

KINDNS

KINDNS

An Initiative to Promote DNS Operational Best Practices

Ulrich Wisser
Technical Engagement Manager, Europe
ICANN

What Is It?

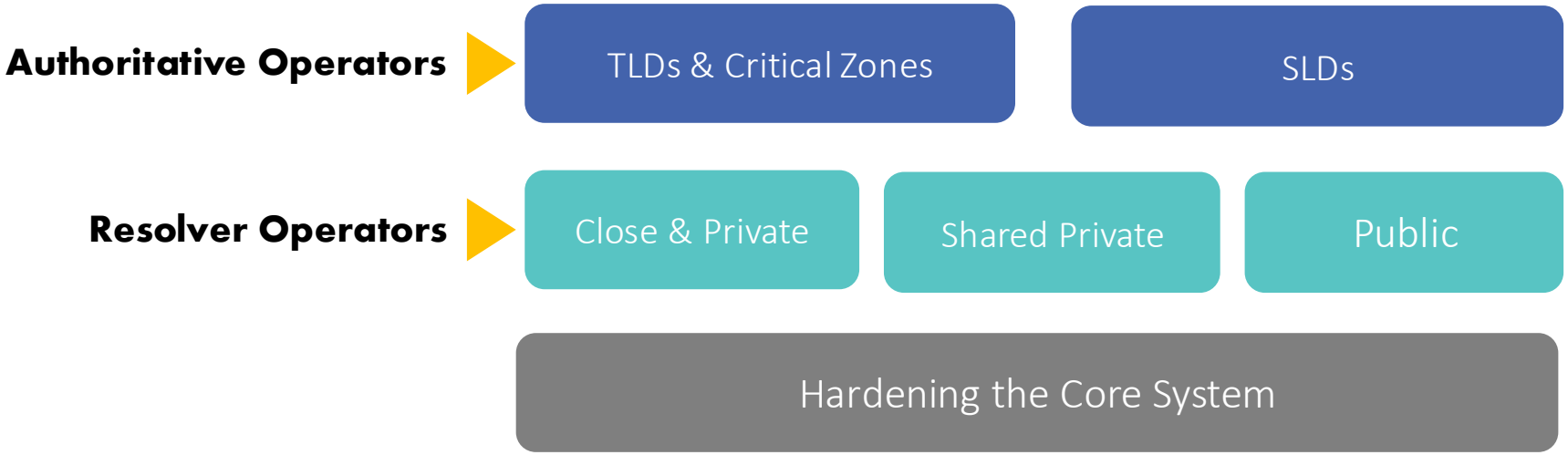
Knowledge-sharing and **I**nstantiating **N**orms for **D**NS
(Domain Name System) and **N**aming **S**ecurity

A simple framework that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices that the industry identifies for better security and more effective DNS operations.

***.....** is pronounced "**kindness**"*

KINDNS

Targeted Operators



- Each category has 6-8 practices that we will encourage operators to implement. See www.kindns.org, for more details
- By joining KINDNS, DNS operators are voluntarily committing to adhere to these identified practices and act as "goodwill ambassadors" within the community.

KINDNS

Authoritative DNS Operators of Critical Zones

TLDs & Critical Zones

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

KINDNS

Authoritative DNS Operators of SLDs

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

KINDNS

Closed & Private Resolver Operators

Private resolvers are not publicly accessible and cannot be reached over the open internet. They are typically found in corporate networks or other restricted-access networks

Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled
2. Access control list **(**ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that makes up your DNS infrastructure **MUST** be monitored
7. DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **SHOULD** be enabled

KINDNS

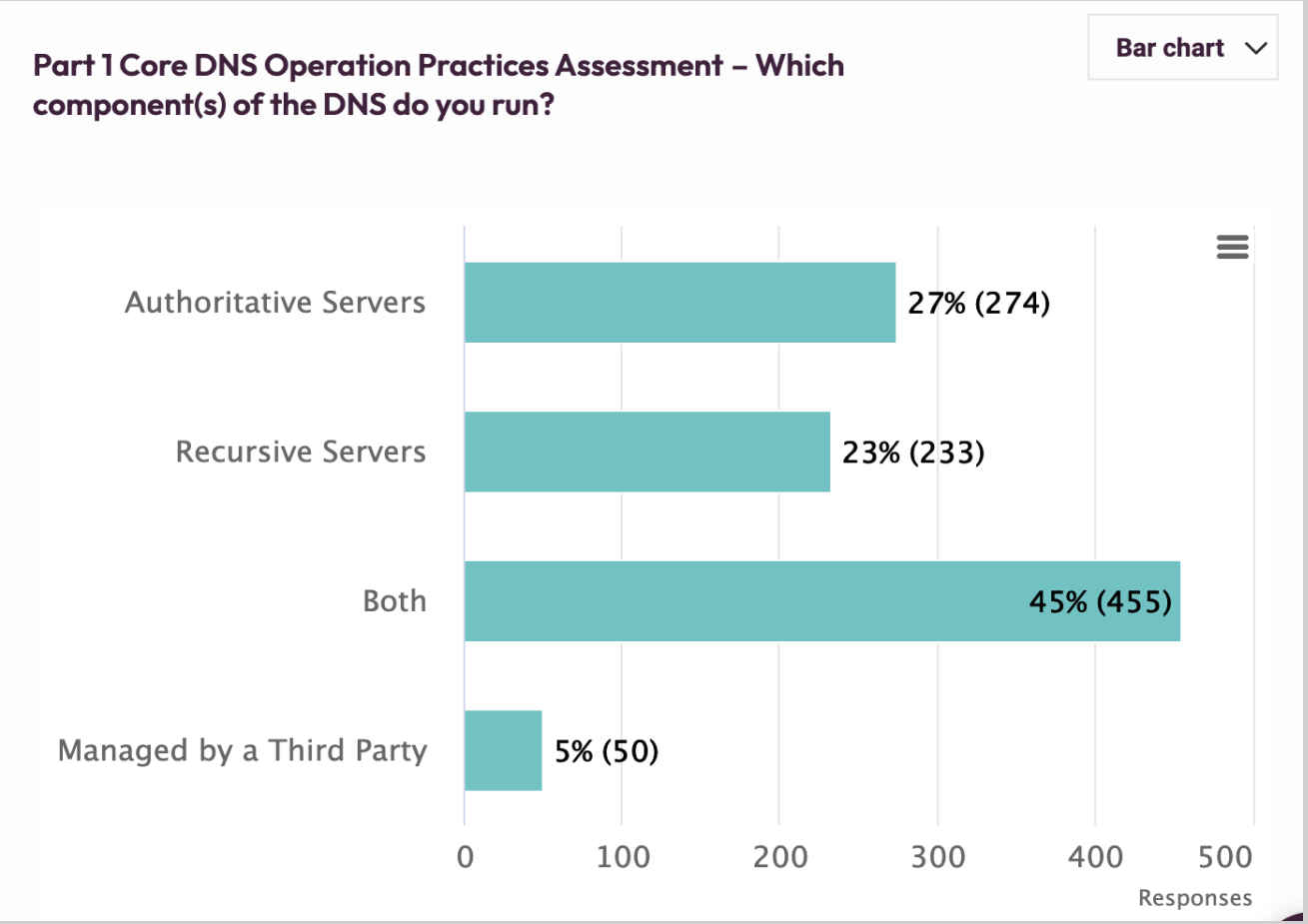
Public Resolver Operators

“Fully open” public DNS resolvers are available to any users on the Internet freely to use, whether they are stub resolvers (clients) or recursive servers using the open resolver as a forwarding service.

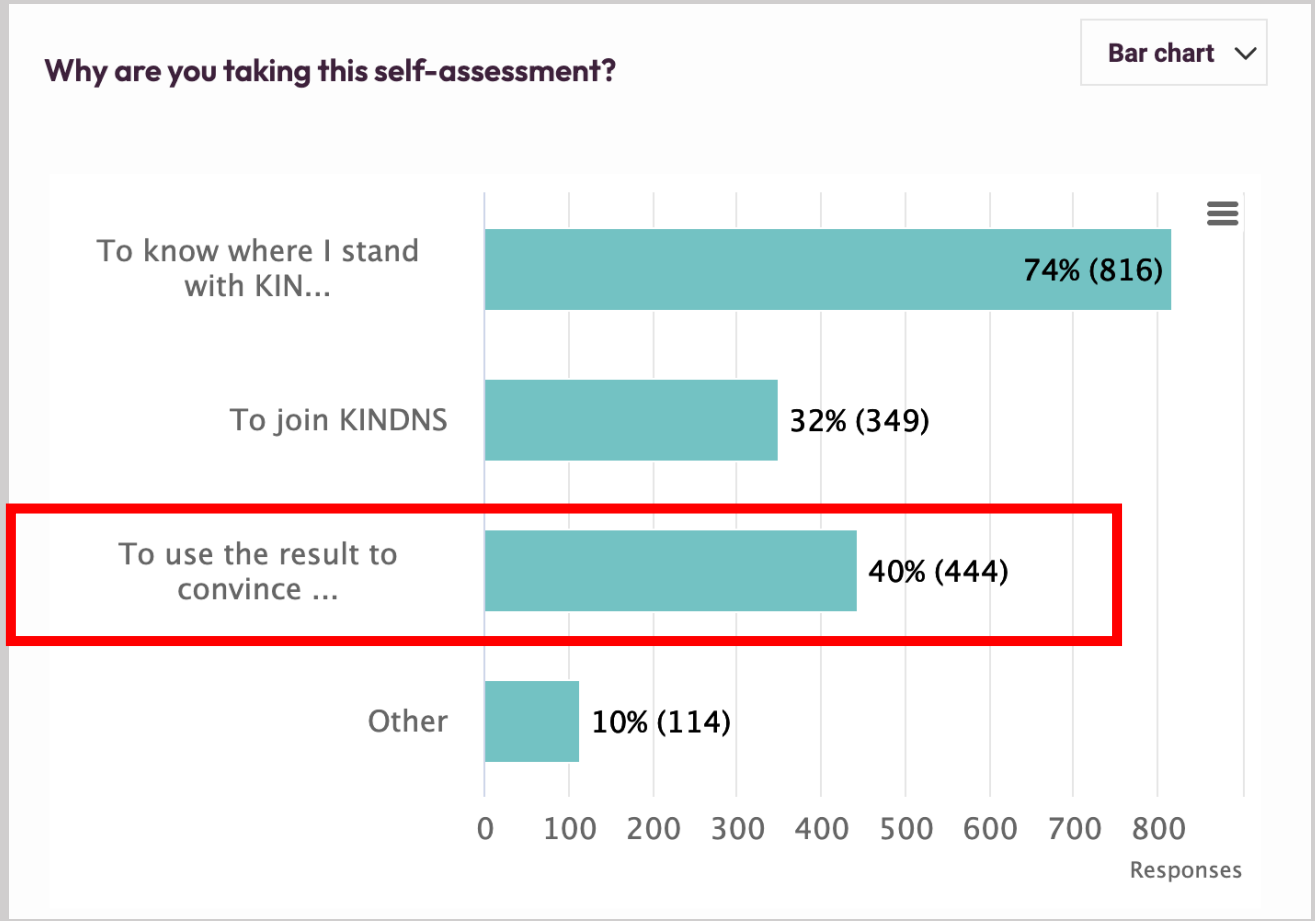
Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled
2. DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **MUST** be enabled
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that makes up your DNS infrastructure **MUST** be monitored
7. DNS Query data **MUST** only be retained for as long as is necessary for the sound operation of the service offered

KINDNS


Part 1 Core DNS Operation Practices Assessment – Which component(s) of the DNS do you run?
Bar chart
Authoritative Servers
27% (274)
Recursive Servers
23% (233)
Both
45% (455)
Managed by a Third Party
5% (50)
0
100
200
300
400
500
Responses

KINDNS

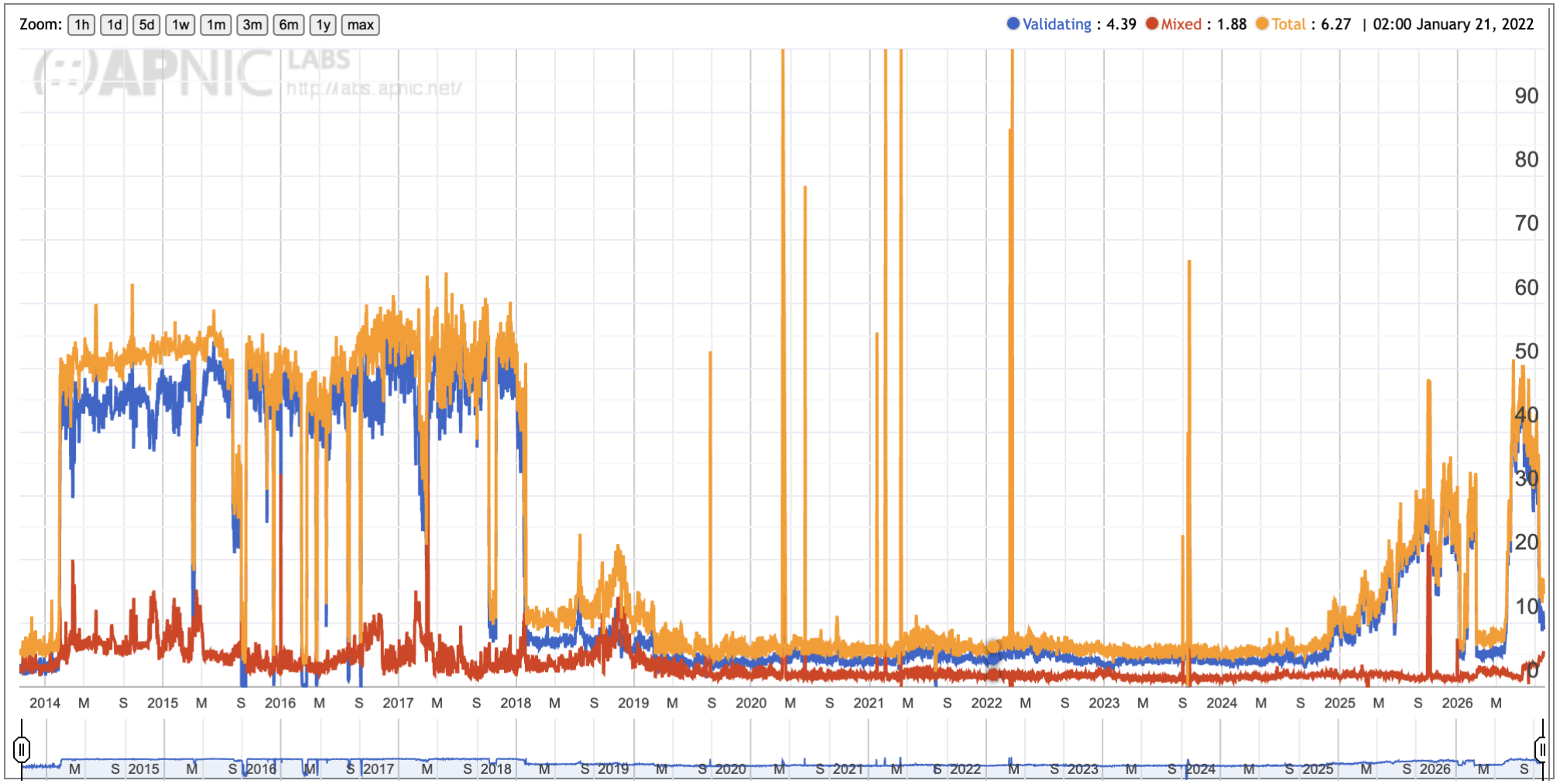

Why are you taking this self-assessment?
Bar chart
To know where I stand with KIN...
74% (816)
To join KINDNS
32% (349)
To use the result to convince ...
40% (444)
Other
10% (114)
0
100
200
300
400
500
600
700
800
Responses

DNSSEC Statistics



KINDNS

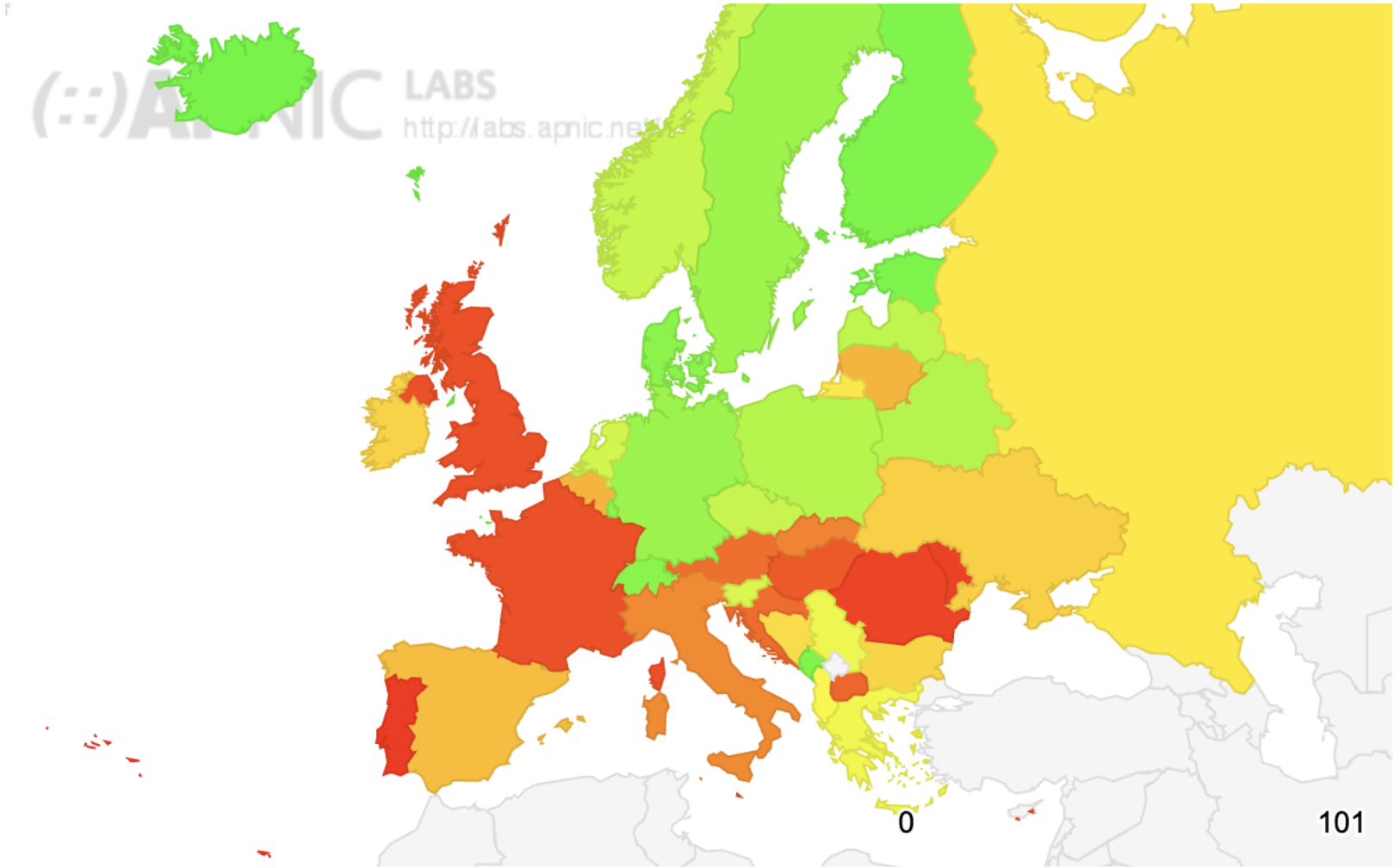
Use of DNSSEC Validation for Romania



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

KINDNS

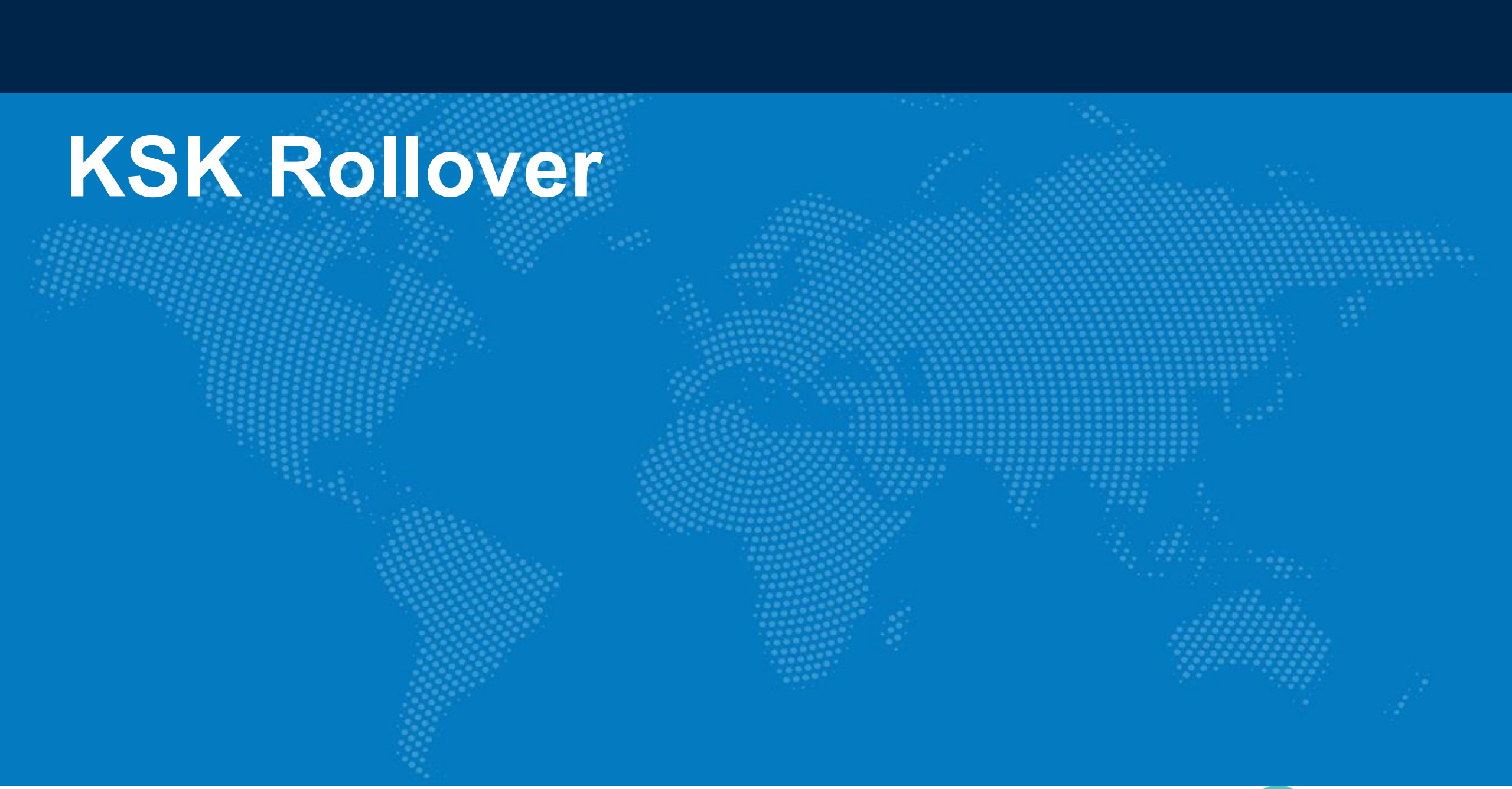
Use of DNSSEC Validation for Europe



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

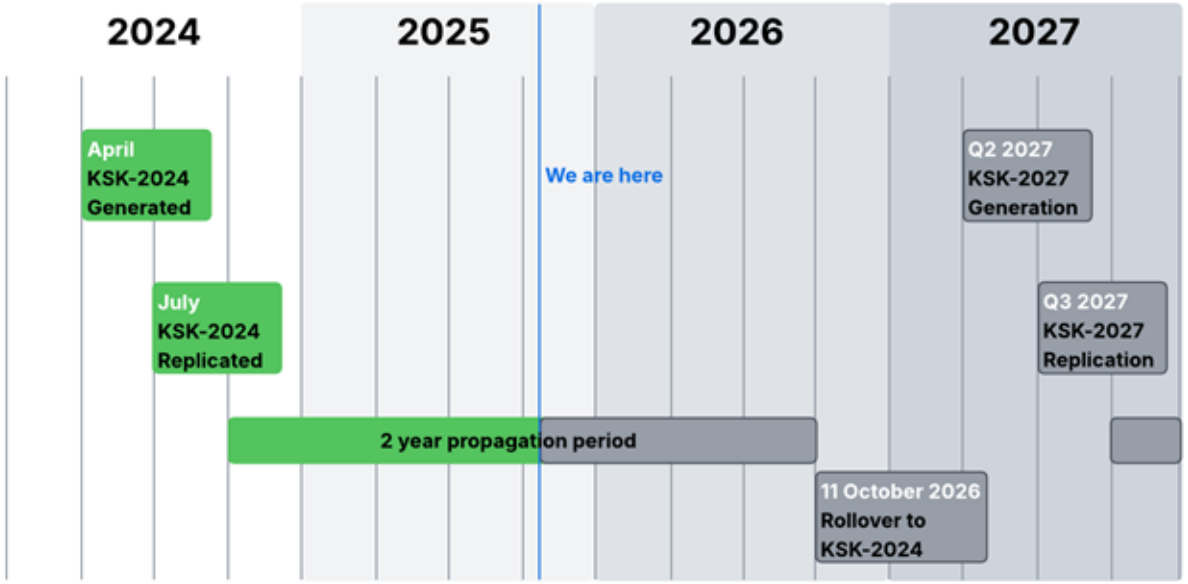
KINDNS

KSK Rollover



KSK Rollover

- Introduces a new Root Zone KSK (KSK-2024)
- Updates the DNS root trust anchor
- Gradually transitions systems to trust the new key



Key status

This table provides information on the keys generated for Root Zone KSK operations. Software implementers should rely on the XML trust anchors file for normative parameters on keys.

INFORMAL NAME	STATUS	DETAILS
KSK-2024	Pre-Publication	Generated 2024-04-26 (attestation) with key tag 38696 and label Kmyv6jo. Expected to supersede KSK-2017.
KSK-2017	Active	Generated 2016-10-27 (attestation) with key tag 20326 and label Klajeyz. Signing since 2018-10-11.
KSK-2023	Abandoned	Generated 2023-04-27 (attestation) with key tag 46211 and label Kmrfl3b. Will not be used, superseded by KSK-2024.
KSK-2010	Retired	Generated 2010-06-16 (attestation) with key tag 19036 and label Kjqmt7v. Signing between 2010-07-15 and 2018-10-11.

KINDNS

Trust Anchor Management

Trust anchors are critical for validation

Resolvers using RFC 5011 can:

- Automatically learn new trust anchors
- Update trust anchors without manual intervention

Resolvers not using RFC 5011 may require:

- Manual trust anchor updates
- Configuration validation
- Additional operational testing

Risk: Resolvers without the new trust anchor may return SERVFAIL responses

KINDNS

Operator Preparation Checklist

Preparation checklist

- ✓ Verify RFC 5011 support
- ✓ Confirm trust anchor configuration
- ✓ Test validating resolvers
- ✓ Review monitoring and alerting
- ✓ Update operational documentation
- ✓ Follow ICANN and IANA updates

KINDNS

Checking my Resolver Readiness

KINDNS

Let’s check if your resolver does do DNSSEC

Run the following command for all your Resolvers, where you replace <ip-address> with the IP address of each resolver.

dig @<ip-address> dnssec-failed.org +dnssec

If the answer contains status: SERVFAIL
Your resolver does do DNSSEC validation and you should follow on with this guide.

If you got an answer with an IP address, your resolver does not perform DNSSEC validation and you don’t need to do anything about the Root-Key rollover. But you should of course consider switching on DNSSEC validation.

KINDNS

DNS as a Service

Protective DNS is used by many organizations.
Obviously you can't do anything about the Root KSK Rollover as you don't run DNS Resolvers your own, but you can ask your service provider what they are doing.

KINDNS

Commercial Software

If you use a commercial software the new key should already be included in one of your latest updates. You should install the latest updates and if you for some reason can’t do that, you should plan for an update some time before 11 October 2026. Talk to your vendor about the Root KSK Rollover and ask in what update the new key is/will be included.

KINDNS

New Trust Anchors, where to find them

You can use *curl* or *wget* to obtain the official trusted anchors file in XML format directly from the IANA data repository:

```
curl -O https://data.iana.org/root-anchors/root-anchors.xml
```

KINDNS

New Trust Anchors, where to find them

You can use a command similar to the following to extract all the keys in the generally accepted format for the BIND Resolver configuration for example:

```
awk '/<KeyDigest/,/<\/KeyDigest>/ {print}' root-anchors.xml | awk '
/<\/KeyDigest>/ { if(tag!="") print "    . static-ds " tag " " alg " " type " \"" dig
"\";"; tag=""; alg=""; type=""; dig="" }
/<KeyTag>/ {gsub(/<\/?KeyTag>/,""); gsub(/[ \t]/,""); tag=$0}
/<Algorithm>/ {gsub(/<\/?Algorithm>/,""); gsub(/[ \t]/,""); alg=$0}
/<DigestType>/ {gsub(/<\/?DigestType>/,""); gsub(/[ \t]/,""); type=$0}
/<Digest>/ {gsub(/<\/?Digest>/,""); gsub(/[ \t]/,""); dig=$0}
'
```

You should get something similar to this:

```
. static-ds 19036 8 2 "49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5";
. static-ds 20326 8 2 "E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457104237C7F8EC8D";
. static-ds 38696 8 2 "683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A4C0FB2B16";
```

KINDNS

Open Source Software: BIND

There are several methods of configuring DNSSEC validation in BIND.

1. Please check your BIND configuration for the following statement “dnssec-validation auto;”.
   BIND will update the trust-anchor automatically. In the latest versions of BIND this configuration is the default. If “dnssec-validation” is not configured at all, it means you are on “auto”.

2. If your configuration says “dnssec-validation yes;” please consider changing to “auto”.
   If you can’t change to “auto” you will need to update the key file manually. Please see below for the correct content.

3. If your bind configuration contains a section called “trust-anchors”
   a. you should have a list of keys, which starts with “. initial-ds” or “. initial-key”.
   b. If you see a definition containing “. static-ds” or “. static-key” you need to either change the “static” to “initial” or add the new key manually to your configuration.

KINDNS

Open Source Software: BIND

4. **Run “rndc managed-keys status”**
   It should display two keys, one with keyid 20326 (current KSK from 2017 to be replaced) and one with keyid 38696 (new replacement KSK 2025).

5. **Run “rndc secroots”**
   It writes a file called “named.secroots” (see below for folders to check). It should contain two keys as
   ./RSASHA256/20326
   ./RSASHA256/38696

6. If you do not use views, your current initial set of trust-anchors should be in a file named “bind.keys” (usually in /etc/bind) and the dynamic set of trust-anchors “managed-keys.bind” (usually in /var/cache/bind), usually found where your bind configuration lives. If you use views, you should have one or more “.mkeys” files. Check the files, they should contain two keys.

Open Source Software: BIND

Here is an example of the file bind.keys contents that is created by a current version of bind when you first install bind on a machine:

```
trust-anchors {
        # This key (20326) was published in the root zone in 2017, and
        # is scheduled to be phased out starting in 2025. It will remain
        # in the root zone until some time after its successor key has
        # been activated. It will remain this file until it is removed
        # from the root zone.
        . initial-key 257 3 8 \
              "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
               +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
               ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
               0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
               oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
               RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
               R1AkUTV74bU=";

        # This key (38696) will be pre-published in the root zone in 2025
        # and is scheduled to begin signing in late 2026. At that time,
        # servers which were already using the old key (20326) should roll
        # seamlessly to this new one via RFC 5011 rollover.
        . initial-ds 38696 8 2 \
              "683D2D0ACB8C9B712A1948B27F741219298D0A450D612C483AF444A
               4C0FB2B16";
};
```

KINDNS

Open Source Software: UNBOUND

There are several methods of configuring DNSSEC validation in unbound.

1. **Please check your unbound configuration for the following statement "auto-trust-anchor-file:" Unbound will update the trust-anchor automatically. Check the file for correct contents.**
2. **If your configuration uses "trust-anchor-file:" or "trusted-keys-file:" statements please consider changing to auto-trust-anchor-file. If you can't change to auto-trust-anchor-file you will need to update the key file manually. Please see below for the correct content.**
3. **If your unbound configuration contains "trust-anchor:" the keys are defined explicit. Check that both keys (keyid 20326 and 38696) are in the list. Preferably switch to "auto-trust-anchor-file:".**

KINDNS

Open Source Software: UNBOUND

Depending on the configuration statement you use, please check the file configured to have a content similar to the content below.

```
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1773685071 ;;Mon Mar 16 18:17:51 2026
;;last_success: 1773685071 ;;Mon Mar 16 18:17:51 2026
;;next_probe_time: 1773728077 ;;Tue Mar 17 06:14:37 2026
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
.     3600  IN    DNSKEY     257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExO
LAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3E
gVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6n
WeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555
KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ;{id = 20326 (ksk), size = 2048b}
;;state=2 [  VALID  ] ;;count=0 ;;lastchange=1773667482 ;;Mon Mar 16 13:24:42
2026
.     3600  IN    DNSKEY     257 3 8
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJNnOAlFNKF2j
BosZBU5eeHspaQWOmOElZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vrhbu6irwCzVBApESjbUdpWWmE
nhathWu1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge71M3ej2/7CPqpdVwuMoTvoB
+ZOT4YeGyxMvHmbrxlFzGOHOijtzN+u1TQNatX2XBuzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxPvYLw
4z9mR7K2vaF18UYH9Z9GNUUeayffKC73PYc= ;{id = 38696 (ksk), size = 2048b}
;;state=2 [  VALID  ] ;;count=0 ;;lastchange=1773667482 ;;Mon Mar 16 13:24:42
2026
```

KINDNS

Open Source Software: UNBOUND

Finally run

```
dig @<ip-address> trustanchor.unbound CH TXT +noall +nocomments +answer
```

Against your resolver. The answer should contain one line with

```
trustanchor.unbound. 0 CH TXT ". 20326 38696"
```

KINDNS

Open Source Software: KNOT

Since version 4.0 Knot Resolver has switched on DNSSEC validation by default. No trust-anchor file is needed, everything is compiled into the executable.
Check your configuration for any appearance of "trust_anchors". Please check with the Knot documentation at https://knot-resolver.readthedocs.io/en/stable/config-dnssec.html how to proceed.

There is an undocumented way of checking (given to us by the Knot developers), this may or may not work in your version of the knot-resolver.

```
$ echo 'trust_anchors.summary()' | sudo socat - /run/knot-resolver/control/0
```

```
.                       86400   DNSKEY  257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExO
LAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3E
gVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+eoZG+SrDK6n
WeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555
KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ; Valid: ; KeyTag:20326
.                       86400   DNSKEY  257 3 8
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJNnOAlFNKF2j
BosZBU5eeHspaQWOmOElZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vrhbu6irwCzVBApESjbUdpWWmE
nhathWu1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge71M3ej2/7CPqpdVwuMoTvoB
+ZOT4YeGyxMvHmbrxlFzGOHOijtzN+u1TQNatX2XBuzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxPvYLw
4z9mR7K2vaF18UYH9Z9GNUUeayffKC73PYc= ; Valid: ; KeyTag:38696
```

KINDNS

Open Source Software: PowerDNS

Please check your configuration for "`trustanchorfile`". It gives you the location of the file to check for the trust-anchors. Please make sure the file contains both keys, similar to

```
. IN DNSKEY 257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixH
lFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WG
e2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eN
buv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6
+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU= ; keytag
20326
. IN DNSKEY 257 3 8
AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJNnOAl
FNKF2jBosZBU5eeHspaQWOmOElZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vrhbu6irwCzVBA
pESjbUdpWWmEnhathWu1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUKEpUge71M3e
j2/7CPqpdVwuMoTvoB+ZOT4YeGyxMvHmbrxlFzGOHOijtzN+u1TQNatX2XBuzZNQ1K+s2CXk
PIZo7s6JgZyvaBevYtxPvYLw4z9mR7K2vaF18UYH9Z9GNUUeayffKC73PYc= ; keytag
38696
```

Open Source Software: PowerDNS

Additionally you can run

```
rec_control get-tas
```

The output should look like this

```
Configured Trust Anchors:
.
  20326 8 2
     e06d44b80b8f1d39a95c0b0d7c65d08458e880409bbc683457104237c7f8ec8d
  38696 8 2
     683d2d0acb8c9b712a1948b27f741219298d0a450d612c483af444a4c0fb2b16
```

When you restart your resolver, please check for a message saying something similar to

```
you need to update package with trust anchor
```

In that case you should strongly consider changing to an updated version of Knot Resolver. The new key is shipped with Knot since summer 2024.

KINDNS

Stay Informed and Contribute



Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Mailing list	kindns-discuss@icann.org

KINDNS