Report on DNSSEC Adoption

At the core of every Internet interaction is the **Domain Name System (DNS)** – but DNS, by itself, lacks built-in trust. This is where **Domain Name System Security Extensions (DNSSEC)** comes in: it ensures that DNS responses can be verified as authentic and untampered.

When your system receives a DNSSEC-verified DNS response, you can rest assured it was given by the authorized DNS server and the response has not been manipulated while it was in transit to your machine. You may safely use the given data and act upon it – for example, point your browser to your bank's online service and log in into your account. Or, if it's a DNS reply which could not be DNSSEC-verified, your system's resolver will suppress the information and foil a potentially harmful action.

Logically, DNSSEC is something everyone should want – it's about knowing and not just believing you're communicating with the right service.

In the eco Association, our Email, Anti-Abuse, and Names & Numbers Competence Groups have long been committed to the rapid and widespread introduction and use of DNSSEC. The extensions offer numerous advantages, such as:

- enabling of further security protocols such as DANE (DNS-based Authentication of Named Entities)
- increased trust and reliability on the Internet
- protection against falsified DNS responses
- protection against DNS cache poisoning
- prevention of Man-in-the-Middle attacks

In light of this, the eco Association recently conducted a survey to determine which hurdles are currently still preventing companies from introducing and using DNSSEC across the board. The Competence Groups want to use this to find out how companies that are still hesitant can be helped.

To deepen our understanding of current adoption challenges and to share findings directly with stakeholders, **eco hosted a members-only webinar on 15 March 2025**. The session offered an interactive exchange on the results of our DNSSEC survey and explored concrete steps toward broader implementation.

DNSSEC Adoption: Key findings from the webinar

The webinar was hosted by **Lars Steffen**, eco's Head of International, Digital Infrastructure & Resilience, and **Patrick Ben Koetter**, Leader of the eco Email

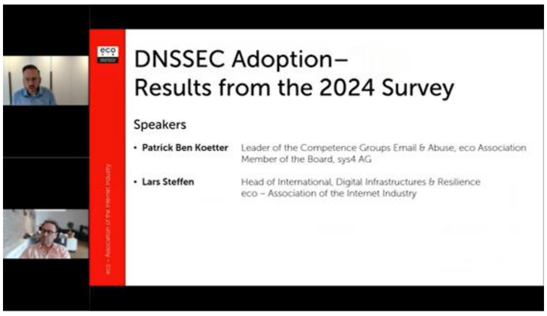
Competence Group. The two panelists discussed results from eco’s DNSSEC survey conducted from August through December 2024, which garnered approximately 120 respondents.

Webinar recording:

DNSSEC Adoption

The 2024 Survey of the eco topDNS Initiative

DNSSEC Adoption:



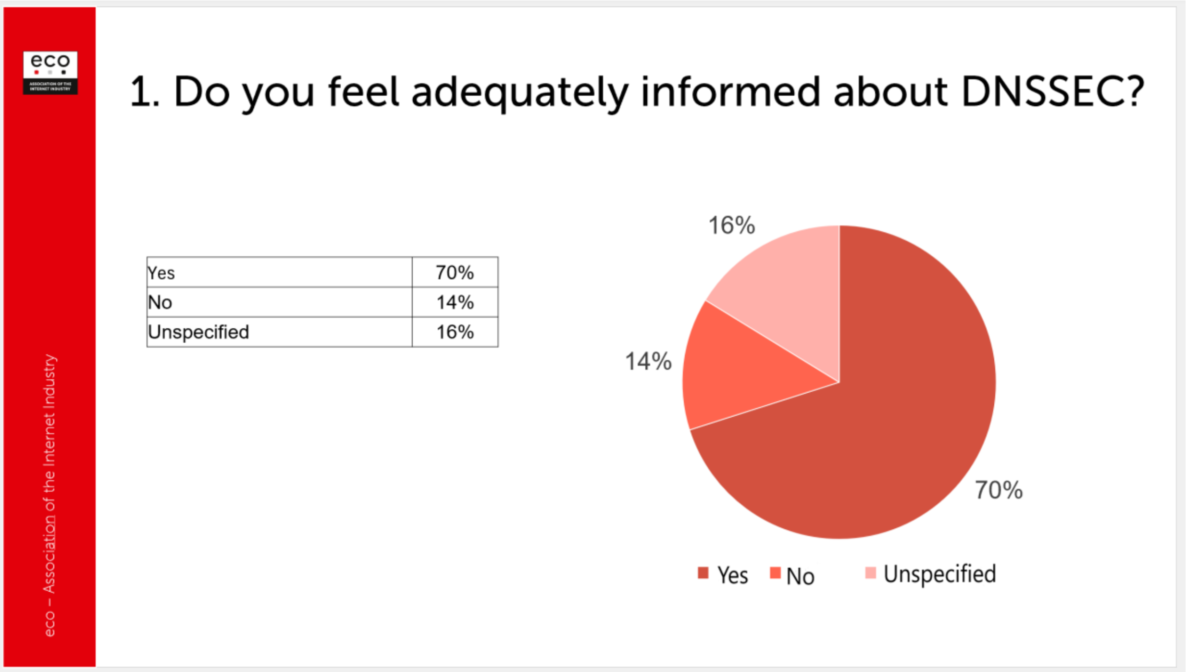
DNSSEC Adoption–
Results from the 2024 Survey

Speakers

- **Patrick Ben Koetter** Leader of the Competence Groups Email & Abuse, eco Association
Member of the Board, sys4 AG
- **Lars Steffen** Head of International, Digital Infrastructures & Resilience
eco – Association of the Internet Industry

At the webinar, a range of DNS and email security experts gathered to explore the current state of DNSSEC adoption and investigate why progress has stalled despite widespread awareness.

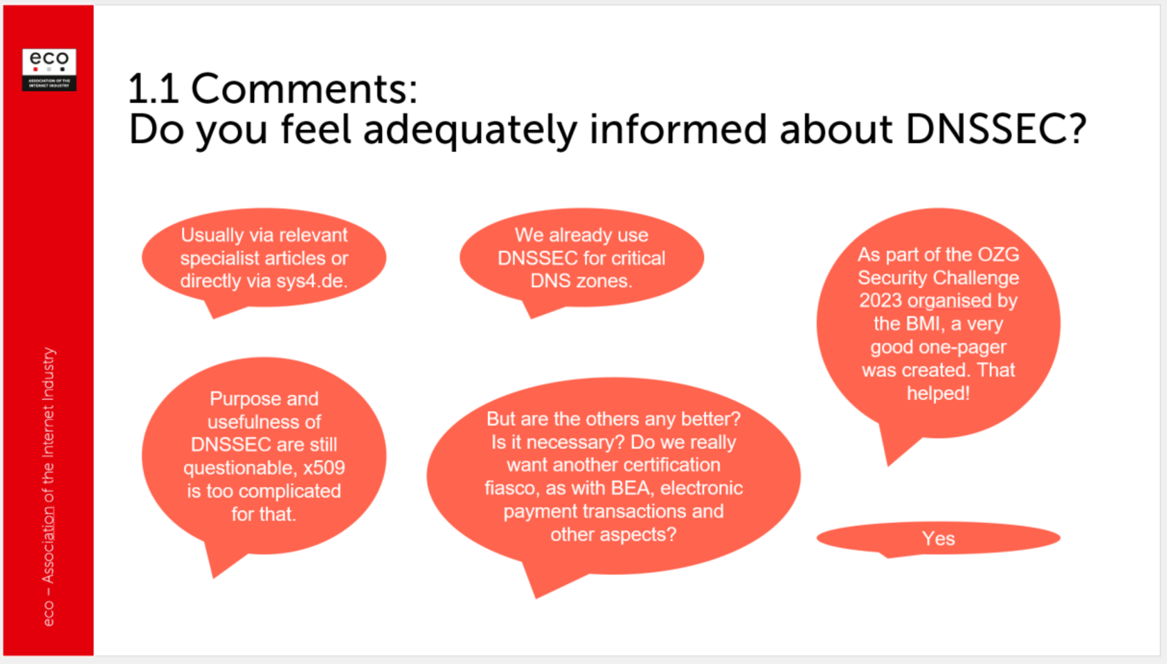
Slide 1 of the survey showed that while overall awareness of DNSSEC is relatively high – with 70% of respondents stating they feel adequately informed – 30% are either unspecified or feel uninformed.



1. Do you feel adequately informed about DNSSEC?

Yes	70%
No	14%
Unspecified	16%

As Koetter observed, while the majority of people feel informed about DNSSEC, some lack the practical knowledge or confidence needed for implementation – indicating a gap between understanding its purpose and knowing how to use it. This is demonstrated in one instance in **Slide 1.1**.



eco – Association of the Internet Industry

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 of DNSSEC are still questionable, x509 is too complicated for that.

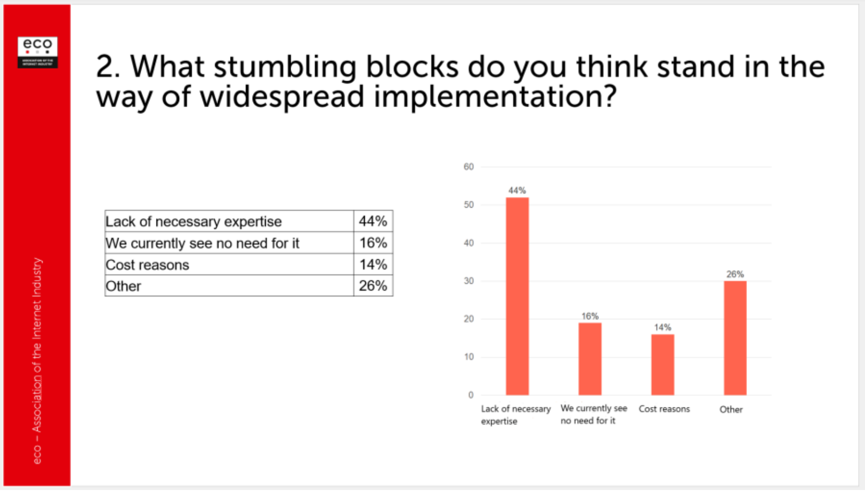
But are the others any better? Is it necessary? Do we really want another certification fiasco, as with BEA, electronic payment transactions and other aspects?

Yes

In relation to these comments, Koetter acknowledged that DNSSEC is often perceived as overly complicated but emphasized the significant improvements made to simplify its implementation. He cited BIND as one example, with configuration becoming much easier compared to years ago. He also mentioned an emerging initiative to develop a standardized DNS administration API across popular open-source DNS services, which could further reduce complexity barriers by offering consistent interfaces regardless of the product used.

Understanding the roadblocks to adoption

While many participants noted that they had already adopted DNSSEC – some for more than 15 years – the survey also highlighted persistent barriers to broader deployment. As shown in **Slide 2**, the most frequently cited reason for not implementing DNSSEC was a lack of necessary expertise (44%), followed by no perceived need (16%), cost-related concerns (14%), and a significant “other” category (26%). This significant “other” category prompted Koetter to note, “I don't have the crystal ball with me right now,” acknowledging that understanding these unspecified barriers would require deeper investigation in future research. He also pointed out a surprising inconsistency: although many respondents said they felt well-informed about DNSSEC, they still cited expertise as a barrier – suggesting a gap between awareness and operational confidence.



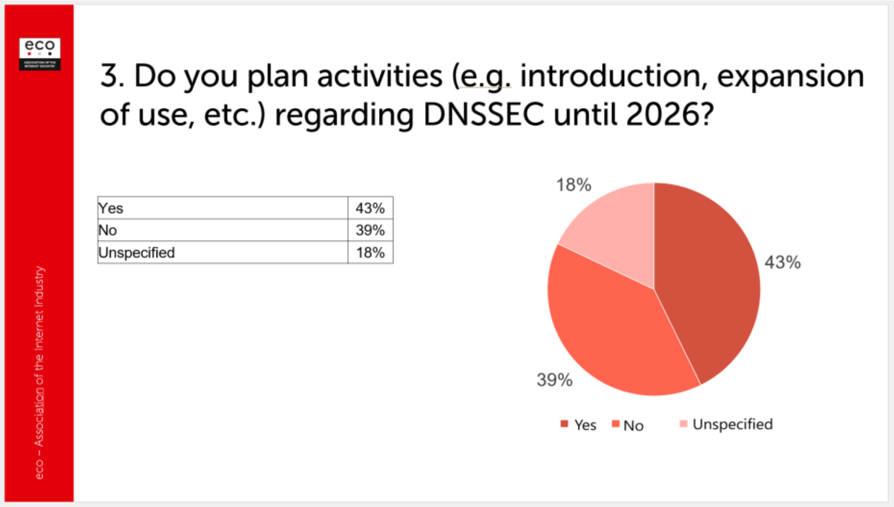
eco – Association of the Internet Industry

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%

Bridging the gap between awareness and action in DNSSEC Adoption

A further central theme emerged around the disconnect between perceived awareness and actual implementation expertise. Despite many respondents indicating they feel adequately informed, a surprising number still cite lack of expertise as a barrier – prompting questions about whether the gap lies in technical knowledge or confidence in operationalizing DNSSEC. As highlighted in **Slide 3** of the survey, responses show a nearly even split (approximately 50-50 when excluding unspecified responses) between those planning to introduce or expand DNSSEC and those with no plans, highlighting the persistent uncertainty in the industry.



eco – Association of the Internet Industry

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

Yes	43%
No	39%
Unspecified	18%

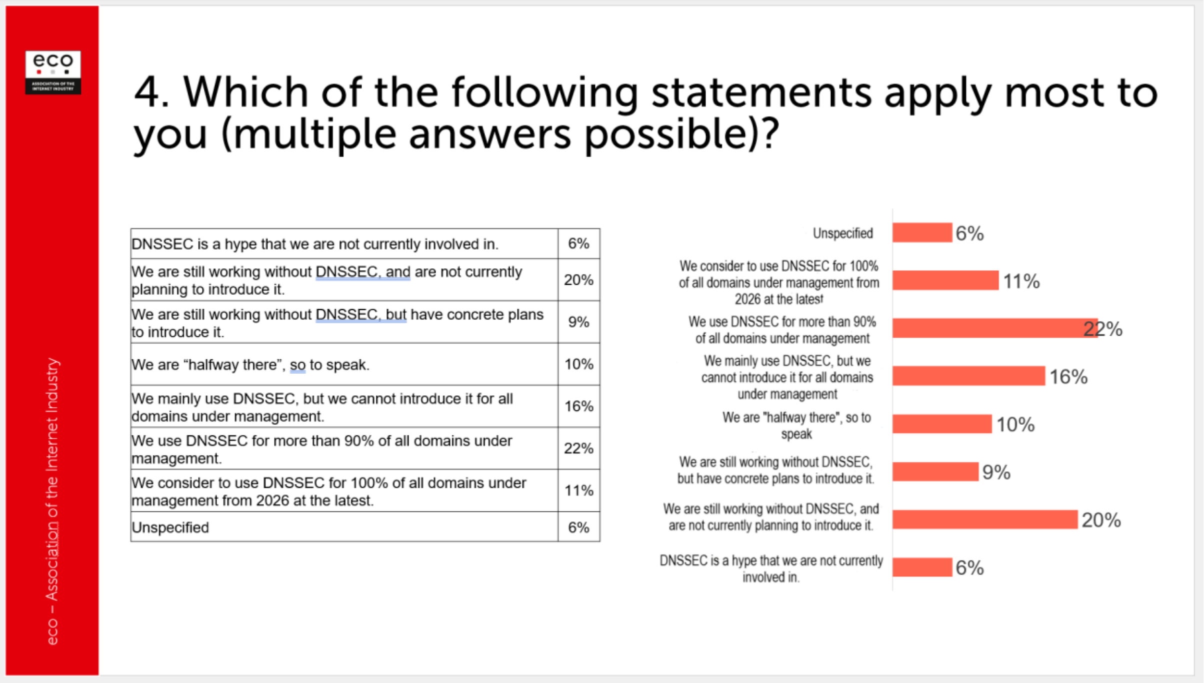
Koetter emphasized the need for myth-busting, hands-on education, and policy-driven adoption – arguing DNSSEC should be the default, especially for critical infrastructure. He pointed to countries like the Netherlands, where government-backed incentives and opt-out models have driven higher adoption, contrasting it with Germany's relatively stagnant uptake.

Learning from email: Industry-led momentum?

A parallel was drawn to email security protocols like SPF, DKIM, and DMARC, which only gained widespread adoption after major mailbox providers made them mandatory.

Mohammed Zaman from DMARC Advisor asked: "Do we need something like the sender requirements for DNSSEC to be more widely adopted – and is DNSSEC required to help to increase the adoption rate?" Koetter agreed that such a push could certainly help, noting how email security protocols gained traction after major providers made them mandatory. "That's a service provider-driven view," he added. "The US government, on the other hand, requires any US office using a .gov domain to DNSSEC-enable their domain. The benefit of DNSSEC is clear – it's just that there isn't enough money in the market for companies to offer it."

As displayed in **Slide 4**, while 22% of participants use DNSSEC for over 90% of domains, many are still in early or pilot stages – or are not using it at all. This reinforces the idea that while some organizations are far along, others are only experimenting – or have abandoned it altogether.



eco – Association of the Internet Industry

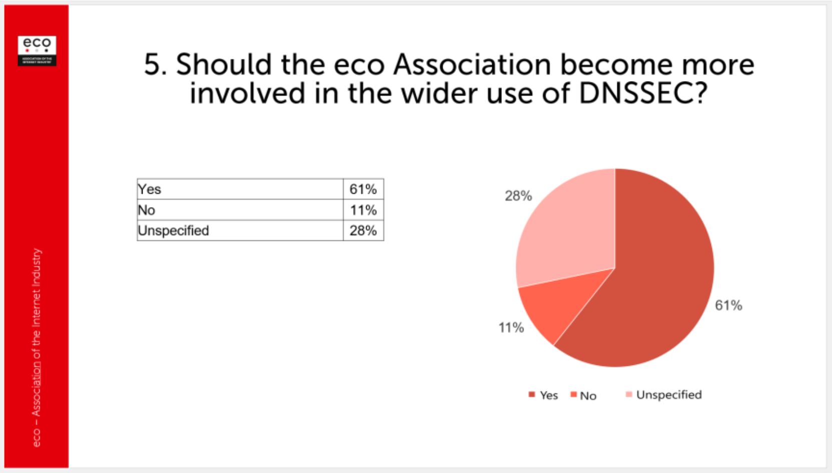
4. Which of the following statements apply most to you (multiple answers possible)?

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%

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

eco plans hands-on workshop and outreach campaign

The survey results, particularly those shown in **Slide 5**, clearly indicate that the community expects the eco Association to take a more active role in promoting DNSSEC. Lars Steffen summarized this sentiment, noting options such as providing material, given that this is relevant for all providers based in the EU. He also highlighted that it should be promoted as the best practice. As he noted, participants called for more educational resources, implementation guidance, and technical support – especially around enabling DNSSEC in existing production environments, where uncertainty and perceived risk still deter adoption.



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

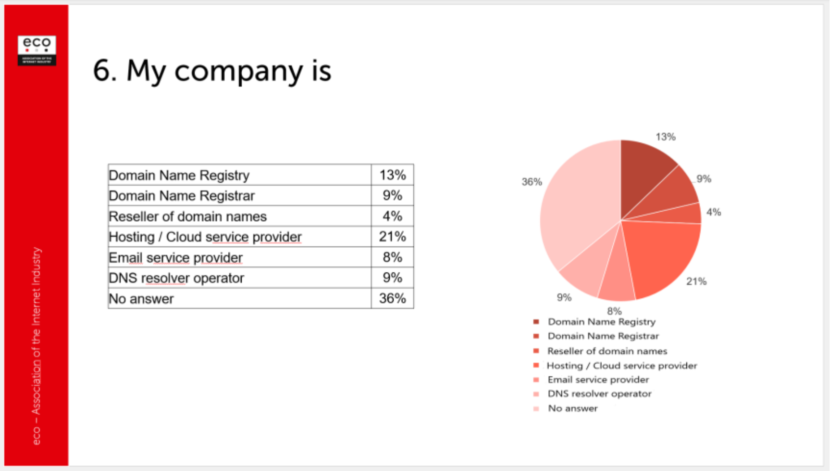
Yes	61%
No	11%
Unspecified	28%

Patrick Ben Koetter emphasized the need for a shift in mindset, advocating for DNSSEC to become a “comply or explain” default – particularly for critical infrastructure. He highlighted successful efforts in countries like Switzerland, where automation through CDS/CDNSKEY has eased deployment. While some voiced skepticism about DNSSEC’s impact, Koetter argued that the technology’s goal – trustworthy DNS communication – is more essential than ever, stating, “You should not believe in DNS. You should know.”

In response to the feedback, eco announced two initiatives:

- A joint awareness campaign with the German Federal Office for Information Security (BSI) to promote email and DNS security best practices.
- A hands-on DNSSEC implementation workshop for German-speaking providers in late 2025.

As was subsequently noted, participants included registries, registrars, cloud providers, email service operators, and more. This was demonstrated in **Slide 6**.



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%

This offers readers context on who participated in the survey. While diverse, the results also point to a need for better granularity in identifying respondent roles – something eco plans to refine in future surveys.

Is regulation the only way forward?

Koetter emphasized that the issue is no longer technical but economic: “The discussion, the issues we’re having right now are issues with clashing business models. And if we don’t find business cases for the businesses, where they start earning or not spending money, they will not go and implement things. In this absence of market incentives, Koetter acknowledged that regulatory pressure may become necessary. The German BSI is reportedly preparing an outreach campaign in partnership with eco to promote DNSSEC and related standards across the German digital economy.

As noted by Lars Steffen: “We are working on a campaign with the BSI in Germany where we are currently preparing an outreach campaign to businesses, email service providers, hosting providers.” As he highlighted, the goal is to increase awareness around email and DNS security measures, including DNSSEC.

Final thought: No trust without verification

Koetter’s closing remarks captured the heart of the issue: “Almost everything on the Internet starts by sending out a DNS query. If we can’t trust that response, then nothing built on it is reliable.” As he further indicated, DNSSEC is the only tool that is there today to verify those responses. Without it, trust remains a matter of faith – not proof.

Resources & Further Reading

🎥 **Event Recording Link**: https://international.eco.de/news/dnssec-adoption/