# To Deploy or Not to Deploy, That's the Question

## How to convince your boss to deploy DNSSEC and RPKI

**Introduction**

In order to strengthen the security of the internet for all its users, it is of great importance that the latest generation security-related internet standards and ICT best practices are deployed at a massive scale. This report focuses on two internet standards, DNSSEC and RPKI, as explained below. Currently the deployment rate of these two standards is average at best, depending on the standard or best practice[1]. This leaves users of the internet needlessly exposed to certain threats, hacks and potential harm, e.g. privacy and financial. The Internet Standards, Security and Safety Coalition (IS3C), an United Nations Internet Governance Forum Dynamic Coalition of experts, has made it its goal to raise deployment numbers. One way to do so is to make higher management and leadership understand why deployment of security-related standards is important for their organisations, their customers, and society as a whole.

This document provides you with arguments you could use when you have to convince your superiors to invest in the deployment of two specific security-related internet standards and associated ICT best practices. These arguments have been compiled for you by a team of international experts. Deployment is important for two reasons.

1. We can use online services and communicate on the internet because of open and agreed upon standards. However, the first generation of standards were created with interoperability and openness in mind. There was far less focus on security as at that time the internet was a more limited environment, and the first users knew and trusted each other. After the internet was opened in the mid-nineties and more and more people and organisations came online, these first generation standards left them exposed to all forms of harm on the internet, from receiving spam to identity theft and financial loss. In response internet engineers in the Internet Engineering Task Force (IETF)[2], developed a new generation of standards to fix certain flaws and therewith threats that come along with them. Unfortunately, deployment of these new standards is not a given. This document argues for a change, i.e., to make adoption at least an explicit consideration, and better, to make the use of certain standards the norm.

2. Decision takers in organisations need to understand why it is important to deploy these standards. Experience of technical experts shows that decision takers often take other considerations into account than merely technical security. Arguments technicians at times are less prepared for. This paper provides arguments that decision takers may need to hear to be convinced.

---

[1] This APNIC chart shows the differences around the globe per country on DNSSEC validation: https://stats.labs.apnic.net/dnssec. Deployment in many countries is extremely low. For RPKI this is different, see: https://labs.ripe.net/author/job_snijders/rpki-2023-review-growth-governments-and-innovation/. There is still room for improvement.

[2] https://www.ietf.org/

This document provides you with answers to this question, based on the example of two standards, the Domain Name System's Security Extensions (DNSSEC) and the Resource Public Key Infrastructure (RPKI)[3].

*IS3C*

The Internet Standards, Security and Safety Coalition (IS3C) is an IGF Dynamic Coalition that brings together key stakeholders from the technical community, civil society, government policymakers, regulators, and corporate and individual adopters, with the shared goal of making online activity and interaction more secure and safer by achieving more widespread and rapid deployment of existing, security-related internet standards and ICT best practices.

*IS3C Working Group 8 goals*

IS3C's Working Group 8[4] (WG8) started its work after the IGF of 2023 in Kyoto. It was decided that it would focus on two technologies: DNSSEC and RPKI, as examples for the much wider range of internet standards that need to be deployed[5]. Under WG8, a team of international experts gathered who agreed on the text of and arguments in this report. These experts are:

| | |
|---|---|
| David Conrad | Co-Founder/Partner/CTO, Layer 9 Technologies |
| Dick Brandt | CISO Masterclass (NL) / MKB Cyber Advies Nederland |
| Eric Osterweil | Assistant professor, George Mason University |
| Fredrik Hansen | Senior information and security expert |
| Jad el Cham | RIPE NCC |
| Neil Dundas | Co-founder Domain Name Services and DNS Africa |
| | |
| Bastiaan Goslings | SIDN (former RIPE NCC) (vice-chair) |
| David Huberman | Expert ICANN office of the CTO (chair) |
| Wout de Natris | De Natris Consult / IS3C (coordinator) |

IS3C WG8's goal is to improve the narrative around these technologies for the purposes of helping organisational leaders better understand them, convince them of their importance, and offer persuasive reasons for why their organisations might want to adopt each. While DNSSEC and RPKI are very different technologies that address challenges in two different problem spaces, the Working Group has chosen these technologies because we believe they should be part of an organisation's wider security management strategy. To note that it is not to be assumed that these two technologies should be packaged together in every case as the requirements, needs and arguments might differ greatly depending on the technology, organisation's role and services offered. We think they can improve all organisations' overall security posture, and they should be known about in the corridors of management and in the

[3] An explanation of both technologies is provided below.
[4] IS3C has working groups on different topics, see www.is3coalition.org
[5] See e.g. IS3C's advisory list of 23 standards, https://is3coalition.org/docs/is3c-working-group-5-report-and-list/

corporate boardroom. Internet governance organisations like ICANN and the RIPE NCC deem standards deployment  of importance and have provided the resources to start the work processes.

This Working Group provides a work plan, containing among others a new and different narrative and recommendations for the next phase, including an outreach plan at the global level.

**Background**

Research conducted in an IGF project in 2019[6] contains causes of, and recommendations to change, the slow uptake of internet standards and ICT best practices deployment. One of the causes presented in the report, on the basis of input from the internet community at large, pointed to the fact that deployment is often seen as a technical issue, needing a technical solution. While technical challenges definitely are to be considered, community feedback demonstrates that (non-) deployment often is determined by financial, economic, security related, or social considerations as well. Accordingly, the traditional narrative aimed at encouraging deployment of relevant standards and best practices has been insufficiently and unsuccessfully tailored to make a positive impact on individuals in decision-taking positions inside organisations[7]. The report gave two consecutive recommendations: a) include and engage individuals in decision-taking positions and; b) change the narrative in such a way that decision takers will decide favourably on deployment. On this basis, IS3C started a new working group focused on RPKI and DNSSEC deployment.

**The Importance of DNSSEC and RPKI**

The Domain Name System (DNS), the addressing system (IPv4 and IPv6 addresses), and the global system of routing are, together, argued by many to be what constitutes the core of the internet's infrastructure. They are fundamental technologies we all rely on when we use the internet for work, rest, and play.

These technologies were created in the 1970s, 80s, and 90s, when the internet was used on a small scale, mainly by universities and the military in the United States.

In the early 1990s, the significant vulnerabilities and associated attacks on the DNS were documented[8], leading to the development of a bolt-on security standard: DNSSEC ("Domain Name System Security Extensions"). As the internet grew, misconfigurations that led to outages informed later attack models on the routing system and incidents started to occur more often. So in the late 2000s, work started to invent a system to help secure routing, and eventually RPKI ("Resource Public Key Infrastructure") was developed as an underlying

[6] https://www.intgovforum.org/en/filedepot/folder/182 'Setting the standards' Wout de Natris, Marten Porte (Haarlem 2020)
[7] https://www.intgovforum.org/en/filedepot/folder/182 'Setting the standards' Wout de Natris, Marten Porte (Haarlem 2020)
[8] https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/bellovin.pdf 'Using the Domain Name System for System Break-Ins', Steve Bellovin (Usenix 1995)

infrastructure on top of which improved routing security could be implemented. You find an in-depth explanation of the two standards and why extra focus on their deployment in Annex 1 below.

**Workplan and procedure**

IS3C and its chairs engaged a diverse group of experts representing various regions and stakeholder communities. These experts collaborated throughout fall 2023 to develop a comprehensive framework for promoting the adoption of DNSSEC and RPKI standards across industry and government sectors.

The expert team conducted a thorough analysis of the current landscape and identified critical gaps in existing approaches to standards adoption. Based on this analysis, they developed a new framework that articulates clear rationales for adopting these best practices, tailored to specific decision-maker needs and priorities.

Different sectors require distinct approaches because their motivations and constraints vary significantly. Government decision-makers often prioritise national security, critical infrastructure protection, and compliance with regulatory frameworks. In contrast, industry leaders typically focus on cost-benefit analysis, competitive advantage, and operational efficiency. Educational institutions must balance academic freedom with security requirements and limited budgets, while healthcare organisations prioritise patient data protection and service reliability. Financial services firms, meanwhile, concentrate primarily on transaction security and maintaining customer trust.

The framework addresses two distinct implementation scenarios, each requiring different approaches. The first scenario involves direct deployment, where organisations implement these standards within their own infrastructure. This approach presents several challenges: organisations must make significant initial investments in technology and expertise, prepare for extended implementation timelines, secure specialised technical knowledge, and account for ongoing maintenance requirements.

The second scenario involves procurement and contract negotiations, where organisations need to incorporate these standards into service contracts with vendors. This requires careful attention to vendor capability assessment, strategic contract negotiation, thoughtful cost allocation, detailed service level agreements, and robust compliance monitoring mechanisms.

The team's initial draft report underwent global consultation from March through early April 2024, with stakeholder feedback incorporated into the documentation. This led to a second draft report that was discussed again in October 2024. The iterative consultation process ensured that the framework addresses real-world implementation challenges while remaining adaptable to different organisational contexts.

**What are the arguments for deploying DNSSEC and RPKI today, and why do they fail?**

Some of the main arguments used for years to sell DNSSEC and RPKI include:

1. Regulatory and Compliance Requirements

   Governments and regulatory bodies in various regions have increasingly recognized the importance of securing DNS and internet routing. Compliance with regulations that mandate DNSSEC and RPKI adoption may be required for businesses to operate or participate in certain industries. For example, there is a significant movement by the United States government to mandate RPKI adoption and deployment by regulated ISPs[9].

2. Mitigating DNS Abuse and Fraud

   DNSSEC and RPKI can significantly reduce the risk of domain name abuse, such as phishing attacks that exploit domain name spoofing. By validating the authenticity of domain names and IP address allocations, organisations can prevent fraudulent activities associated with their brand or online services.

3. Internet Resilience and Stability

   Securing the DNS infrastructure and internet routing helps maintain a stable and resilient online environment. This is crucial for businesses that rely on uninterrupted online services to serve customers and maintain business continuity.

4. Building Customer Trust

   Security breaches and cyber incidents erode customer trust. DNSSEC and RPKI provide additional assurance to customers that an organisation takes cybersecurity seriously, leading to enhanced trust and confidence in its brand.

5. Cyber Insurance Premium Reduction

   Some insurance companies offer incentives or reduced premiums for organisations that demonstrate strong cybersecurity practices. Implementing DNSSEC and RPKI can be viewed positively by insurers when evaluating cyber risk.

6. National Security and Critical Infrastructure Protection

   For organisations involved in critical infrastructure, such as telecommunications, finance, or government services, DNSSEC and RPKI are vital to national security efforts, as they strengthen the resilience of these essential services.

**Why do these arguments insufficiently resonate or fail?**

[9] https://www.fcc.gov/document/fcc-proposes-internet-routing-security-reporting-requirements-0 'FCC Proposes Internet Routing Security Reporting Requirements', June 2024

*Cost and Resource Constraints*

There can be a mistaken presumption that implementing DNSSEC and RPKI requires significant investments in hardware, software, training, and ongoing maintenance. Smaller organisations, startups, or those with limited budgets may think this cost to be beyond their resources. This is generally not true (especially so for RPKI).

*Complexity and Technical Challenges*

DNSSEC and RPKI implementations can be technically complex. Although better automated tooling has become available during recent years, specialised knowledge and expertise are often still required if an organisation wants to do everything itself and be in full control. Organisations without security teams experienced in these technologies may hesitate to undertake these projects due to concerns about potential disruptions or complications.

There also might be concerns, because of perceived complexity, that operational risks are introduced when deploying both authoritative DNSSEC and RPKI. With every new component or technology introduced in the network, it comes with its own set of risks. Deploying these technologies can, if mistakes are made, result in domains or routes vanishing from the Internet. However, if properly prepared for and managed, it will lead to a better security posture of the whole organisation.

*Perceived Low Risk*

Some organisations may underestimate their risk exposure or believe their current security measures are sufficient. This complacency can lead to a lack of urgency in adopting additional security protocols like DNSSEC and RPKI.

*Lack of Awareness and Education*

Despite increased awareness of cybersecurity, not all organisations fully understand the benefits and importance of DNSSEC and RPKI. They may not be familiar with the risks they face or the potential impacts of not adopting these measures. They also lack experienced and knowledgeable staff to deploy and maintain these technologies.

*Organisational Priorities and Decision-making Processes*

Convincing senior management to allocate resources and prioritise security initiatives can be challenging, especially in larger organisations with complex decision-making processes.

**The Alternative Narrative, a Call To Action for Leaders**

Our story focuses on public and private decision takers, those at the top of organisational hierarchies, and poses the question: why should they approve the allocation of resources necessary to adopt and deploy both DNSSEC and RPKI? The answer is that these technologies are security measures that help plug important holes in an organisation’s security posture, and are part of a larger-scale effort to make the broader internet more

secure. Now that digitisation is impacting every aspect of our societies, the security and resulting trust in the DNS and routing infrastructure become increasingly important. Our online lives, and the ambitions we have globally to reap the benefits the internet brings for all, including those that are not yet connected, are completely dependent on the secure functioning of these underlying building blocks.

1) *The deployment of DNSSEC and RPKI represents a crucial foundation for national cybersecurity resilience, providing cryptographic protection when it comes to the authorization of critical internet resources, which helps safeguard the online delivery of public services, citizens' data, and national security assets.*

National critical infrastructure - including power grids, financial systems, healthcare networks, and government services - depends on secure and reliable internet connectivity for essential operations. DNSSEC and RPKI provide complementary security controls that protect two fundamental internet protocols: DNS and BGP (Border Gateway Protocol). DNSSEC prevents attackers from manipulating DNS responses through cryptographic signatures, protecting against attacks like DNS cache poisoning that could redirect traffic to malicious servers. Meanwhile, RPKI enables network operators to cryptographically verify the origin of BGP route advertisements, preventing both inadvertent route leaks and deliberate BGP hijacking attempts that could lead to traffic interception or denial of service. Together, these protocols create a chain of trust for both domain name resolution and internet routing, enabling organisations to automatically detect and reject unauthorised changes that could compromise network integrity. This enhanced security posture is particularly critical for government agencies and critical infrastructure operators who require high confidence in the authenticity of their internet communications[10].

*2) The implementation of DNSSEC and RPKI represents a strategic approach to regulatory compliance and cybersecurity best practices, providing demonstrable technical controls that protect data integrity and infrastructure reliability - key requirements across global regulatory frameworks and industry standards.*

Modern organisations face an increasingly complex regulatory landscape that demands robust technical controls for data protection and system integrity. Critical regulations include the EU's General Data Protection Regulation (GDPR), which mandates appropriate technical measures to ensure data security (Article 32), the U.S. Health Insurance Portability and Accountability Act (HIPAA) Security Rule requiring protection against unauthorised data access, and the Payment Card Industry Data Security Standard (PCI DSS) which explicitly requires secure protocols and cryptographic controls.

DNSSEC and RPKI provide specific technical capabilities that directly support compliance objectives. In terms of authentication and integrity protection, DNSSEC cryptographically signs DNS records, preventing DNS spoofing attacks that could redirect users to fraudulent

[10] As mentioned in the previous section, there are operational risks associated with deploying DNSSEC and RPKI. Organisations must prepare for these risks by properly training staff, creating strong operating processes and procedures, ensuring they have the appropriate risk management controls in place, and by having fallback plans for when emergencies occur.

websites. RPKI validates routing announcements, preventing unauthorised BGP route advertisements that could lead to traffic interception. When deployed together, these controls significantly mitigate the risk of credential theft through phishing sites and man-in-the-middle attacks.

The regulatory and standards landscape strongly supports these protocols. The Internet Engineering Task Force (IETF) has standardised both DNSSEC (RFC 4033-4035) and RPKI (RFC 6480). All five Regional Internet Registries (RIRs) - AFRINIC, APNIC, ARIN, LACNIC, and RIPE NCC - actively support and promote RPKI deployment. Additionally, ICANN requires DNSSEC for new generic Top-Level Domains (gTLDs).

These protocols align seamlessly with major security frameworks. They map directly to NIST Cybersecurity Framework's requirements for data-in-transit protection (PR.DS-2), the CIS Controls' data protection requirements (Control 7), and ISO 27001's communications security controls (A.13).

Market adoption demonstrates the protocols' growing importance. Over 90% of top-level domains (.com, .org, .NL, etc.) support DNSSEC[11]. Leading cloud providers and content delivery networks have embraced RPKI validation as a standard security practice.

The deployment of these protocols demonstrates concrete commitment to security best practices, providing organisations with defensible evidence of due diligence for auditors and regulators. As cyber threats continue to evolve, regulators increasingly view these fundamental security controls as essential components of a comprehensive security program, particularly for organisations handling sensitive data or operating critical infrastructure.

*3) For commercial organisations, the deployment of DNSSEC and RPKI offers compelling security and business advantages that directly impact the bottom line while protecting critical infrastructure. These technologies provide essential safeguards against increasingly sophisticated cyber threats by ensuring the authenticity and integrity of internet routing and domain name resolution.*

Brand reputation and customer trust benefit significantly from DNSSEC and RPKI implementation. By preventing DNS spoofing attacks and unauthorised BGP route hijacking, these technologies protect customers from being redirected to fraudulent websites or having their data intercepted. This demonstrated commitment to security strengthens an organisation's reputation as a trustworthy digital business partner and helps maintain customer confidence in online services.

From a compliance perspective, DNSSEC and RPKI are increasingly becoming mandatory requirements in various regulatory frameworks. For instance, in the Netherlands, public authorities must either implement these technologies or provide explicit justification for non-compliance. The Internet.nl testing platform[12], which evaluates adherence to modern internet

[11] See: https://ithi.research.icann.org/graph-m7.html#M72
[12] See https://en.internet.nl/

standards, specifically checks for both DNSSEC and RPKI implementation. Early adoption of these technologies positions organisations advantageously for future regulatory requirements while demonstrating proactive risk management.

The protection of critical infrastructure takes on new importance as organisations increasingly depend on online operations. DNSSEC ensures that DNS queries return authentic responses, preventing man-in-the-middle attacks that could redirect traffic to malicious servers. Similarly, RPKI validates the legitimacy of routing announcements, protecting against accidental route leaks or deliberate BGP hijacking attempts that could disrupt critical services or facilitate data theft.

The financial implications of implementing these technologies extend beyond mere compliance. While initial deployment requires investment, the cost is modest compared to potential losses from security incidents. DNS hijacking and BGP attacks can lead to extended service outages, data breaches, and loss of customer trust—all of which carry substantial financial and reputational costs. DNSSEC and RPKI serve as cost-effective preventive measures against these specific types of attacks.

Industry leadership in security practices increasingly includes DNSSEC and RPKI deployment. Major technology companies and financial institutions have implemented these protocols, establishing them as fundamental components of a robust security posture. Organisations that adopt these technologies demonstrate alignment with industry best practices and position themselves as security-conscious market leaders.

The deployment of DNSSEC and RPKI also addresses duty of care obligations under consumer protection laws. Organisations handling customer data have a responsibility to implement reasonable security measures to protect that information. By securing DNS resolution and BGP routing—two critical internet infrastructure components—organisations demonstrate due diligence in safeguarding customer data and communications. This commitment to security not only meets legal obligations but also reinforces brand trust and customer loyalty.

*4) Each user/organisation holds a moral obligation to uphold these standards for the benefit of society as a whole*

There is an increasing desire among organisations to contribute positively to the world; an understanding that using the internet comes with responsibilities toward fellow users. Ensuring the safety and availability of commonly used internet resources is an effective addition to that desire. Why?

Not deploying these standards ultimately makes all users of the internet, including your own organisation, unnecessarily unsafe and vulnerable to attacks, abuse, and harm. Deploying is synonymous to protecting your customers, suppliers, partners, employees, and your own organisation’s information and interests. This moral obligation cuts both ways. It helps protect the vital assets of all involved.

## Conclusion

The adoption of RPKI and DNSSEC is not just about meeting regulatory requirements or industry standards. It's about safeguarding an organisation's reputation, protecting its critical services, vital information and related infrastructure, and demonstrating its commitment to cybersecurity. It's a strategic investment in a future that enhances brand reputation and helps ensure the integrity and authenticity of online services. With the ongoing digitisation of our societies, online presence should be considered part of organisations' core business, and as such it is imperative that they incorporate considerations regarding DNSSEC and RPKI in their strategic plans to promote trust in the provision of their services.

When is this project a success? IS3C is of the opinion that this project is not a success when we have rewritten the narrative and published it. It can only be called a success when people in the position to put emphasis on the need to deploy DNSSEC and RPKI (and all other relevant internet standards and ICT best practices for that matter) start using these arguments, convincing their superiors of the need to deploy. 100% may be overstretching ourselves, but in the end that is what the world needs to bring a more secure and safer internet a huge step closer.

## ANNEX 1

*A Quick Primer on DNSSEC*

The DNS was invented in 1983 with little in the way of security built-in to it. With this limited security, DNS is vulnerable. Attackers for example can falsify responses to DNS queries, allowing these attackers to transparently redirect end-users to web sites under their own control (for account and password collection).

In response to this threat, the Internet Engineering Task Force (IETF), the international standards development organisation responsible for internet-related protocols, developed DNSSEC to cryptographically ensure DNS content cannot be modified after it has been signed by its source without being detected. Once fully deployed, DNSSEC stops the attacker's ability to redirect users using the DNS.

DNSSEC works by digitally signing each DNS record set so that any tampering of that record set can be detected. The digital signatures, and keys used to create them, are distributed just like any other records in the DNS, making DNSSEC backward compatible and incrementally deployable. However, for the public to benefit fully from DNSSEC via the chain of security it establishes from content source to end-user, it must be supported by every entity along this chain, from the domain name owners to all of the world's ISPs.

*A Quick Primer on RPKI*

Routing is the process of determining the path of how internet traffic flows in order for online connected end-devices to communicate with each other. Any time you open an app or go to a website, the packets move back and forth from your device to the site you are visiting via the internet's system of routing.

Similar to the DNS, this system of routing was invented and deployed without full consideration of the likely security requirements the internet would face by early internet pioneers who were just trying to connect everyone. Moreover, early internet routing configuration was performed manually (not by automated scripts). Mistakes (e.g., typos) were sometimes made when humans would misspell IP addresses (e.g., transposing two numbers) causing routing to break until the mistake was fixed. The first major routing mistake was probably in 1997 when the operators of AS 7007[13] misconfigured their router causing a major outage[14]. Then in 2008, a large-scale mistake was made: all the routing traffic bound for YouTube was redirected to a country's national telco, effectively taking YouTube offline[15].

[13] AS stands for Autonomous System. This "is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain, that presents a common and clearly defined routing policy to the Internet"\ https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[14] https://www.kentik.com/blog/a-brief-history-of-the-internets-biggest-bgp-incidents/

[15] See https://www.ripe.net/about-us/news/youtube-hijacking-a-ripe-ncc-ris-case-study/

Work then began at the IETF on new solutions, and an evolutionary product of this work is RPKI, a security framework used to improve the safety and reliability of Internet routing. By using digital certificates and cryptographic signatures, the RPKI framework helps prevent not just accidental misconfigurations, but also route hijacking and IP address spoofing, which are common attack vectors used to redirect traffic to malicious destinations.

*Current State of DNSSEC and RPKI Deployment*

Because there is limited visibility of the entire DNS tree, it is not straightforward to measure the current state of DNSSEC deployment across the whole DNS. The root is DNSSEC signed, and the vast majority of top-level domains are signed. However, beneath the top-level domains, it becomes less clear. There are projects which measure the number of domain names registered, configured with name servers, and then look for DNSSEC signatures. These projects seem to show few DNSSEC-signed domains[16]. In addition, measuring the deployment of DNSSEC validation efforts is not easy. One good source of measurement is at APNIC, which shows roughly one-third of all resolvers validate DNSSEC signatures[17].

Since the deployment model for routing information is fundamentally different from the DNS and a good understanding of the full routing "tree" of the Internet is possible, RPKI measurements are somewhat easier. On an aggregated level, well over 50% of allocated IPv4 address space is covered by route origin authorisation (ROA) attestations as of late 2024[18].

[16] StatDNS for example shows approximately 4% of domain names in .COM are signed. See https://www.statdns.com/
[17] https://stats.labs.apnic.net/dnssec
[18] https://rpki-monitor.antd.nist.gov/