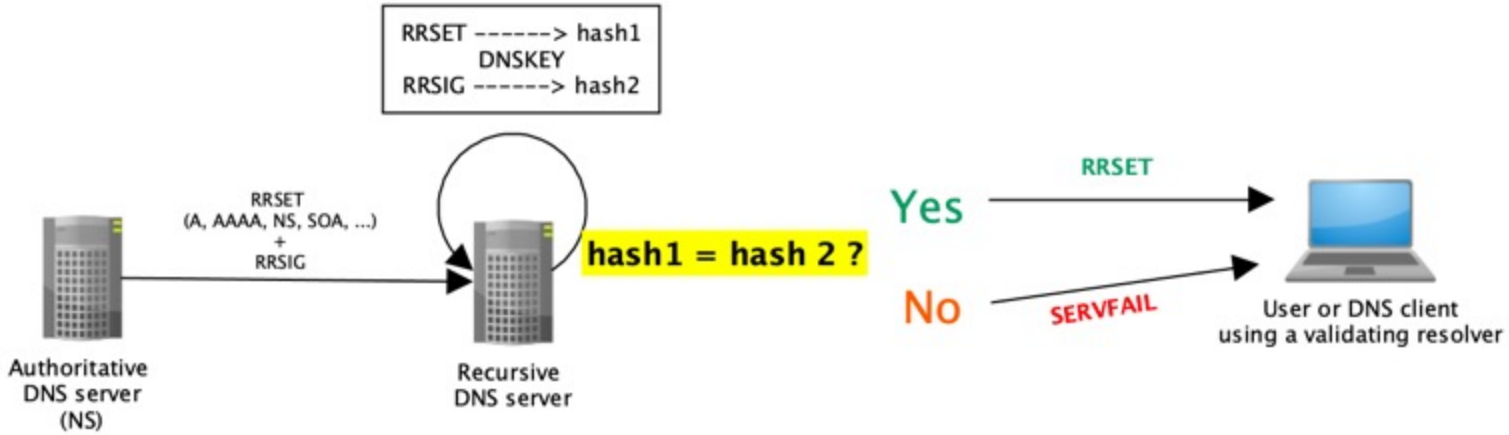
- Registry operator (TLD): ccTLD and IDN ccTLD Registry Operators.
- Companies and businesses:
  - **Sign** your domains or get them signed: the DNS root zone is signed since 2010 and all gTLD are signed today while 60% ccTLDs are signed. At second level, signing is still low.
  - Activate DNSSEC **validation** on your recursive resolvers.
- ISPs, MNOs:
  - Activate DNSSEC **validation** on your recursive resolvers.
  - **Sign** your domains and the ones you host for your customers.
- Hosting providers, registrars:
  - Accept DNSSEC records such as DS and push to the registry (registrars).
- Registrants: sign your domains or get them signed.

DNSSEC signing: technical high level overview

- What/how is the existing DNS infrastructure ?
- Plan and get prepared
- Involve partners: 3rd Party, registrars,
- DNSSEC software solution (OpenDNSSEC, Bind, …), architecture, signing methodology, key generation and management, etc.
- Generate DNSSEC signing keys.
- Test signing and plan for signing in production.
- Sign and when comfortable, upload DS to parent zone: your zone is officially signed.
- Refresh signatures and keys as per best practices and your operational constraints.
- Update Business Continuity Plans
- Monitor, analyze, improve, implement, monitor.

DNSSEC Validation high level overview

- The process of **checking the signatures on DNSSEC data** that help to verify authenticity and integrity of signed zones.
- Protects your customers/users from being redirected to a wrong/fake destination (web site, online service, …)
- Most validation today occurs in recursive resolvers. Can also occur in apps and stub.
- For signed domains, DNSSEC signatures data come alongside with the DNS response.



What do you need to enable DNSSEC validation ?

- If you run your own DNS recursive resolvers (open source or commercial), activate DNSSEC validation is usually **simple and does not require a new investment**. Most software already have it embedded, you just need to perform some verification: hardware resources, server clock synchronization (NTP), correct root trust anchor, EDNS(0), TCP port 53 should be open, exclude forward-zones (if you have any!).
- If you are using external recursive resolvers, make sure that they are DNSSEC validating. If not, you can refer to their administrators and suggest them to activate it.
- Well known open public recursive resolvers are validating and lot of ISPs and operators in the world as well. Go to https://stats.labs.apnic.net/dnssec and see the trends.

State of DNSSEC Validation

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

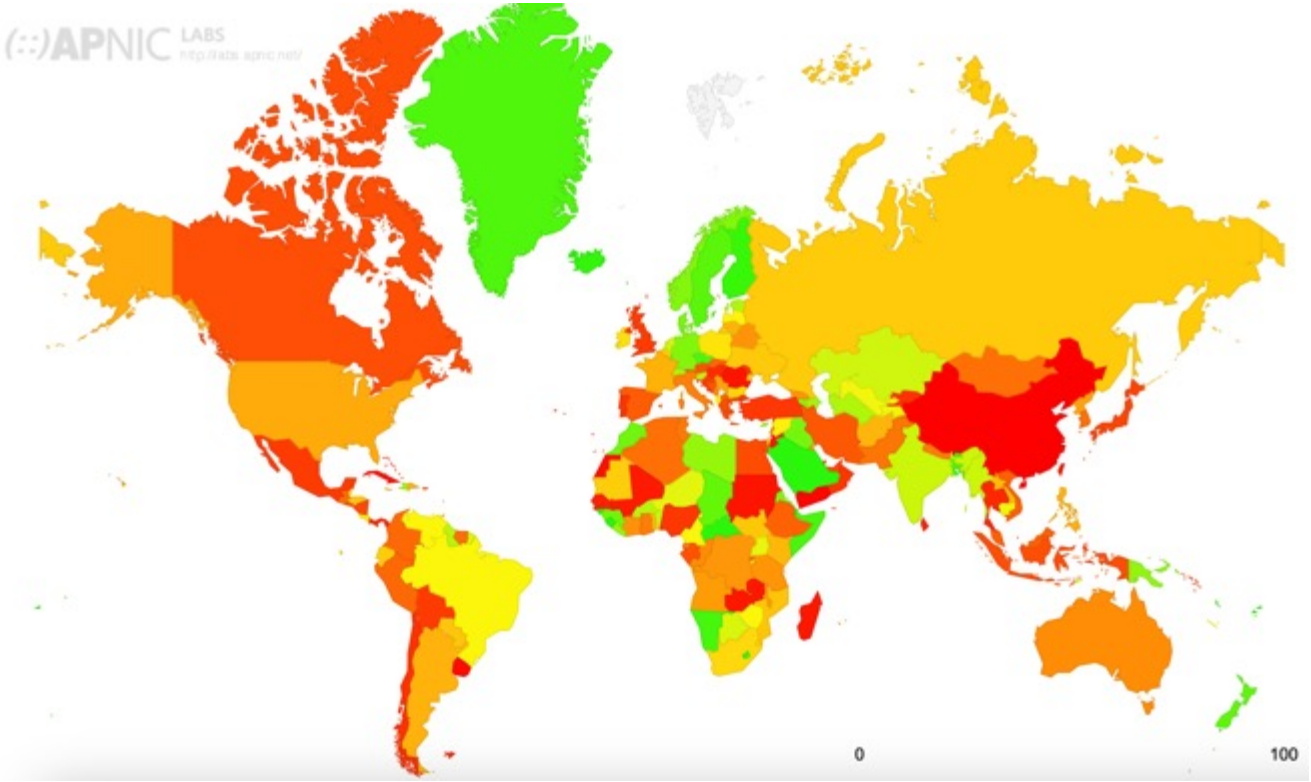
  ≈ 31 % of DNS responses are validated according to APNIC Labs*

  Too many resolvers still 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
- https://stats.labs.apnic.net/dnssec/

State of DNSSEC Validation: world and Africa



Region	DNSSEC Validates
World	30.64%
Oceania	43.32%
Europe	39.85%
Americas	33.20%
Africa	29.20%
Asia	27.57%
Unclassified	3.42%

SubRegion	DNSSEC Validates
Southern Africa, Africa	48.03%
Middle Africa, Africa	34.86%
Eastern Africa, Africa	29.72%
Northern Africa, Africa	29.24%
Western Africa, Africa	21.46%

Top 10 DNSSEC validating countries in Africa

Country	DNSSEC Validates
Central African Republic, Middle Africa, Africa	100.00%
Djibouti, Eastern Africa, Africa	99.62%
Guinea-Bissau, Western Africa, Africa	99.28%
Sierra Leone, Western Africa, Africa	99.07%
Lesotho, Southern Africa, Africa	98.28%
Namibia, Southern Africa, Africa	94.32%
Somalia, Eastern Africa, Africa	89.17%
Chad, Middle Africa, Africa	83.46%
Guinea, Western Africa, Africa	83.22%
Morocco, Northern Africa, Africa	83.12%

Less 10 DNSSEC validating countries in Africa

Equatorial Guinea, Middle Africa, Africa	16.71%
Gabon, Middle Africa, Africa	15.93%
Egypt, Northern Africa, Africa	14.99%
Angola, Middle Africa, Africa	12.76%
Nigeria, Western Africa, Africa	9.42%
Mali, Western Africa, Africa	7.55%
Senegal, Western Africa, Africa	5.16%
Madagascar, Eastern Africa, Africa	5.15%
Zambia, Eastern Africa, Africa	4.16%
Sudan, Northern Africa, Africa	4.05%

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

How can we assist you ?

- Trainings and hands-on labs to the ISPs and operators technical staff
- Guidance in your readiness assessment: prerequisites, etc.
- Sharing documentation and operational manuals
- Advise in parameters, best practices, but we cannot choose on your behalf.
- Work with you in test bed and guide you until go-live but cannot configure for you.
- Email us at octo@icann.org for support, we will then get in touch with you and evaluate how we can assist you in your journey to deploying DNSSEC.
- **"DNSSEC Deployment Guidebook for ccTLDs", OCTO-029**: a guidebook for DNSSEC deployment, aims to assist operators in understanding a DNSSEC signing deployment project.
- Download the guidebook at : https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf

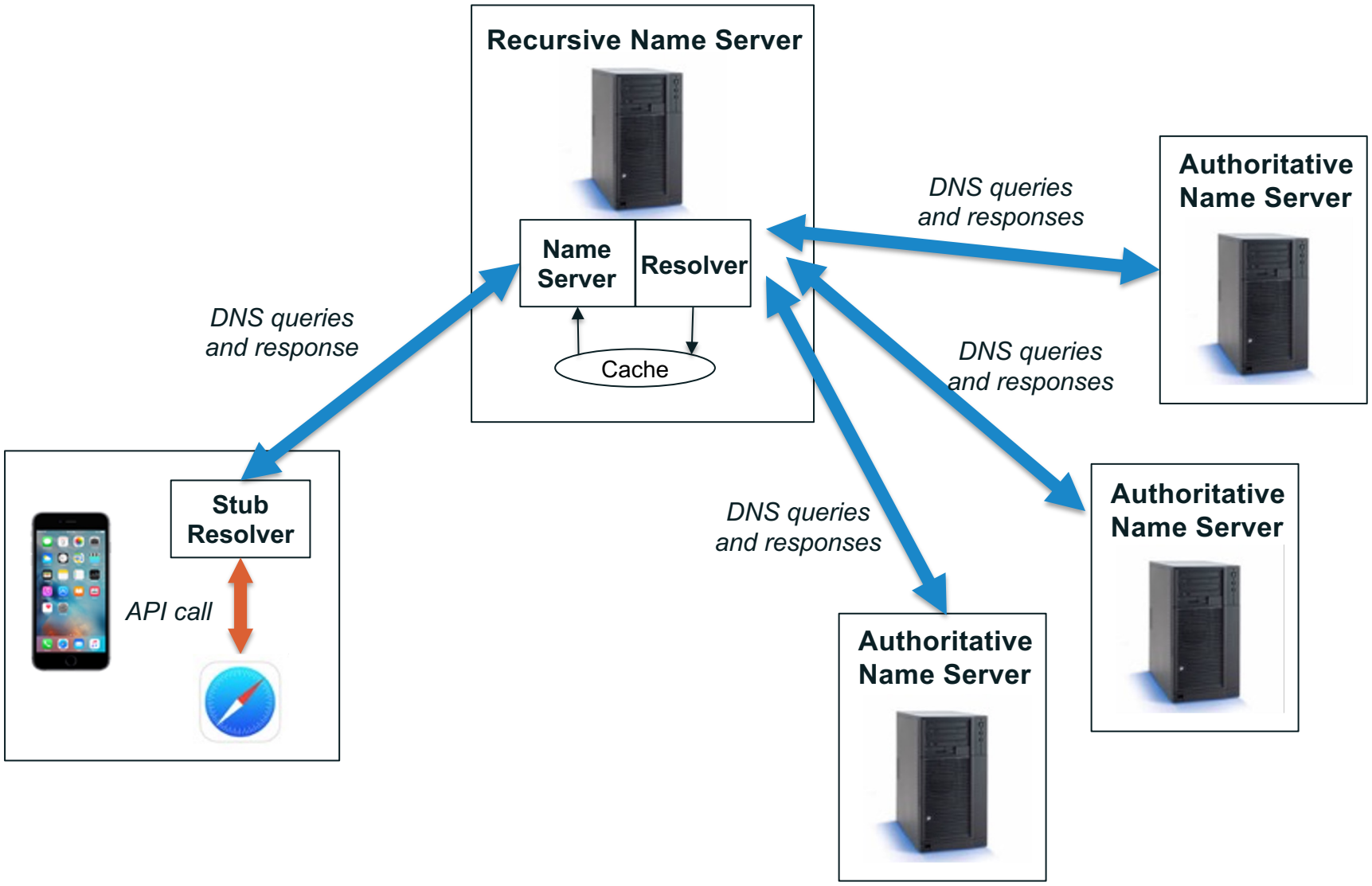
Next steps

1. Are you interested in activating DNSSEC validation ?
2. If yes, let’s work together with your DNS team

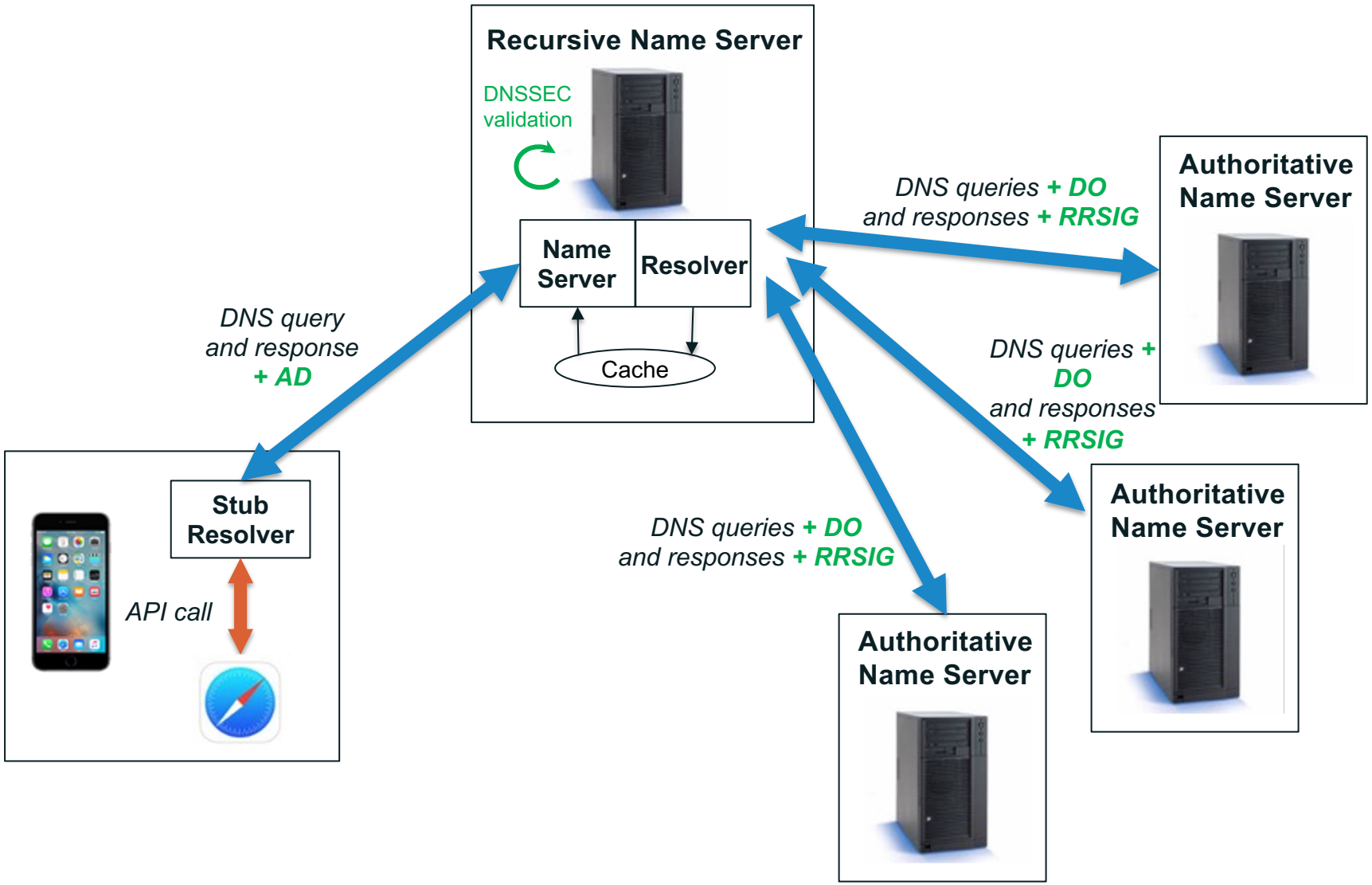
DNSSEC Validation

DNSSEC enabled - resolvers in action

DNS resolution process with DNSSEC



DNS resolution process with DNSSEC



Enabling DNSSEC Validation in few recursive resolvers

Enable 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; };
};
~
```

Enable 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
4. For “large resolver installations”, optimization is necessary:

   https://nlnetlabs.nl/documentation/unbound/howto-optimise/

Enable DNSSEC Validation in Infoblox

- Infoblox DNSSEC deployment Guide (signing and validation): https://www.infoblox.com/wp-content/uploads/infoblox-deployment-guide-dnssec.pdf

DNSSEC validation

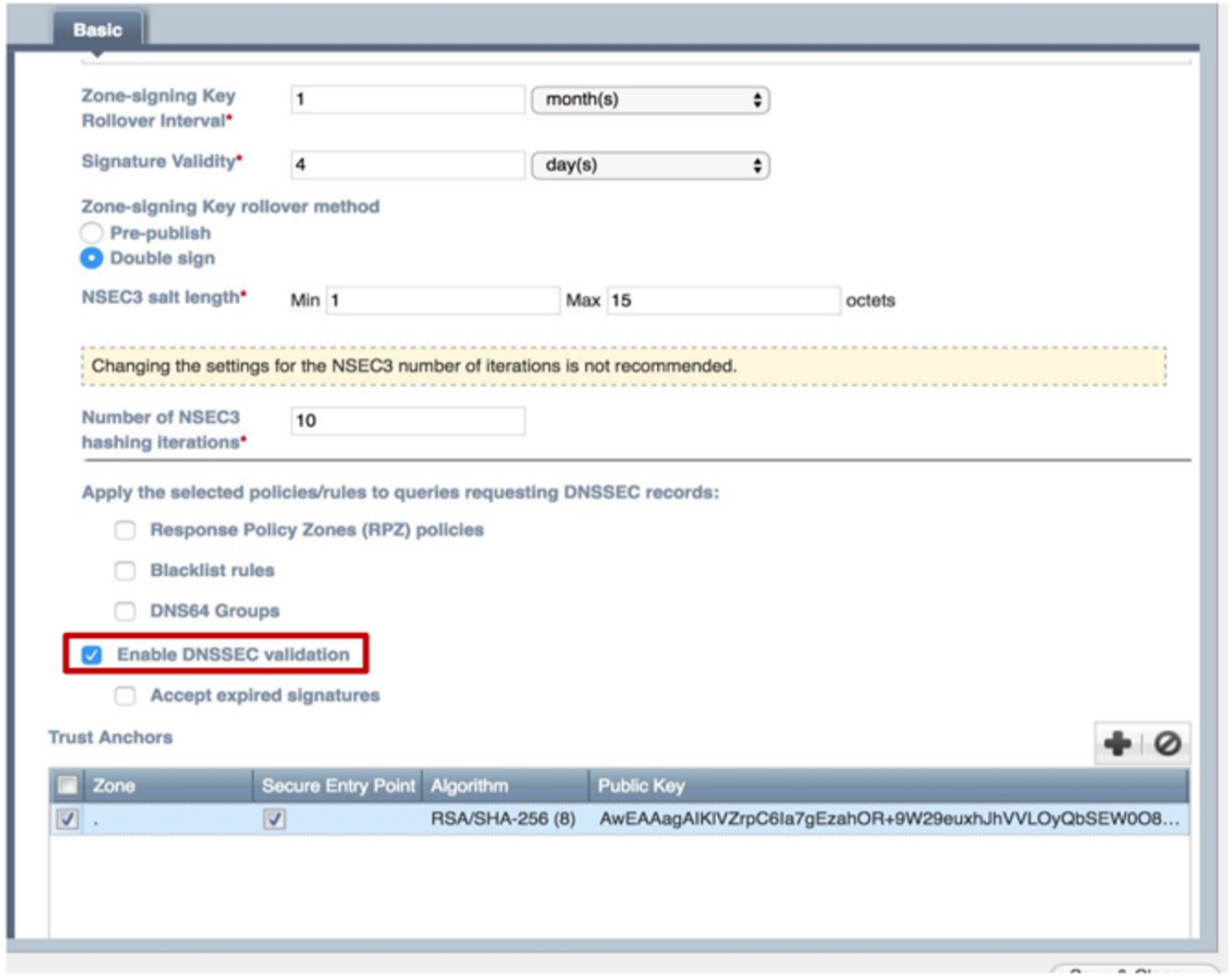
Prerequisites

1. EDNS0 must be enabled and supported by your networking equipment.
    a. Check the section Troubleshooting for a quick method on how to test if your environment supports EDNS0.
2. Recursion must be enabled.

Steps to enable DNSSEC Validation

1. Go to **Data Management > DNS > Grid properties**
2. Toggle advanced on (if not already enabled)
3. Click on DNSSEC
4. Check the Enable DNSSEC box
5. Scroll down and check the Enable DNSSEC validation checkbox
6. Once you have enabled the feature, you will need to obtain the root key(s) in a secure way and enter it/them under Trust Anchors

Enable DNSSEC Validation in Infoblox



Enable DNSSEC Validation in Infoblox

- Ascertain Root Key (Trust Anchor):

```
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGC
zh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6
CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0s
GIcGOYI7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz 0=
```

- Add this key under Trust Anchors for “.” and set the algorithm to 8

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

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

AFRINIC WEBINAR SERIES

DNNSEC @ AFRINIC

Presenter: David Njuki
Date: 10th August 2023

AFRINIC
The Internet Numbers Registry for Africa

https://twitter.com/afrinic
https://www.youtube.com/afrinic
https://facebook.com/afrinic

AFRINIC DNS

AFRINIC manages and publishes Reverse DNS (**rDNS**) zone data for the IP space we allocate or assign to members.

IPv4

- 41.in-addr.arpa.
- 196.in-addr.arpa.
- 197.in-addr.arpa.
- 102.in-addr.arpa.
- 105.in-addr.arpa.
- 154.in-addr.arpa

IPv6

- 0.c.2.ip6.arpa.
- 3.4.1.0.0.2.ip6.arpa.
- 2.4.1.0.0.2.ip6.arpa.

DNSSEC Operations

- Sign **rDNS** zones.
- Publish **DS** record in parent zones -> **.in-addr.arpa .ip6.arpa**
- Accept **DS** records from reverse delegated zones from our members
- Monitoring of hosted **rDNS** infrastructure

The above operations aims to build the chain of trust for the assigned and delegated **rDNS** resources.

- We run validating resolvers for our Infra and Corporate Network
- Our forward zone **afrinic.net** is DNSSEC signed.

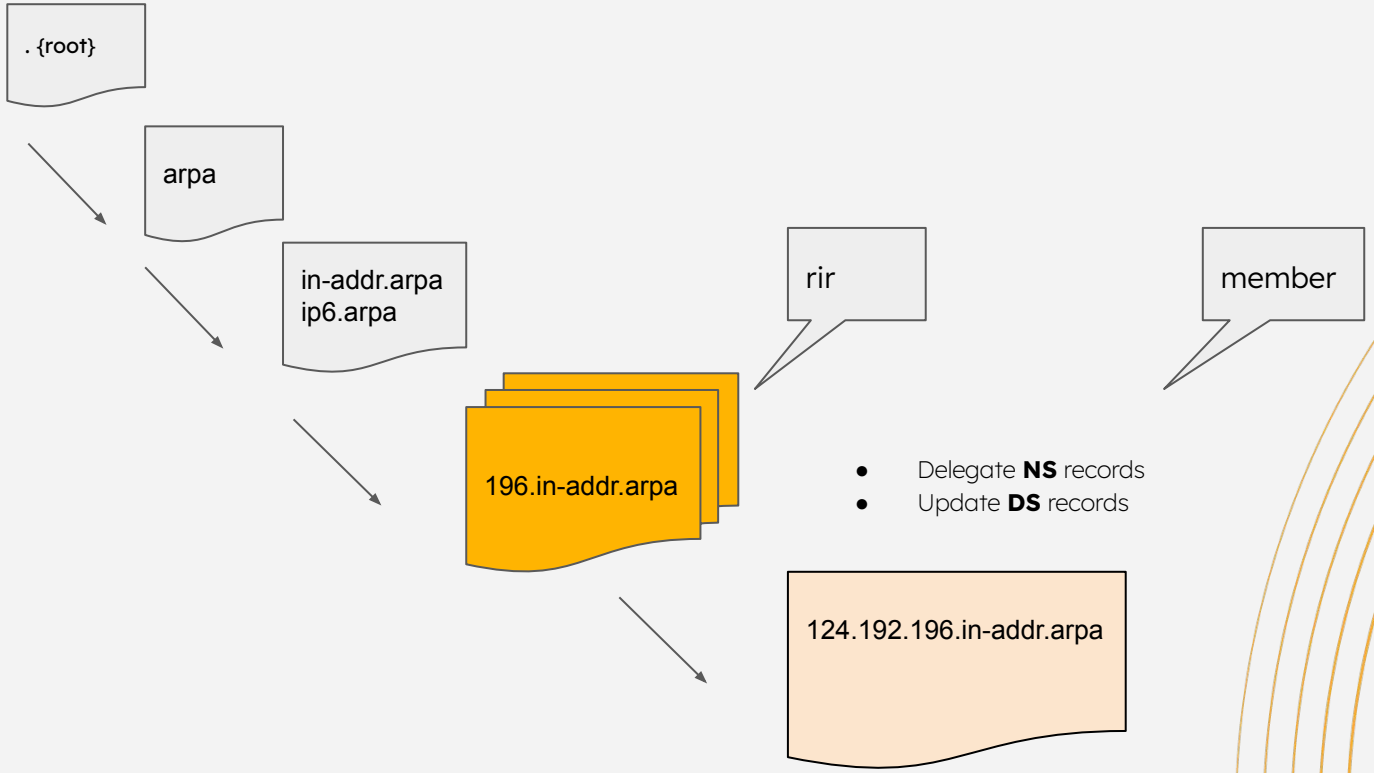
* RDNS zone data are published on FTP **https://ftp.afrinic.net/zones**

Reverse DNS Provisioning

- Domain objects from the **WHOIS** database
- Authoritative NS by AFRINIC and other RIRs as secondary
- Delegation and management of reverse zones on **MyAFRINIC**

```
domain:       196.in-addr.arpa
organisation: Administered by AFRINIC
nserver:      afrinic.authdns.ripe.net.
nserver:      ns1.afrinic.net.
nserver:      ns2.afrinic.net.
nserver:      ns3.afrinic.net.
nserver:      ns3.lacnic.net.
nserver:      ns4.apnic.net.
nserver:      rirns.arin.net.
ds-rdata:     17735 8 1 661c53d38db7ab79d30d5a4e9b3bca30bc905d73
ds-rdata:     17735 8 2 e5ed9b92336af2c4dd592b472a03ddf4d15a0acfcedeed7a905225f108634d95
ds-rdata:     54334 8 1 6e3196011ed9841b30621686dca055bcb6e3ed49
ds-rdata:     54334 8 2 ba6e6fd4d66107d6c2d7fbdc91e0bd3d0570182d3555b17c05f0a1c760ece9b2
```

rDNS Chain of Trust



rDNS Update on MyAFRINIC Portal

Edit RDNS

Reverse Zone: 124.192.196.in-addr.arpa

Reg Date: 2014-08-21

*** Name Servers:**

Provide the primary and secondary name servers for this reverse delegation [Please note: we need the hostname(s) here, not the ip address(es)]

ns1.afrinic.net

ns2.afrinic.net

[More | Less] Fields

DS Records:

Provide Delegation Signer Resource Records (RFC 4034)
keytag: {0-65535} ; Algorithm:{3|5|6|7|8|10|12|13|14|15|16|253|254} ; Digest type :{1-4} ; Digest:{alphanumeric}

IMPORTANT this current version of MyAFRINIC accepts digest type 3 and 4 but cannot verify these particular digest.
Please, make sure that your record is correct if you use digest type 3 or 4.

6265 8 2 13a2be6e3c96d016deb75bed3e4ded16ecba2c23fa619fd3bf96721ece799d00

10867 8 2 633b32e61eee3f53126f5329a0b0a34b572d96b6c622b3499cd6846e432a6610

[More | Less] Fields

*** Description:**

Provide the description of this reverse delegation.

rDNS for 196.192.124.0 - AFRINIC Mombasa OPS

Domain Objects Updated on WHOIS

```
domain:         124.192.196.in-addr.arpa
descr:          rDNS for 196.192.124.0 - AFRINIC Mombasa OPS
nserver:        ns1.afrinic.net
nserver:        ns2.afrinic.net
org:            ORG-AFNC1-AFRINIC
admin-c:        IT7-AFRINIC
tech-c:         IT7-AFRINIC
zone-c:         IT7-AFRINIC
mnt-by:         AFRINIC-IT-MNT
mnt-lower:      AFRINIC-IT-MNT
ds-rdata:       6265 8 2 13a2be6e3c96d016deb75bed3e4ded16ecba2c23fa619fd3bf96721ece799d00
ds-rdata:       10867 8 2 633b32e61eee3f53126f5329a0b0a34b572d96b6c622b3499cd6846e432a6610
remarks:        #171852- renumbering
source:         AFRINIC # Filtered
```

Publication of DS records to Parent

- Parent in this case is **196.in-addr.arpa**
- Publication runs are automated to run hourly
- Allow at least 4 hours for full propagation

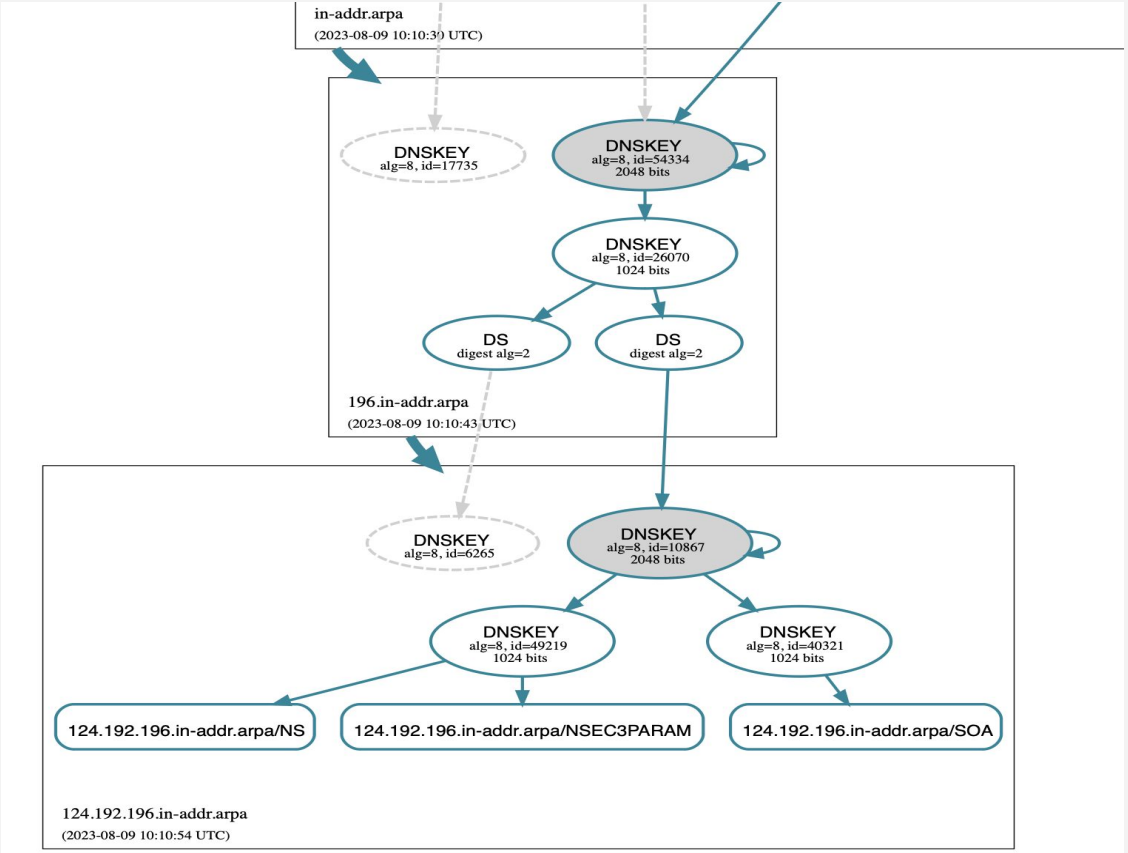
rDNS DNSSEC Validation

```
; <<>> DiG 9.10.6 <<>> 124.192.196.in-addr.arpa dnskey @dns1.mu.afrinic.net
+multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8944
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;124.192.196.in-addr.arpa. IN DNSKEY

;; ANSWER SECTION:
124.192.196.in-addr.arpa. 1199 IN DNSKEY 256 3 8 (
            AwEAAbewwbw2KAzPsbz9IDvqBolZ+JEtaPHRS+anmQaX
            zQDH21uYf8IOpix/A4YzkwIwy+nVnkMe6xF+vNOIccdU
            jDPkDiURj4W14qsbFeBMMohgkBzionvrcXiWi3/fAA4F
            qjbV0seFF3+wV8p9jUBaZrGAhDTHaFIHmsVJhElRmwkj
            ) ; ZSK; alg = RSASHA256 ; key id = 40321
```

rDNS DNSSEC Validation

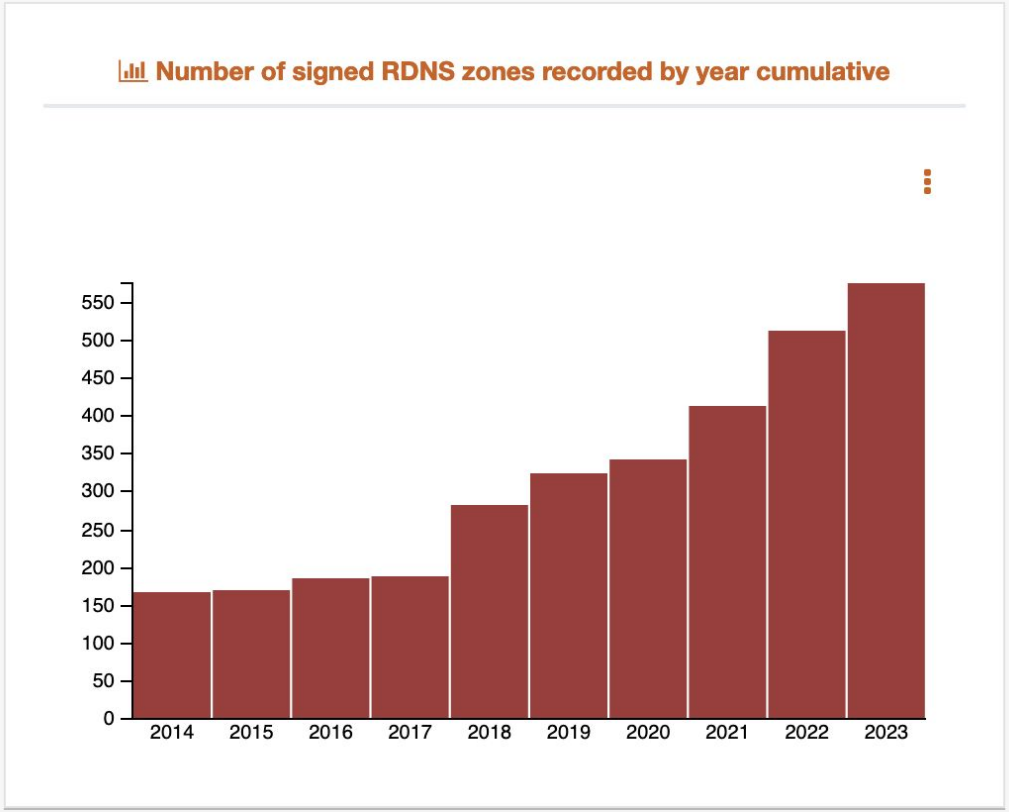
```
124.192.196.in-addr.arpa. 1199 IN DNSKEY 257 3 8 (
            AwEAAek9JqU5hoUGLd0PQpHGdUj2/pzuDsxitQqEoTfT
            Fn3qqpb0GlfdKjs4cbA8G7CQki4QUzBAWR98L5d58AxG
            r0VO3XrK/EBnN850E2lt/UKMss8V6a3Xro24/s96Qd6s
            eydv7IDaE6jApK1h/jAFEFyNuKX13brL9ZvJzod17ar8
            b3dDx9CeO8uqNQE0uuJ9o+/k9kqyWrCdRXnsNBC/ioR9
            yIUH4k/JAdPdKYnaToi1x2bLHjklmS8IoIauLxWgcykZ
            IZZHREdmMFjvKfmDJXMk/VibLqqv0/TDUsmLgURytH2y
            iOr9ELxpLHKqO89bPiGyLCSNjpy/gCodySv4QcM=
            ) ; KSK; alg = RSASHA256 ; key id = 10867
124.192.196.in-addr.arpa. 1199 IN DNSKEY 256 3 8 (
            AwEAAdRuw+dIPK6INzjKJXW0ypKZhTLq7BzB2Jx14D5f
            frrvoTkG6hG5l4am8cwuTSWXDHGinXSQm5UJMIYPYdad
            PYfoyq0ZIbBgQrp8Wkhe8HULg56NiroiT2gAbTvro85v
            71XKQskWS7mxSl+5qOuEcGqP3xjpLF+onpVSwpTwoKs5
            ) ; ZSK; alg = RSASHA256 ; key id = 49219
```

rDNS DNSSEC Validation …continued



DNSVIZ validation tool
https://dnsviz.net

DNNSEC Adoption in the AFRINIC region



- Numbers still low
- Operations require skills
- Capacity building efforts

Questions?


GOVERNANCE
E-LEARNING
ACADEMY
POLICY
ASNs
COMMUNITY
SOFT-LANDING
INNOVATION
BYLAWS
RESEARCH
NETWORK
Connecting
Africa
RIR
We distribute
Internet Number Resources
that network society
IP
MAINTAINER
ADDRESS BLOCKS
INTERNET RESOURCES