

# DNSSEC: worth adding to your cybersecurity strategy

## Presentation

Yazid Akanho

ICANN Office of the CTO

March 2025



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

**RSAC 2022: The Rise of DNS-Based Attacks**

Kory Underdown  
June 14, 2022

With RSAC 2022 behind us, we're reflecting on one of the most important themes at the conference: Rising DNS-based attacks.



## Akamai's Insights on DNS in Q2 2022



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 ...

## DNS-Based Attacks are on the Rise

DNS is an often-overlooked component of the security stack. But 70% of attacks involve the DNS layer in some way. Attacks are either launched via deceptive sites, or websites are used in malware exploits. And of course, many sites are leveraged as a way of spreading malware or phishing, despite that site not being deceptive on its own.

Further analysis on the most reused kits in Q2 2022, counting the number of different domains used to deliver each kit, shows that the **Kr3pto** toolkit was the one most frequently used and was associated with more than 500 domains (Figure 6). The tracked kits are labeled by the name of the brand being abused or by a generic name representing the kit developer signature or kit functionality.

In the case of Kr3pto, the actor behind the phishing kit is a developer who builds and sells unique kits that target financial institutions and other brands. In some cases, these kits target financial firms in the United Kingdom, and they **bypass MFA**. This evidence also shows that this phishing kit that was initially created more than three years ago is still highly active and effective and being used intensively in the wild.

## 300% Increase in Phishing Attacks

Phishing, along with other deceptive categories on our network, has grown over the last few years. According to **Trend Micro**, 90% of cyberattacks begin as spear phishing emails. Many of these emails opt for links as opposed to attachments, because it's much easier to convince someone to click a link. Attachments are inherently suspicious, and links are harder to catch so it makes sense that threat actors are favoring phishing emails with links—often taking their time to impersonate someone ahead of asking for anything.

## New cyber threats exploit and abuse DNS

In 2021, **44% of organizations** identified DNS-based attacks as one of their top security challenges. A quick look back over the past year makes the reasons clear.

<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/>

Blocking Threats at the DNS Layer is Necessary

Threats are increasing daily, and prioritizing protection against DNS-based threats should be on the mind of every cybersecurity professional. Secure your organization with DNSfilter for 14 days free.

# 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.
- ⦿ Helps increase **security and reputation** on the Internet, provides more **online trust** and **confidence**.
- ⦿ **Complementary** to other technologies like SSL widely used to secure web communications.

# How does DNSSEC work ?



**Two actions** are required :

- ⦿ Registry operators and Registrants should **sign their domain**: generate and maintain the cryptographic keys as well as signatures for the zone. Registrars and DNS hosting providers should facilitate.
- ⦿ DNS operators, ISPs, mobile operators, hosting providers, companies, ... should **activate DNSSEC validation** for **signed domains** (to verify authenticity of DNS data from signed zones) in their recursive resolvers: system administrators should turn on the functionality.
- ⦿ Signing and validation **complement each other**: one without the other is **like nothing done**.

# 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.

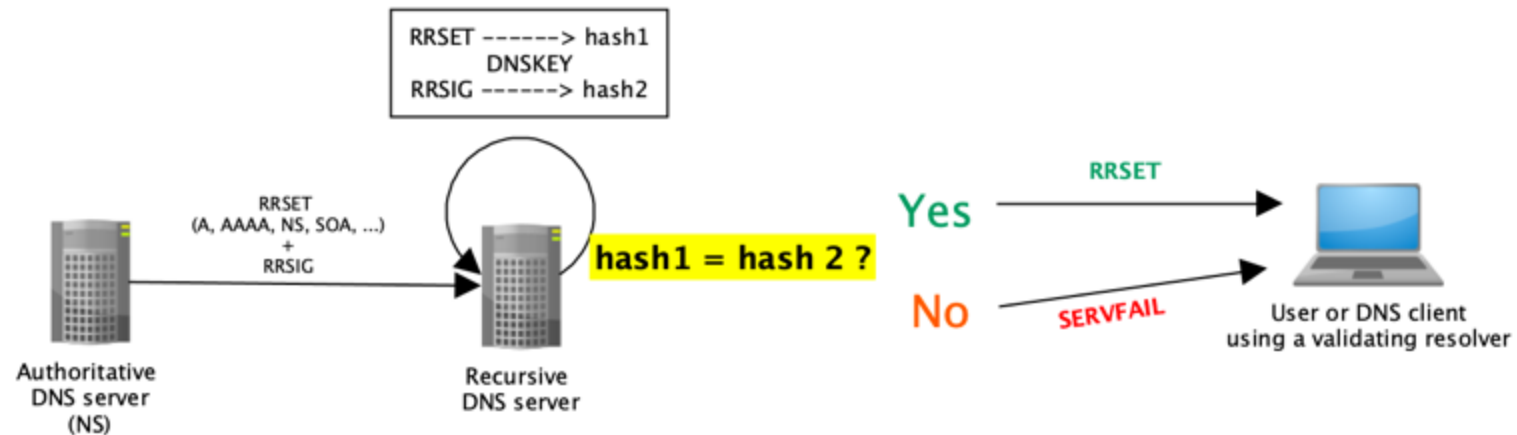
# DNSSEC signing: technical high level overview

---

- ◉ What/how is the existing DNS infrastructure ?
- ◉ Plan and get prepared
- ◉ Involve partners: 3<sup>rd</sup> 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:
  - $\approx 31\%$  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 in your country

---

Live demo 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](mailto: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

---

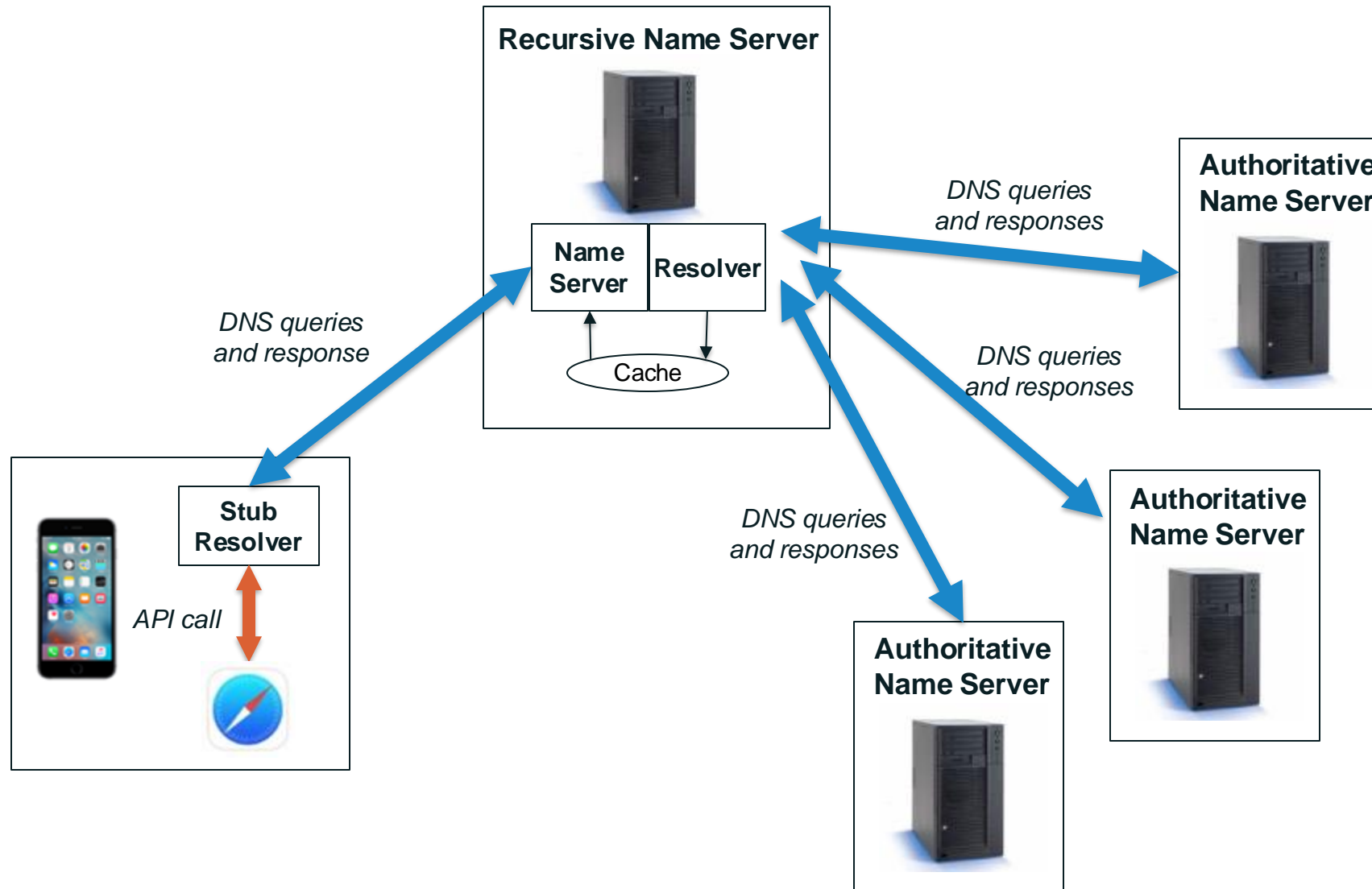
1. Are you interested in activating DNSSEC validation ?
2. If yes, let's work together with your DNS team

# DNSSEC Validation

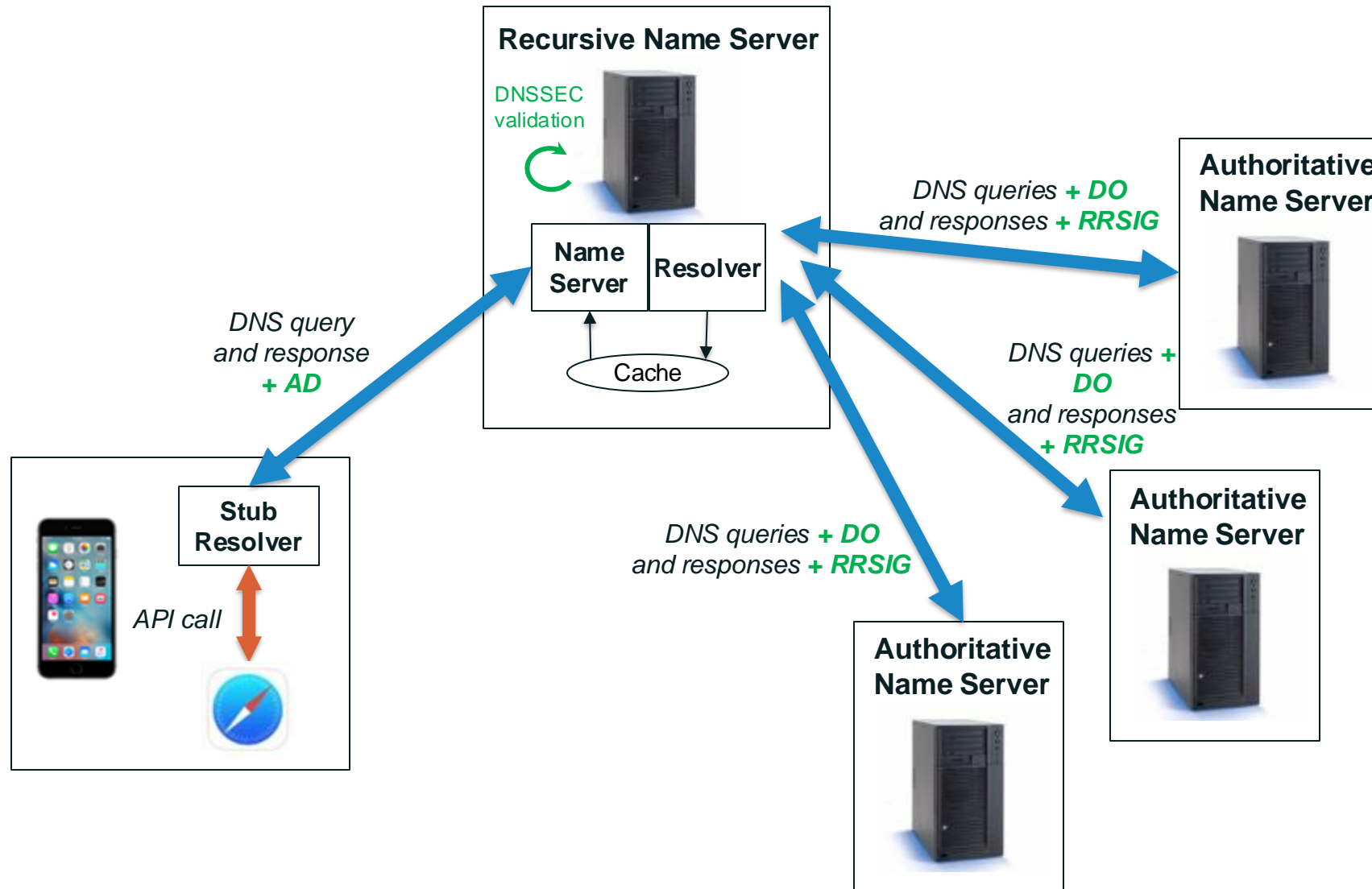
DNSSEC enabled - resolvers in action



# 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-optimize/>

# 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

**Basic**

Zone-signing Key Rollover Interval\* 1 month(s)

Signature Validity\* 4 day(s)

Zone-signing Key rollover method

☐ Pre-publish

☒ Double sign

NSEC3 salt length\* Min 1 Max 15 octets

Changing the settings for the NSEC3 number of iterations is not recommended.

Number of NSEC3 hashing iterations\* 10

Apply the selected policies/rules to queries requesting DNSSEC records:

☐ Response Policy Zones (RPZ) policies

☐ Blacklist rules

☐ DNS64 Groups

☒ Enable DNSSEC validation

☐ Accept expired signatures

Trust Anchors

Zone	Secure Entry Point	Algorithm	Public Key
<input checked="" type="checkbox"/> .	<input checked="" type="checkbox"/>	RSA/SHA-256 (8)	AwEAAgAIIKIVZrpC6la7gEzahOR+9W29euxhJhVVLOyQbSEW008...

# Enable DNSSEC Validation in Infoblox

- ◉ Ascertain Root Key (Trust Anchor):

```
AwEAAagAIKIVZrpC6la7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGC  
zh/RStloO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6  
CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0s  
GlcGOYI7OyQdXfZ57relSQageu+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](https://icann.org)



@icann



[facebook.com/icannorg](https://facebook.com/icannorg)



[youtube.com/icannnews](https://youtube.com/icannnews)



[flickr.com/icann](https://flickr.com/icann)



[linkedin/company/icann](https://linkedin/company/icann)



[slideshare/icannpresentations](https://slideshare/icannpresentations)



[soundcloud/icann](https://soundcloud/icann)