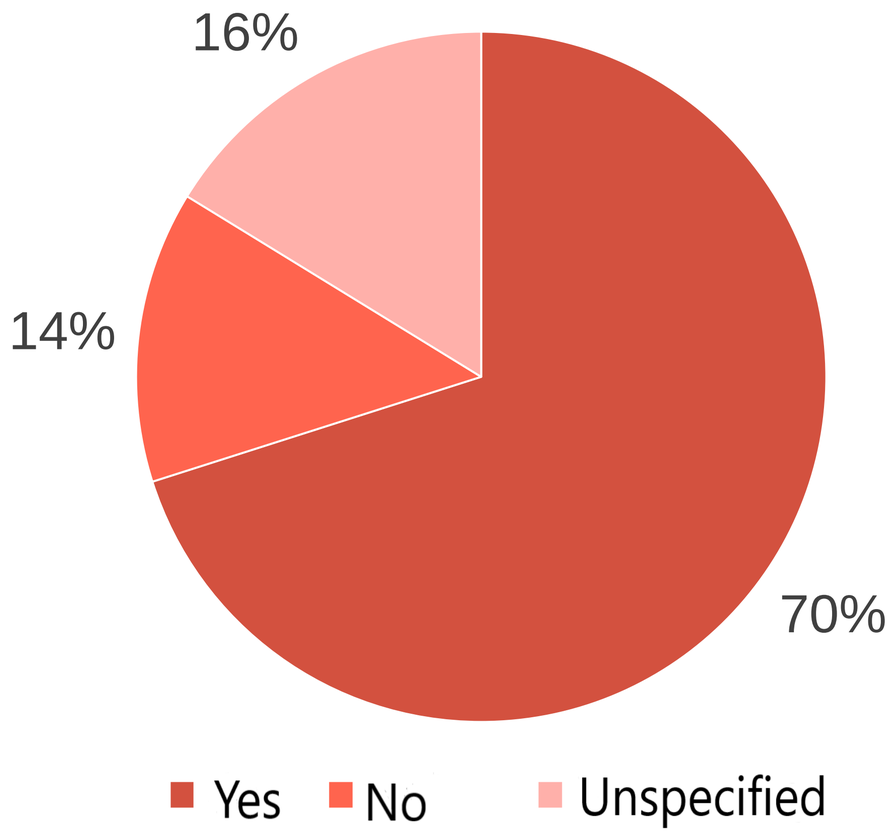
DNSSEC Adoption

The 2024 Survey of the eco topDNS Initiative

eco – Association of the Internet Industry

1. Do you feel adequately informed about DNSSEC?

Yes	70%
No	14%
Unspecified	16%



1.1 Comments: Do you feel adequately informed about DNSSEC?

Usually via relevant specialist articles or directly via sys4.de.

We already use DNSSEC for critical DNS zones.

As part of the OZG Security Challenge 2023 organised by the BMI, a very good one-pager was created. That helped!

Purpose and usefulness are still questionable, x509 is too complicated for that.

But are the others any better? Is it necessary? Do we really want another certification fiasco, as with BEA, electronic payment transactions and other aspects?

Yes

1.2 Comments: Do you feel adequately informed about DNSSEC?

We work with open protocols, so we take the initiative to review protocol updates. Naturally, sharing more information/knowledge is beneficial for all.

Yes we do, in fact the Stack PDNS+PHPIPAM works very well with DNSSEC, so every Services Provider *SHOULD* use it!

I’ve implemented the DNSSEC adoption program for .nl.

Primarily thanks to the .NL registry (SIDN).

We use a DNS provider (ironDNS) that has mastered DNSSEC for years. We chose it specifically because it has mastered DNSSEC for 10 years, handles TLSA records, and is based in Germany.

1.3 Comments: Do you feel adequately informed about DNSSEC?

We've been using DNSSEC for over 15 years.

DNSSEC has been used productively since 2018.

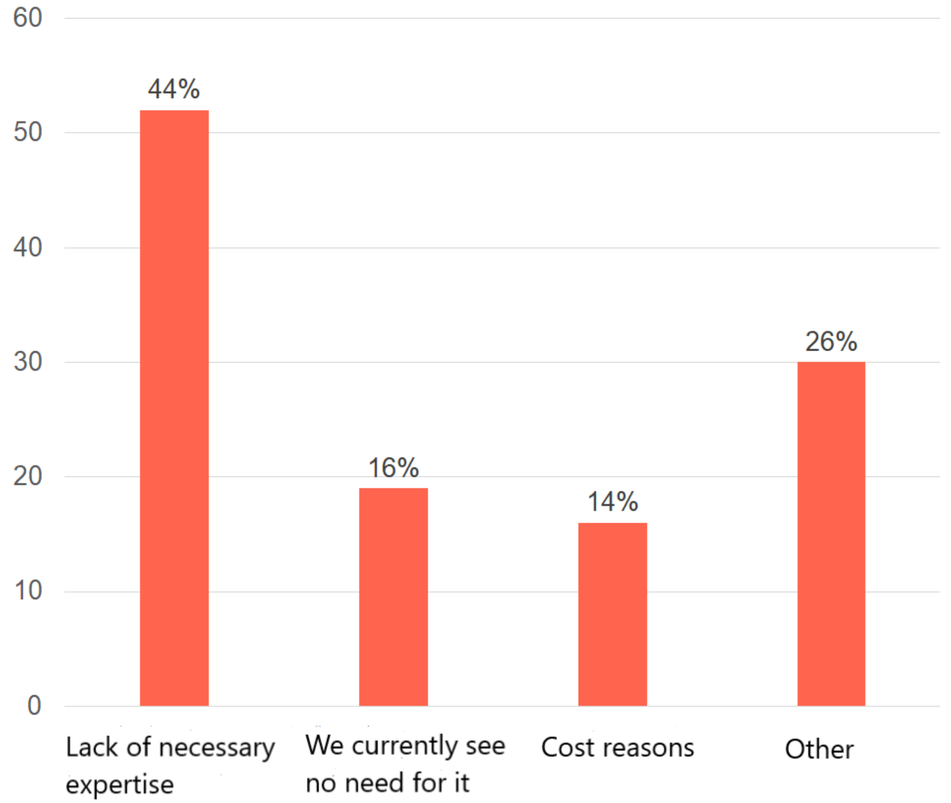
I develop DNS resolvers with DNSSEC validation for my paid job.

We sign and validate and encourage others to also do this.

Actively using it and installed for over 10 years.

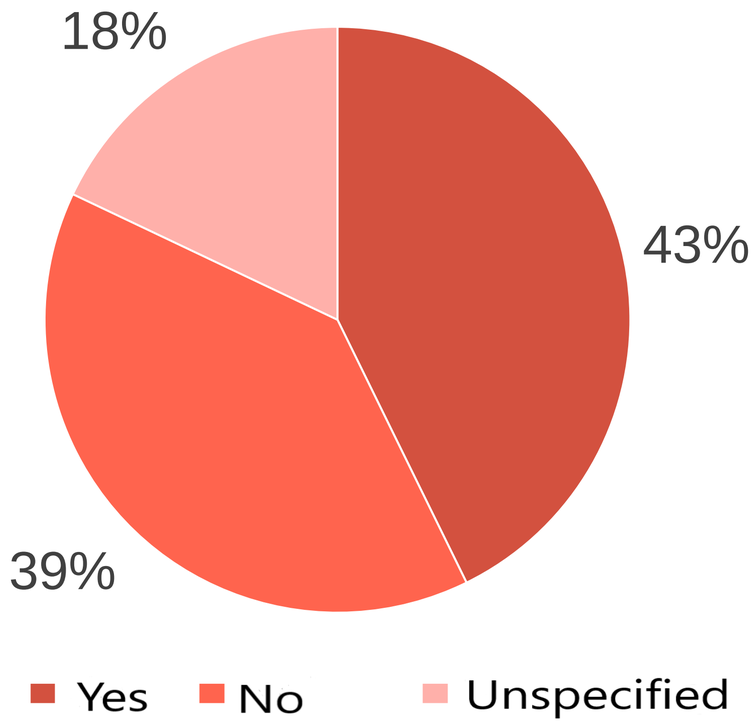
2. What stumbling blocks do you think stand in the way of widespread implementation?

Lack of necessary expertise	44%
We currently see no need for it	16%
Cost reasons	14%
Other	26%



3. Do you plan activities (e.g. introduction, expansion of use, etc.) regarding DNSSEC until 2026?

Yes	43%
No	39%
Unspecified	18%



3.1 Do you plan activities (e.g. introduction, expansion of use, etc.) regarding DNSSEC until 2026?

DNSSEC for rDNS.

We implement DNSSEC wherever feasible and encourage our customers to do the same.

We recommend enabling DNSSEC on our systems. We plan to make it default so that it needs to be de-activated in case a customer does not want to use it.

We have abandoned use of DNSSEC.

We are currently in beta phase.

Maybe with custom DNS servers, currently it´s managed.

3.2 Comments: Do you plan activities (e.g. introduction, expansion of use, etc.) regarding DNSSEC until 2026?

Extended use of DNSSEC planned.

Yes, I will continue signing my zones as I have for many years.

Yes, we plan to use DNSSEC for each and every domain that supports it. Sadly, there are still some TLDs that are not supporting DNSSEC. For new TLDs, it should be mandatory to have DNSSEC support.

We are satisfied with the 58% adoption rate in .nl.

DNSSEC is deployed. We validate on our resolvers, and our authoritative nameservers support DNSSEC. DNSSEC on the authoritative nameservers now is currently “opt-in”, but we plan to change it to “opt-out”.

We have already implemented DNSSEC everywhere possible.

3.3 Comments: Do you plan activities (e.g. introduction, expansion of use, etc.) regarding DNSSEC until 2026?

Already supporting it for most TLDs.

DNSSEC for customer domains is still on the agenda.

Already fully deployed.

We already sign all client domains on our NS, unless the client explicitly tells us not to.

There has been little take-up by larger security focused corporations like banks etc. It is mostly DNS hobbyists that are using the feature.

Opt Out for unsigned zones.

3.4 Comments: Do you plan activities (e.g. introduction, expansion of use, etc.) regarding DNSSEC until 2026?

We consider to use DNSSEC for 100% of all domains under management, from 2026 at the latest.

We've been using it since 2006, and it has saved us many times from what would have been horrible breaches. We definitely won't stop employing it ubiquitously until something better comes along.

Already using DNSSEC.

Already rolled out.

As a recursive operator, we welcome new updates to the DNSSEC protocol to increase software compliance and ease of use. We will work with our vendors and researchers to identify issues and resolve implementation challenges as any arise.

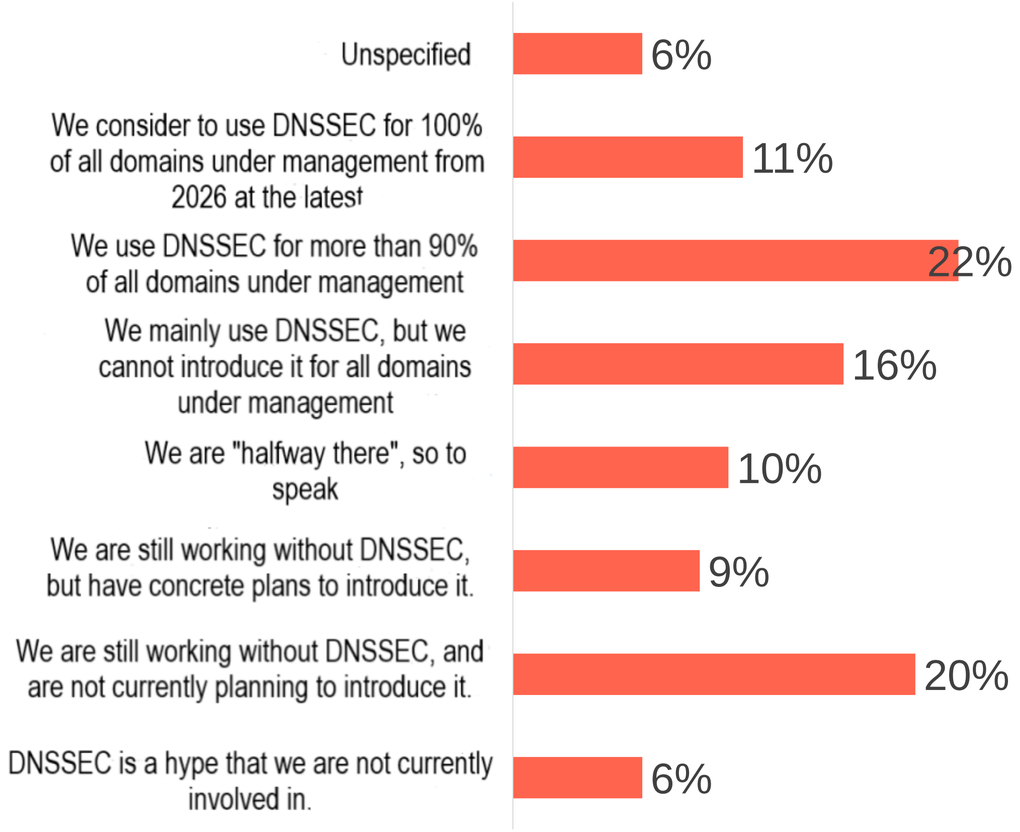
My DNS zones already use DNSSEC (self-hosted)

It's already at 100%.

Possible, it depends on the level of automation.

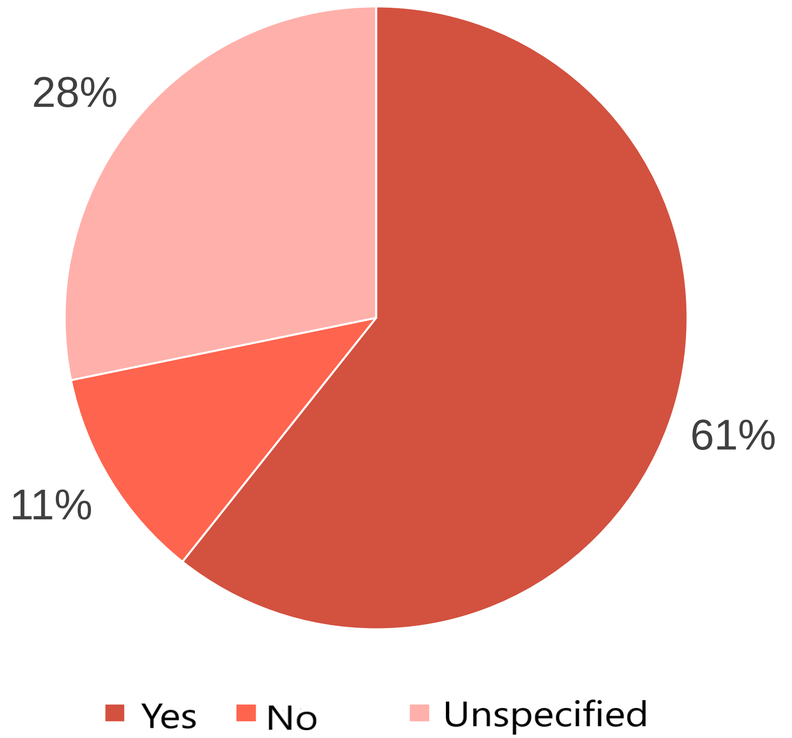
4. Which of the following statements apply most to you (multiple answers possible)?

DNSSEC is a hype that we are not currently involved in.	6%
We are still working without DNSSEC, and are not currently planning to introduce it.	20%
We are still working without DNSSEC, but have concrete plans to introduce it.	9%
We are “halfway there”, so to speak.	10%
We mainly use DNSSEC, but we cannot introduce it for all domains under management.	16%
We use DNSSEC for more than 90% of all domains under management.	22%
We consider to use DNSSEC for 100% of all domains under management from 2026 at the latest.	11%
Unspecified	6%



5. Should the eco Association become more involved in the wider use of DNSSEC?

Yes	61%
No	11%
Unspecified	28%



5.1 Comments: Should the eco Association become more involved in the wider use of DNSSEC?

Wrong association for technical definitions, their implementation and dissemination. (See Anti-Spam-Summit. The aim there was to make email more permeable without addressing the evaluation, if the recipient wants this. The General Data Protection Regulation achieved more!)

It is too complex.

It should be included as a mandatory criterion in various recommendations.

In particular for assistance of CDS/CDNSKEY support (RFC8078).

Possibly through the provision of information material.

100% - The EU needs to drive this.

5.2 Comments: Should the eco Association become more involved in the wider use of DNSSEC?

DNSSEC has failed. Stop throwing good money after bad.

I'm unable to answer this as I'm not sure what eco is, nor what it does. I would however welcome more adoption of DNSSEC from all parties.

Yes, please implement schemes that can motivate more German ISPs to implement features such as DNSSEC, IPv6, QUIC, DNS-over-TLS, etc. It's astonishing how many very big providers use none of these technologies and some very small providers use all of them. Also Germany desperately needs to increase the 4% DNSSEC pickup rate!

It should also engage in dialogue about ways to improve DNSSEC - see for example https://419.consulting/encrypted-dns/f/dnssec-non-deployment-what-can-be-done.

Very much so.

5.3 Comments: Should the eco Association become more involved in the wider use of DNSSEC?

Absolutely! Just yesterday, the media once again reported that providers are manipulating DNS queries. See the German media: https://www.golem.de/news/netzsperren-provider-kapern-dns-anfragen-an-google-und-cloudflare-2408-187859.html

eco should encourage registries to offer discounts for signed zones.

I favour the direction towards technologies like DANE and similar approaches - where ad-hoc certification is replaced by information that's directly in DNS (and secured by DNSSEC).

It's really a matter of spreading the understanding of what it does. Educate people, and they'll adopt it.

Resilience against DNS abuse is significantly improved with DNSSEC.

Absolutely!

6. My company is

Domain Name Registry	13%
Domain Name Registrar	9%
Reseller of domain names	4%
Hosting / Cloud service provider	21%
Email service provider	8%
DNS resolver operator	9%
No answer	36%