Measuring the Deployment of DNSSEC Bootstrapping Using Authenticated Signals

Q Misell
qmisell@mpi-inf.mpg.de
Max Planck Institute for Informatics
Saarbrücken, Germany

Florian Steurer
fsteurer@mpi-inf.mpg.de
Max Planck Institute for Informatics
Saarbrücken, Germany

Johannes Zirngibl
jzirngib@mpi-inf.mpg.de
Max Planck Institute for Informatics
Saarbrücken, Germany

Anja Feldmann
anja@mpi-inf.mpg.de
Max Planck Institute for Informatics
Saarbrücken, Germany

Tobias Fiebig
tfiebig@mpi-inf.mpg.de
Max Planck Institute for Informatics
Saarbrücken, Germany

Abstract

The DNS, the Internet's address book, traditionally does not guarantee authenticity of data. The DNS Security Extensions (DNSSEC) exist to add cryptographic authenticity checks to the DNS. In spite of DNSSEC being over 30 years old, its widespread deployment has not yet come to fruition. Current work in the IETF tries automating the setup of DNSSEC, in the hopes of furthering its deployment.

In this paper, we analyze the current state of DNSSEC, where automated deployment may prove useful, and how DNS operators are deploying this new standard. We find that DNSSEC deployment remains lackluster. An increase to DNSSEC deployment could be achieved by the implementation of - optionally non-authenticated (RFC 8078) - automatic DNSSEC configuration by domain name registries and registrars. Only 3 DNS operators implement authenticated bootstrapping, but those that do generally implement this new standard well, with 99.9 % of their zones conforming.

CCS Concepts

• **Networks → Naming and addressing**.

Keywords

DNSSEC, Authenticated Bootstrapping

ACM Reference Format:
Q Misell, Florian Steurer, Johannes Zirngibl, Anja Feldmann, and Tobias Fiebig. 2025. Measuring the Deployment of DNSSEC Bootstrapping Using Authenticated Signals. In *Proceedings of the 2025 ACM Internet Measurement Conference (IMC '25), October 28–31, 2025, Madison, WI, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3730567.3764501

1 Introduction

The Domain Name System (DNS) was initially designed without security and authenticity in mind. However, with DNS Security Extensions (DNSSEC) a mechanism to authenticate the data of DNS resolutions has existed since 1997 [15]. While DNSSEC is essential to secure the DNS and thus the Internet, it has not seen widespread deployment [6, 7, 44, 32]. A major challenge is that DNSSEC deployment requires synchronization between a zone and its parent zone; that is, the `DS` Resource Records (RRs) securing the delegation must be correctly installed in the parent. This can be challenging to coordinate, especially when the DNS operator differs from the domain's registrar.

To improve on this situation, the Internet Engineering Task Force (IETF) has standardized additional DNSSEC features in multiple steps, *(i)* `CDS` and `CDNSKEY` RRs in 2014 [24], *(ii)* automated bootstrapping in 2017 [18], and most recently *(iii)* Authenticated Bootstrapping (AB) in 2024 [42]. Together, these allow automating the configuration of DNSSEC and regular key rollovers without requiring action by the domain owner. Therefore, they can drastically reduce the barrier for deploying DNSSEC through automation.

However, successfully utilizing these features requires a correct implementation and careful setup. Insights into the current state of DNSSEC, required RRs, and the early state of AB are important to guide future deployments. This work takes a first, large-scale look at the ecosystem of AB for DNSSEC.

Contributions: Our core contributions are:
(i) We conduct a large-scale measurement of the DNS ecosystem, focusing on DNSSEC using YoDNS [40]. Resolving more than 287 M zones, we find only 15.8 M successfully signed zones and 640 k that even fail validation.
(ii) We evaluate the deployment of required `CDS` and `CDNSKEY` RRs, as well as their content and correctness. In most cases, the served `CDS` RRs are consistent, thus, deployments fulfill a major requirement. However, we find 5 333 inconsistencies using YoDNS.
(iii) We evaluate the state of AB as of April 2025, finding 272 k zones on 3 DNS operators supporting AB.

2 Background

Initially, the DNS was designed without any authentication mechanism. In 1997, the IETF set out to rectify these shortcomings in the DNS with the DNSSEC [15]. DNSSEC employs cryptographic signatures over DNS data to ensure the integrity and authenticity of data. To achieve this, new RR types have been added to the DNS:

`DNSKEY` RRs are public keys used to sign data in the DNS.
`RRSIG` signatures over RRs with a `DNSKEY`'s private key.
`NSEC/NSEC3` RRs to authenticate negative responses.
`DS` RRs are hashes of `DNSKEY`s, inserted into the parent zone next to the delegation `NS` RRs.

IMC '25, Madison, WI, USA

ACM ISBN 979-8-4007-1860-1/2025/10
https://doi.org/10.1145/3730567.3764501

Especially the DS RR leads to deployment challenges given the organizational hierarchies in DNS (see Sec. B). It has to be synchronized between a zone and its parent: *(i)* The DNS operator of a zone needs to create the RRs. *(ii)* The domain registrar synchronizes between the DNS operator and the registry. *(iii)* The registry operating the respective parent zone adds the RRs to its zone.

If the registrar is the DNS operator, details of setting up NS and DS RRs can be hidden. However, if the DNS operator is not the registrar itself, a domain owner must copy NS and DS RRs from their DNS operator to their registrar to be given to the registry and inserted into the zone file. This is usually achieved via a web interface for the customer to access, and the Extensible Provisioning Protocol (EPP) [21] with the DNSSEC Extensions [22] between the registrar and the registry. If a DNS operator deploys DNSSEC, but the customer does not install the DS RRs at the parent, then a situation called a secure island arises.

CDS and CDNSKEY: To remove the need for a customer to take action to deploy DNSSEC, it is desirable to have this happen automatically and with minimal to no interaction. In 2014, the IETF defined a mechanism to manage the rollover of DS RRs in the parent via corresponding RRs in the child called CDS and CDNSKEY [24]. Two RR types exist, as some registries wish to calculate the DS RR themselves (e.g., to allow the registry cryptographic hash agility), whilst others are content with allowing the DNS operator to calculate the DS RR. If a DNS operator publishes one of a CDS or a CDNSKEY RR, they should publish both. The most common setup is for the registry to use the CDS RRs. For brevity, in the rest of this document, CDS refers to CDS and CDNSKEY RRs.

The CDS RR can also be used to disable DNSSEC. This is achieved by signalling a null algorithm in the CDS RR. It is never seen in DS RRs and only has meaning in the context of CDS RRs. Disabling DNSSEC can be helpful when a domain name moves between two DNS operators that cannot, or do not wish to, coordinate a proper rollover.

Initially, the rollover mechanism only covered the rollover of DS RRs, i.e., resigning a zone using new keys. The new CDS RRs are signed using the old DNSKEYs to allow such a rollover. As such, this mechanism in its original form cannot be used to bootstrap DS RRs - they must be extant to verify the new CDS RRs published by the DNS operator. An initial mechanism to effectuate bootstrapping was specified by the IETF in 2017 [18]. This mechanism did not cryptographically authenticate the CDS RRs used for bootstrapping, leading to policies for AB being proposed by the IETF (see Sec. C).

Authenticated Bootstrapping: These policies present operational, organizational, or security difficulties to the deployment of DNSSEC, and none are entirely automated whilst maintaining the security expected of modern Internet protocols. In 2024, RFC9615 [42] was published, standardizing AB. The standard enables the automatic configuration of DNSSEC on domain names, without the operational and security limitations of previous attempts at this. Additional copies of the CDS RRs are published in a signalling zone with extant DNSSEC to achieve this. Signalling zones are based on nameservers (NSes) (see Listing 1). For AB to be accepted by the parent (i.e., registry) the following must be true:
(i) The domain name is not already signed with DNSSEC. *(ii)* All NSes authoritative for the domain return the same CDS RRs. *(iii)* All NSes authoritative for the signal zones return the same CDS RRs as zone's NS. *(iv)* All CDS RRs for the signal zones are secured with DNSSEC. *(v)* The zone passes DNSSEC validation with the new DS RRs.

Listing 1: Example of where CDS RRs must be published for Authenticated Bootstrapping.

```
example.co.uk
_dsboot.example.co.uk._signal.ns1.example.net
_dsboot.example.co.uk._signal.ns2.example.org
```

Iff all the above are true, then the parent can secure the domain with DNSSEC, with the cryptographic assurance that these are the correct DS RRs for this domain. At the time of writing, AB is supported by .ch [2], .li [2], .swiss [12], and .whoswho [3]. Additionally, one registrar implements AB and one unAB [5]. In the case a registry does not implement this standard, any party with authority to update the DS RRs in the parent zone can process these authenticated RRs and make the appropriate updates. At the time of writing, only one such registrar implementation exists.

DS Bootstrapping Limitations: The standard does not cover all possible bootstrapping situations, but aims to address most situations where DNSSEC is not currently routinely configured. Unusually long child zone names, or NS hostnames, can cause additional RRs to exceed the maximum DNS label length of 255 octets [13]. Additionally, a zone with only in-domain name servers (i.e., example.com with name servers of ns1.example.com and ns2.example.com) cannot be bootstrapped with this standard, as there is no extant DNSSEC chain to the relevant signalling RRs.

3 Methodology

We conducted a large-scale scan of the DNS to ascertain various zones' DNSSEC and AB status. We focused only on publicly registrable domains, directly under DNSSEC signed TLDs, as the TLD-registrant boundary is the largest pain point of DNSSEC deployment [7].

Domains: A comprehensive dataset of zones is required to get a comprehensive view of the deployment of AB in the DNS. We combined various sources to compile a list of domain names from different Top-level Domains (TLDs) to scan. We considered only those zones directly underneath an ICANN public suffix in the Mozilla Public Suffix List [36], e.g., zones such as example.com and example.co.uk, but not a.example.com. This work focuses on the pain point of DNSSEC configuration between the registry and the DNS operator, not any organizational interactions in the DNS. We also exclude zones where all NSes were inside the zone, as these could never be bootstrapped. This resulted in 287.6 M domain names to scan from these sources:
(i) Domains from different top lists: Tranco [25], Majestic [28], Cisco Umbrella [8], and Cloudflare Radar [9].
(ii) Zone files available from the Centralized Zone Data Service (CZDS). These files contain every delegated domain name and its NSes in each Generic TLD (gTLD) zone.
(iii) Country Code TLDs (ccTLDs) available via the AXFR protocol [26]: .ch, .li, .se, .nu, and .ee.
(iv) ccTLDs available via private arrangement: .uk[1], and .sk.

[1]The Nominet zone files were provided under license to one of the authors in their capacity as a member of Nominet.

(v) Besides available full ccTLD zone files, we utilized the OpenINTEL list of ccTLD domain names compiled from Certificate Transparency Logs (CTLogs) [43].

Scans: As explained in Sec. 2, AB requires consistency between all NSes of the zone and signaling zone [42]. Therefore, we use the YoDNS scanning tool [40] designed for large-scale DNS scans. It resolves the whole dependency tree of a zone and queries all authoritative NSes. We query for all zones' DNSSEC related RRs (`DNSKEY`, `NSEC`, and `RRSIG`), the `DS` records in the parent zone, query every NS for the `CDS` RRs, and query every NS authoritative for the signal zones for `CDS` RRs, and associated `RRSIG`.

In our scans, we limited each scan machine to 50 Queries per Second per NS, to limit the impact of our scans on DNS operator's load (also see Sec. A). Unfortunately, due to the dominance of Cloudflare in the DNS market, and their practice of serving zones from a pool of only a few anycasted IP addresses, this severely slowed down our scans. The usual setup for a zone hosted by Cloudflare, is to have two NSes - such as `asa.ns.` and `elliot.ns.cloudflare.com.` - both of which have 3 IPv4 and 3 IPv6 addresses, giving a total of 12 NSes to query for each domain on Cloudflare. Due to the way Cloudflare's network operates, almost any IP address originated by them will respond to DNS queries for a zone, and all queries will be load-balanced internally to any one of hundreds of backing DNS servers. Thus, these IP addresses do not refer to Internet hosts in the traditional sense [4]. To allow our scans to complete in a reasonable time, we decided to only scan two NSes for 95 % of domain names hosted on Cloudflare (1 IPv4 and 1 IPv6). The other 5 % were scanned in their entirety. To validate this methodology, we conducted a full scan of all zones in the Tranco Top 1 Million list [25] and validated responses received from Cloudflare for consistency. No inconsistencies were observed between any NSes. All RRs returned in all DNS responses for a given query were identical.

We provide a discussion of the feasibility of adoption of AB by registries in the context of our methodology in Sec. D.

Identifying the DNS Operator: To evaluate who is deploying AB, it is necessary to ascertain the DNS operator for a domain. For this, we use the hostnames of the domain's authoritative DNS NSes. For example, if a domain name has NSes ending in `domaincontrol.com`, the DNS service for this domain is provided by GoDaddy; similarly, deSEC operates `ns1.desec.io.` and `ns2.desec.org.` as NSes, and Cloudflare operates those ending with `ns.cloudflare.com`.

We also accounted for white label use of DNS providers, e.g., the US Government using NSes ending in `seized.gov` for websites taken offline subject to a court order or criminal investigation, however these NSes are merely rebranded Cloudflare NSes.

3.1 Limitations

Our source of zone file data does not provide complete coverage of all ccTLDs; in particular, we were unable to obtain access to the zone files for some of the largest ccTLDs such as `.de` and `.nl` [41]. However, we consider that an adequately representative sample of these were obtained through CTLogs, capturing a representative sample of between 43% and 80% of each zone [39].

Our method of identifying the DNS operator has some limitations in edge-cases, such as highly custom DNS setups and multi-operator setups. In cases where the operator was unclear or ambiguous, we left these zones tagged as unknown operators. In any case, multi-operator setups are uncommon enough not to affect the big-picture of our results — a mere 22 domains had a multi-operator setup whilst showing signs of AB deployment.

It is difficult to tell from a perspective outside the DNS operator-registrar relationship, if AB was used to enable DNSSEC on a domain, or some other mechanism. As such, we concentrate our findings on those domains not secured with DNSSEC that otherwise have evidence of AB.

Table 1: DNSSEC amongst the top 20 DNS operators.

Operator	Domains	Unsigned		Secured		Invalid		Islands	
		Num	%	Num	%	Num	%	Num	%
GoDaddy	56 446 359	56 326 752	99.8	107 550	0.2	8 550	0.02	3 507	0.01
Cloudflare	27 790 208	26 541 985	95.5	799 377	2.9	16 694	0.1	432 152	1.6
Namecheap	10 252 586	10 119 070	98.7	126 601	1.2	5 300	0.05	1 615	0.02
Google Domain (SquareSpace)	9 931 131	5 197 647	52.3	4 496 848	45.3	109 499	1.1	127 137	1.3
WIX	7 318 524	5 989 947	81.8	74 423	2.3	2 954	0.04	1 151 200	15.7
Hostinger	6 561 661	6 556 301	99.9			5 360	0.1		
AfterNIC (GoDaddy)	5 360 163	5 349 129	99.8			11 034	0.2		
HiChina	4 637 997	4 628 516	99.8			9 481	0.2		
AWS	3 698 499	3 653 373	98.8	30 005	0.8	4 345	0.1	10 776	0.3
GName	3 558 801	3 556 082	99.9	1 145	0.03	1 002	0.03	572	0.02
NameBright	3 516 303	3 515 548	99.98	73	0.002	680	0.02	2	0.000 1
SquareSpace	2 735 515	2 710 040	99.1	24 278	0.9	1 023	0.04	174	0.01
OVH	2 662 864	1 469 425	55.2	1 169 714	43.9	2 839	0.1	20 886	0.8
Sedo	2 340 028	2 336 383	99.8			3 645	0.2		
BlueHost	1 976 091	1 960 552	99.2	13 188	0.7	136	0.06	1 215	0.06
NameSilo	1 847 474	1 846 251	99.9			1 223	0.1		
Alibaba	1 570 903	1 564 980	99.6	2 675	0.2	1 216	0.1	2 032	0.13
DynaDot	1 552 892	1 552 431	99.97			461	0.03		
Wordpress	1 549 730	1 541 499	99.5	7 824	0.5	347	0.02	60	0.004
SiteGround	1 535 176	1 533 874	99.92			1 302	0.08		

4 Results

Here, we present our results on the state of DNSSEC and AB via `CDS` and `CDNSKEY` key RRs.

4.1 DNSSEC Deployment

After excluding those zones that entirely failed to resolve, we found 268.1 M (93.2 %) zones without DNSSEC, 15.8 M (5.5 %) that were correctly signed with DNSSEC, and 640 k (0.2 %) that did not pass validation - e.g., due to invalid or expired signatures. In addition, we found 3.1 M (1.1 %) that were secure islands, *i.e.*, DNSSEC signed zones that lack DS at the parent. These zones could be secured if a corresponding `DS` RR was inserted at the parent, e.g., with AB.

Table 1 shows the deployment status of DNSSEC across zones operated by the top 20 most popular DNS operators in our dataset, representing approximately 37 % of the total dataset. 7 of these operators do not offer DNSSEC at all; the small percentage of these operators' zones with invalid DNSSEC is due to errant DS records in the parent. The rest have a DNSSEC deployment rate comparable to the whole dataset. The single percentage point deployment rates for DNSSEC can be attributed to these operators treating DNSSEC as an advanced, or premium feature, i.e., asking users to pay more.

There are two notable exceptions to this trend: Google Domains (now SquareSpace), and OVH. The reason is, that Google Domains [17] and OVH enable DNSSEC by default on zones.[2] In spite of this, a large portion of the zones are unsigned. DNSSEC is still viewed as a liability by some [1], causing these users to disable something they do not fully understand based on false pretences.

[2]No public documentation exists from OVH about DNSSEC by default. We purchased test zones from them and observed they had DNSSEC enabled.

Table 2: The top 20 DNS operators publishing CDS RRs, and the percentage of all that operator's domains that have CDS RRs. Swiss operators are marked with 🇨🇭.

#	DNS Operator	Dom. w. CDS Num	%	#	DNS Operator	Dom. w. CDS Num	%
1	Google Domains	4 624 357	46.6	11	Gandi	34 486	3.6
2	WIX	1 326 336	18.1	12	Webland 🇨🇭	26 416	76.3
3	Cloudflare	1 232 531	4.4	13	green.ch 🇨🇭	24 674	16.8
4	Simply.com	218 590	96.8	14	WebHouse	18 766	60.0
5	GoDaddy	111 078	0.2	15	Väs Hosting	13 066	98.3
6	cyon 🇨🇭	60 981	48.1	16	HostFactory 🇨🇭	12 897	68.4
7	Gransy	54 690	98.9	17	INWX	11 303	7.8
8	METANET 🇨🇭	54 522	70.5	18	OpenProvider	10 312	79.5
9	Porkbun	34 989	3.2	19	AWARDIC 🇨🇭	8 898	99.9
10	netim	34 586	40.9	20	3DNS	8 112	75.6

The reason for 16 % of WIX zones being secure islands is not particularly clear. WIX state that they do not support DNSSEC except when the zone is registered directly with them [45]. This may be part of a test deployment of DNSSEC to assess possibilities for wider roll-out. As secure islands are to be treated as unsigned zones by DNSSEC validating resolvers [38], this allows WIX to experiment with DNSSEC deployment without the possibility of causing customer zones to become unavailable.

In general, DNSSEC deployments are still comparably rare. AB may aid adoption by reducing the initial deployment barrier.

> *Key Takeaway:* DNSSEC deployment remains rare, and is still viewed by many as a premium/fickle feature, rather than a help.

4.2 CDS Deployment Status

A working CDS setup is a prerequisite for AB. Thus, an overview on the status of CDS is required, before evaluating the specifics of AB.

Of all zones scanned, 10.5 M (3.7 %) had CDS RRs published, showing some level of support for automatic DNSSEC management from the DNS operator. This is detailed in Table 2. Whereas a few large players dominate the general DNS landscape, those publishing CDS RRs tend to be smaller operators. We posit that this is because smaller organizations have less bureaucratic friction to make infrastructure changes and less technical debt that needs to be resolved before rolling out new standards. 6 of the top 20 DNS operators are Swiss; the reason for this over-representation of Swiss organizations supporting CDS is likely the financial incentives the Swiss government provides to registrars for DNSSEC deployment. This is discussed further in Sec. 6.

CDS in unsigned zones: We discovered 2 854 zones in which CDS RRs were present, despite the zone not being DNSSEC signed, either as a secured chain or as a secured island. Installing the DNSSEC RRs referred to in these CDS RRs would break the delegation of these zones, as no corresponding DNSKEY exists within the zone. The reason for the presence of such CDS RRs is unclear, but is indicative of a misconfiguration on the DNS operator's side. Per RFC8078 [18], implementers of CDS based bootstrapping must verify that the zone will validate with the new DS RRs before installing them. With compliant implementations, these errant RRs should not cause operational problems. These CDS RRs were primarily served by Canal Dominios (2 469 zones). The others had single digits of such domain names - likely test zones.

CDS Delete: For 16 unsigned zones with CDS RRs, the RRs indicated a request to delete the DS RRs in the parent. This indicates that either CDS is not much used to disable DNSSEC, or that the DNS operators that do so are proactive enough to remove CDS RRs once they have served their function. In addition to the aforementioned 16 unsigned zones with deletion requests in their CDS RRs, 3 289 DNSSEC zones had deletion requests in their CDS RRs, but remained signed. None of these had invalid DNSSEC signatures, indicating instead an unwillingness by the TLD operator or registrar to respect the DNS operator's wishes to disable DNSSEC. Conversely, 165.5 k zones were secure islands with CDS deletion RRs, indicating that the TLD operator or registrar had respected the DNS operator's request to disable DNSSEC, but that the DNS operator has not disabled DNSSEC after the DS RRs were removed in the parent. This is not a misconfiguration per se, as DNS resolvers should treat these zones as unsigned [38].

The vast majority of these secure islands with deletion requests - 160.0 k (96.7 % of 165.5 k) - have their DNS operated by Cloudflare. This represents 37.0 % of secure islands hosted by Cloudflare. Using test zones on Cloudflare, we discovered that this happens when a user configures DNSSEC for their zone and then disables it. Cloudflare does not remove DNSSEC signatures from such zones, they merely publish a deletion request via CDS. We posit that this is to avoid cases where a user disables DNSSEC without correctly removing it from their registrar, making the zone/site unreachable.

Lack of support for CDS: Despite the CDS and CDNSKEY RR types being defined in 2014 [24], we observed that for 7.6 M (2.6 % of all domains) domain names, the NSes failed to respond, or returned an error response, when queried about these RRs. Since 2003, NSes should act transparently to unknown RR types [19], and respond with NODATA instead of returning an error. NSes for these zones were either not updated since 2003, or do not follow relevant standards.

CDS correctness: A key element for bootstrapping DNSSEC with CDS is that the CDS and CDNSKEY RRs are consistent between NSes, correctly signed with DNSSEC, and that installation of these as DS RRs into the parent would not cause DNSSEC validation failures. Focusing on those zones that are secure islands, and have CDS RRs present - thus eligible for DNSSEC bootstrapping - the vast majority (179.4 k - 99.7 % of 179.9 k) of these have consistent CDS RRs returned by their NSes, only 5 333 did not. Of these 4 637 (86.9 % of 5333) were domain names where multiple DNS operators were listed as authoritative. When such multi-operator setups are used, care must be taken to coordinate certain RRs - such as DNSKEYs and CDSes - between the multiple operators, to ensure a reliable DNSSEC setup [23]. It is evident from the data that most users of multi-operator setups are not aware of these pitfalls, and thus make such configuration mistakes. However, the use of multi-operator setups remains an uncommon practice. Additionally, only 7 zones had CDS RRs that did not correspond with any DNSKEY in the zone, and only 3 zones had invalid DNSSEC signatures over their CDS RRs. This indicates that these operators are publishing correct zones, but lack the necessary coordination amongst each other.

> *Key Takeaway:* CDS sees similar levels of adoption to DNSSEC, and is generally implemented well by those who use it. Adoption of CDS is primarily driven by smaller operators.

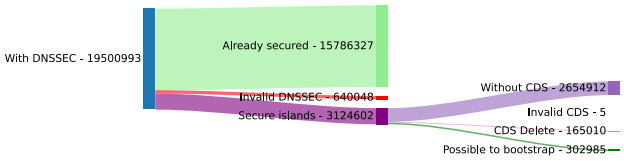

Figure 1: Breakdown of the DNSSEC status and bootstrapping possibility of the scanned dataset.

Table 3: DNS operators publishing CDS RRs in signal zones.

Domains	Cloudflare	deSec	Glauca	Others	Total
with signal CDS	1 229 568	7 314	290	279	1 237 451
↪ already secured	799 169	5 439	233	113	804 954
↪ cannot be bootstrapped	160 268	20	8	143	160 439
↪ deletion request	159 503	0	7	20	159 530
↪ invalid DNSSEC	765	20	1	123	909
↪ potential to bootstrap	270 131	1 855	49	23	272 058
↪ Signal zone incorrect	34	155	1	18	207
↪ Signal zone correct	270 097	1 700	48	5	271 828

4.3 Authenticated Bootstrapping Potential

Of all zones scanned, 271.6 M cannot benefit from AB; of those that cannot benefit, 268.1 M (98.7 %) were zones without any DNSSEC, 640.0 k (0.2 %) were zones with invalid DNSSEC, 2.7 M (1.0 %) were secure islands without extant CDS RRs, 165.0 k were secure islands with deletion requests in their CDS RRs, and 5 were secure islands with CDS RRs that did not match the DNSKEYs in the zone. 15.8 M (5.8 % of all scanned) zones were already signed, allowing them to manage key rollovers with in-zone CDS RRs only.

303 k (0.1 % of all scanned) zones could benefit from AB to complete the DNSSEC delegation chain, in that they are secure islands, with valid in-zone CDS RRs - the traditional unauthenticated bootstrapping criteria. The deployment space for AB is therefore quite small - this is illustrated in Fig. 1. To have a substantial impact on the deployment of DNSSEC, DNS operators will need to first deploy DNSSEC itself more widely, before AB will have notable impact.

Key Takeaway: The primary barrier to further DNSSEC is not adoption of AB, rather adoption of DNSSEC at all.

4.4 Authenticated Bootstrapping Status

Of all scanned, 1.2 M zones have published AB RRs, see Table 3. Three DNS operators – Cloudflare (1.2 M zones with signal CDS), deSec (7 314) and Glauca Digital (290) – generally publish CDS or CDNSKEY RRs in their AB signal zones. For all 3 operators, the zones with AB RRs represent all, or almost all, of their portfolio. In addition, one domain name each from Wordpress, One.com, AWS, 51DNS, and the Verisign Registry had RRs in the signal zone, seemingly as part of a test setup. There were 274 other zones with such RRs, for which a DNS operator could not be identified, most of these appearing to be singular test zones setup by companies or hosted on personal servers.

Of zones with signal RRs, 805.0 k are already secured with DNSSEC, thus not able to benefit from AB. It is impossible to tell, from our dataset, if these zones were configured for DNSSEC with the help of AB or not. Nonetheless, all operators are flouting the recommendation in RFC9615 [42] to remove signal RRs "once a child DNS operator determines that specific signaling RR sets have been processed". This recommendation exists to help manage the size of signal zone files, to facilitate easier processing. In the case of Cloudflare, this is because they do not operate using traditional zone files, but instead generate such DNSSEC RRs on the fly [29]. In the case of deSec, the number of signal RRs in each of the two signal zones is only on the order of 43.9 k - the number of zones with signal RRs, times the number of NSes (deSec has two), times three, one each for the CDS SHA-256 and SHA-384 RRs and one CDNSKEY RR. Excluding those zones which are already DNSSEC secured would only reduce deSec's zone files to around 11 130 RRs. Whilst this is a large number of RRs, it is not unmanageable by modern DNS software. Assuming a worst case uncompressed textual representation of all RRs in the signal zones, they are at most on the order of 6MiB each. It is likely therefore that deSec chose to forgo the additional codebase complexity of checking the DNSSEC status of each zone, in exchange for managing a larger zone file. A similar calculation applies to Glauca Digital.

160.4 k zones with signal RRs cannot be bootstrapped. The vast majority of these (159.5 k) cannot be bootstrapped because there are deletion requests published in the CDS RRs. Deletion requests only make sense in the context of a zone which is already secured with DNSSEC. These RRs are not harmful, but also have no effect in signal zones. Such deletion RRs in signal zones are published by Cloudflare and Glauca Digital, but not by deSec. This may be to reduce code complexity by publishing identical RRs in multiple places, instead of differentiating what is published where.

The other reasons are: 43 are not signed with DNSSEC; 787 are invalidly signed with DNSSEC; 32 see inconsistencies in the CDS RRs returned by different NSes; and 47 have invalid DNSSEC signatures over the in-zone CDS RRs. All those with inconsistencies between NSes were zones with multiple DNS operators, again highlighting the need for cooperation between operators in multi-signer setups.
Signal zone correctness: This leaves 272.1 k (89.8 % of zones that could be traditionally bootstrapped) that are secure islands, with some form of signal RR published, that could benefit from AB - if implemented by the DNS operator.

Publishing any random signal RR is not sufficient to enable AB. The signal zone and its contents must meet several other requirements, in order to ensure the security of the bootstrapping process. The signal zone must not include any zone cuts. Only one zone eligible for bootstrapping violated this requirement - `copacabanasomostudestino.com.bo.`. This happened because, by seemingly a copy-paste error, one of its NSes was set at the registry to `ns1.desc.io.` instead of `ns1.desec.io.`. This alone would not cause a zone cut. However, `desc.io.` is managed by GoDaddy's Afternic domain parking service. The Afternic NSes respond to all queries identically (e.g., responding to NS queries with `ns1.namefind.com.` and `ns2.namefind.com.`), thus creating the illusion of a zone cut at every level of the DNS tree.

The signal RRs must also be published under every NS. 206 violated this requirement. 17 of these were due to the zone having multiple DNS operators, and the signal RRs only being published by one DNS operator. Of the others, 34 were hosted by Cloudflare, 154 by deSec, and 1 by Glauca Digital. 33 zones hosted by Cloudflare that violated this requirement had disagreements between the NSes set as authoritative by Cloudflare, and those set in the TLD

zone. Such a misconfiguration normally causes no harm, and is not even noticeable without looking closely, as all Cloudflare NSes will respond to any query for any zone (see Sec. 3). However, in the case of AB, Cloudflare will not synthesize the RRs for NSes that do not match what it believes the authoritative NSes are, causing this violation of the requirements. The remaining zone (`fonswitch.com.`) was a transient failure by Cloudflare to respond correctly during the scan, and a subsequent check of this zone succeeded.

Similarly, the one zone with such an error from Glauca Digital appeared to be a copy-paste error. After conversations with Glauca, it became evident that the reason for this is that their customer had mistakenly put these RRs into the zone of their own accord — it was not a mistake in the setup of Glauca. Glauca allows customers to create additional `NS` RRs at the zone root to support multi-signer DNSSEC setups.

24 of violating zones hosted by deSec exhibited a similar misconfiguration, with additional spurious NSes, e.g., `ns1.desec.org.`. All other zones were transient failures by deSec to respond correctly during the scan. The one exception to this was `quaddy.vip.`. deSec claimed that it was authoritative for this zone via the `SOA` RR, but also claimed that this zone had *no* NSes. How such a configuration error came about is not at all clear to us.

This leaves 271.8 k (99.9 % of zones with some form of signalling RR) that do not have an erroneous zone cut, and have signalling RRs published under every NS. The `CDS` RRs published in the signalling zone must be correctly signed with DNSSEC. All zones hosted by Cloudflare and Glauca Digital had correctly formatted and validly signed DNSSEC RRs. 70 of those hosted by deSec had DNSSEC validation failures in the signalling zones. As before, following further checks, these were transient errors in which deSec returned invalid signatures during the scan, but now returns correct DNSSEC signatures. There was one additional zone with invalid DNSSEC signatures in the signal zone the signatures in the signal zones had expired. The NSes indicate this is likely a personal test zone setup by an IT professional. It was probably configured for experimentation with AB, then forgotten about and left to decay into this state.

The RRs published in the signalling zones must match those in the zone proper. This was the case with every zone. There were no other errors that would prevent AB. Thus, 271.8 k of 272.1 k zones (99.9 %) that have some indication of AB implement it correctly, and would benefit from it if and when registrars and registries implement it.

Key Takeaway: AB is not widely implemented (only 3 implementations), but is implemented correctly in almost all (99.9 %) cases it is.

5 Related Work

Researchers have evaluated the deployment of DNSSEC and visible errors or misconfigurations throughout the years [34, 27, 10, 6, 7]. In 2017, Chung et al. [7] found that a common problem is the required interaction between domain owners and registrars. Furthermore, Chung et al. [6] showed that 30 % of validation errors are due to missing `DS` RRs. In 2023, Nosyk et al. [31] showed that missing or incorrect `DS` RRs are a common problem. Müller et al. [30] provided insights into DNSSEC key rollovers to allow informed operations. They focus on guidelines, when secure rollovers and DS RR changes are possible but there is no automation of the process. Osterweil et al. [33] evaluated the process of key rollovers in the wild over 15 years. They show, that previous mechanisms do not follow RFC guidance and should be improved.

In 2017, Chung et al. measured DNSSEC deployment rates of 0.6 % to 1.0 %; our work shows an increase in the adoption of DNSSEC to 5.5 %. This matches the DNSSEC deployment statistics published by Verisign for `.com` and `.net` [44].

Additionally, Chung et al. found upwards of 2 % of zones failing DNSSEC validation. We are pleased to see that this has decreased to 0.2 % per our measurements.

To the best of our knowledge, there is no related work regarding (authenticated) bootstrapping. Related work has shown that DNSSEC is not widely deployed, parent-child inconsistencies are common errors and key rollovers are complicated. Our work fills this gap and provides a first view on the current ecosystem and the potential of AB to improve the adoption of DNSSEC.

6 Conclusion

In this paper, we present a large scale study of the current state of DNSSEC, its deployment and correctness of `CDS` and `CDNSKEY` RRs and the potential of the new AB mechanism. While DNSSEC usage remains low (5.5 % in our dataset), we see that adoption has increased compared to previous studies from 2017 [6]. Initial efforts to support AB are visible, and it is deployed correctly by those who implement it, primarily Cloudflare. Of 303.0 k secure islands with correct in-zone `CDS` RRs, 272.1 k already have AB.

Further work is needing on coordination between parties in multi-operator DNSSEC setups. Although they are uncommon, we show errors stemming from inconsistencies in DNSSEC records between operators, likely caused by a lack of such coordination.

Interestingly, we find a notable impact of financial incentives to deploy DNSSEC, e.g., `.se` offers a discount of 10 SEK per year [16], `.eu` offers a discount of 0.12 EUR per year [37], and `.ch` and `.li` offer 1 CHF per year [2]. Of these, only SWITCH–the operator of `.ch` and `.li`–implements AB. As shown in Sec. 4.2, there is a notable concentration of Swiss registrars and DNS operators amongst supporting `CDS`. This indicates that such financial incentives can be highly beneficial in increasing DNSSEC adoption.

Future work could look into other parent/child synchronization mechanisms emerging from the IETF, such as CSYNC records [20].

Acknowledgements

We wish to thank Peter Thomassen, the author of the Authenticated Bootstrapping RFC for his guidance on conducting this work. We additionally extend our thanks to the reviewers for their hard work, and the shepherd for helping us refine this work. Finally, as a disclosure of possible conflicts of interest, we note that Q Misell is also affiliated with Glauca Digital.

References

[1] Derek Atkins and Rob Austein. 2004. Threat Analysis of the Domain Name System (DNS). RFC 3833. (Aug. 2004). doi:10.17487/RFC3833.

[2] 2024. *Automated DNSSEC Provisioning. Guidelines for CDS processing at Switch.* (Apr. 2024). https://www.nic.ch/export/shared/.content/files/SWITCH_CDS_Manual_en.pdf.

[3] Michael Bauland. 2024. CDNSKEY in TANGO Registry Services CORE Registry Software. Retrieved May 9, 2025 from https://www.icann-hamster.nl/ham/soac/ssac/dnssec/icann76/4.5%20Bauland%20-%20CDNSKEY%20Support%20in%20TANGO%20Registry%20Services.pdf.

[4] Robert T. Braden. 1989. Requirements for Internet Hosts - Communication Layers. RFC 1122. (Oct. 1989). doi:10.17487/RFC1122.

[5] Ondřej Caletka. 2025. Support for cds/cdnskey/csync updates. (2025). https://github.com/oskar456/cds-updates.

[6] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. A longitudinal, End-to-End view of the DNSSEC ecosystem. In *Proc. USENIX Security Symposium*. ISBN: 978-1-931971-40-9.

[7] Taejoong Chung, Roland van Rijswijk-Deij, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. Understanding the Role of Registrars in DNSSEC Deployment. In *Proc. ACM Internet Measurement Conference (IMC)*. doi:10.1145/3131365.3131373.

[8] Cisco. 2025. Umbrella Top 1M List. Retrieved May 9, 2025 from https://umbrella.cisco.com/blog/cisco-umbrella-1-million.

[9] Cloudflare. 2025. Cloudflare Radar. Retrieved May 9, 2025 from https://radar.cloudflare.com/.

[10] Tianxiang Dai, Haya Shulman, and Michael Waidner. 2016. DNSSEC Misconfigurations in Popular Domains. In *Cryptology and Network Security*. ISBN: 978-3-319-48965-0.

[11] David Dittrich, Erin Kenneally, et al. 2012. The Menlo Report: Ethical principles guiding information and communication technology research. *US Department of Homeland Security*.

[12] CORE Internet Council of Registrars. 2023. *DNSSEC Practice Statement for the .swiss TLD*. CORE Internet Council of Registrars. (Feb. 2023). https://www.nic.swiss/dam/nic/de/dokumente/SWISS-DPS.pdf.download.pdf/SWISS-DPS.pdf.

[13] 1987. Domain names - implementation and specification. RFC 1035. (Nov. 1987). doi:10.17487/RFC1035.

[14] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *Proc. USENIX Security Symposium*. ISBN: 9781931971034.

[15] Donald E. Eastlake, 3rd and Charles W. Kaufman. 1997. Domain Name System Security Extensions. RFC 2065. (Jan. 1997). doi:10.17487/RFC2065.

[16] Anne-Marie Eklund-Löwinder. 2014. Dnssec deployment in sweden. How do we do it? (June 2014). https://archive.icann.org/meetings/london2014/en/schedule/wed-dnssec/presentation-dnssec-deployment-sweden-25jun14-en.pdf.

[17] Google. 2023. Make domains safe with security settings. Retrieved May 9, 2025 from https://web.archive.org/web/20230318150001/https://support.google.com/domains/answer/9954803?hl=en&ref_topic=3251230.

[18] Ólafur Guðmundsson and Paul Wouters. 2017. Managing DS Records from the Parent via CDS/CDNSKEY. RFC 8078. (Mar. 2017). doi:10.17487/RFC8078.

[19] Andreas Gustafsson. 2003. Handling of Unknown DNS Resource Record (RR) Types. RFC 3597. (Sept. 2003). doi:10.17487/RFC3597.

[20] Wes Hardaker. 2015. Child-to-Parent Synchronization in DNS. RFC 7477. (Mar. 2015). doi:10.17487/RFC7477.

[21] Scott Hollenbeck. 2009. Extensible Provisioning Protocol (EPP). RFC 5730. (Aug. 2009). doi:10.17487/RFC5730.

[22] Scott Hollenbeck and James Gould. 2010. Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP). RFC 5910. (May 2010). doi:10.17487/RFC5910.

[23] Shumon Huque, Pallavi Aras, John Dickinson, Jan Včelák, and David Blacka. 2020. Multi-Signer DNSSEC Models. RFC 8901. (Sept. 2020). doi:10.17487/RFC8901.

[24] Warren "Ace" Kumari, Ólafur Guðmundsson, and George Barwood. 2014. Automating DNSSEC Delegation Trust Maintenance. RFC 7344. (Sept. 2014). doi:10.17487/RFC7344.

[25] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczynski, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proc. Network and Distributed System Security Symposium (NDSS)*. doi:10.14722/ndss.2019.23386.

[26] Edward P. Lewis and Alfred Hoenes. 2010. DNS Zone Transfer Protocol (AXFR). RFC 5936. (June 2010). doi:10.17487/RFC5936.

[27] Wilson Lian, Eric Rescorla, Hovav Shacham, and Stefan Savage. 2013. Measuring the practical impact of DNSSEC deployment. In *Proc. USENIX Security Symposium*. ISBN: 9781931971034.

[28] Majestic. 2025. The Majestic Million. Retrieved May 9, 2025 from https://majestic.com/reports/majestic-million/.

[29] Marek Majkowski. 2019. RFC8482 - Saying goodbye to ANY. Cloudflare, Inc., (Mar. 2019). https://blog.cloudflare.com/rfc8482-saying-goodbye-to-any/.

[30] Moritz Müller, Taejoong Chung, Alan Mislove, and Roland van Rijswijk-Deij. 2019. Rolling With Confidence: Managing the Complexity of DNSSEC Operations. *IEEE Transactions on Network and Service Management*. doi:10.1109/TNSM.2019.2916176.

[31] Yevheniya Nosyk, Maciej Korczyński, and Andrzej Duda. 2023. Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting. In *Proc. ACM Internet Measurement Conference (IMC)*. doi:10.1145/3618257.3624835.

[32] nTLDStats. 2025. DNSSEC SCOREBOARD. Retrieved May 9, 2025 from https://ntldstats.com/tld.

[33] Eric Osterweil, Pouyan Fotouhi Tehrani, Thomas C. Schmidt, and Matthias Wählisch. 2022. From the Beginning: Key Transitions in the First 15 Years of DNSSEC. *IEEE Transactions on Network and Service Management*. doi:10.1109/TNSM.2022.3195406.

[34] Eric Osterweil, Michael Ryan, Dan Massey, and Lixia Zhang. 2008. Quantifying the operational status of the DNSSEC deployment. In *Proc. ACM Internet Measurement Conference (IMC)*. doi:10.1145/1452520.1452548.

[35] Craig Partridge and Mark Allman. 2016. Addressing Ethical Considerations in Network Measurement Papers. *Communications of the ACM*, 59, 10, (Oct. 2016).

[36] 2025. Public suffix list. Mozilla Foundation, (2025). https://publicsuffix.org.

[37] EURid vzw. 2017. *Release Notes: EPP Updates and Bug fixes, DNS Quality Introduction, My .eu Redesign*. EURid vzw. (Aug. 2017). https://registry.eu/media/filer_public/9b/54/9b541d8f-1c0e-4fca-a3a6-46149ad3d387/release_notes_epp_updates_and_bug_fixes_dns_quality_introduction_my_eu_redesign_v10_release_11_october_2017.pdf.

[38] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Protocol Modifications for the DNS Security Extensions. RFC 4035. (Mar. 2005). doi:10.17487/RFC4035.

[39] Raffaele Sommese, Roland van Rijswijk-Deij, and Mattijs Jonker. 2024. This Is a Local Domain: On Amassing Country-Code Top-Level Domains from Public Data. *ACM SIGCOMM Computer Communication Review*.

[40] Florian Steurer, Anja Feldmann, and Tobias Fiebig. 2025. A Tree in a Tree: Measuring Biases of Partial DNS Tree Exploration. In *Proc. Passive and Active Measurement (PAM)*. doi:10.1007/978-3-031-85960-1_5.

[41] 2021. The online world. Nominet UK, (2021). https://nominet.uk/wp-content/uploads/2024/09/The-Online-World-Map-2020.pdf.

[42] Peter Thomassen and Nils Wisiol. 2024. Automatic DNSSEC Bootstrapping Using Authenticated Signals from the Zone's Operator. RFC 9615. (July 2024). doi:10.17487/RFC9615.

[43] Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras. 2016. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. *IEEE Journal on Selected Areas in Communications*. doi:10.1109/JSAC.2016.2558918.

[44] Verisign. 2025. DNSSEC SCOREBOARD. Retrieved May 9, 2025 from https://www.verisign.com/en_US/company-information/verisign-labs/internet-security-tools/dnssec-scoreboard/index.xhtml.

[45] WIX Help Center. 2025. Connecting a Domain to the Wix Name Servers. Retrieved May 9, 2025 from https://support.wix.com/en/article/connecting-a-domain-to-the-wix-name-servers.

A Ethics

Our measurements focus on generally public data. The overall scan campaign follows standards by our institution and the community [11, 35, 14]. We limit the impact on infrastructure with a conservative scanning rate and informed others about our measurements via WHOIS, reverse DNS entries, and websites hosted on all scanning machines. We react to all inquiries and opt-out requests, but we received no request regarding this study. Furthermore, we submitted our study design to our ethical review board, who attested no concerns.

B Organizational Hierarchies in the DNS

The DNS is a protocol that interacts with people, therefore its operation is not only constrained technically, but also by the organizational and legal relationships and hierarchies present in the real world. There are a few key entities relevant to the deployment of DNSSEC:

Registries operate TLDs such as `.com` and `.net`. Each TLD has exactly one registry in charge of it. These registries collect registration fees from registrars for domain names, and maintain the DNS zone file with zones registered in that TLD.

Registrars negotiate contracts with the registries who operate the TLDs they wish to sell to their customers, and are the main customer-facing view of the DNS. When a Internet user wants a new domain name, they go to their registrar of choice to purchase it.

DNS operators run the authoritative DNS servers for a given domain name, often being authoritative for several domain names.

Many pieces of information are exchanged between these entities to fulfil their legal obligations to each other, but the two pieces of information of interest to us are the NS RRs given to the registry by the registrar to delegate the domain name to its DNS operator, and the DS RRs given to allow its securing using the DNSSEC.

C Policies for Bootstrapping without RFC9615

The following lists different policies suggested by the IETF to authenticate CDS before AB. They are based on RFC8078 [18] and only listed for brevity here.

Accept via an Authenticated Channel in which the DNS operator has some authenticated backchannel to send CDS RRs to the registry. This option presents operational difficulties due to the lack of a standardized backchannel and authentication mechanism.

Accept with Extra Checks where the registrar sends an email, or other such notification, to the customer, asking them to confirm the provisioning of CDS RRs. This also presents operational difficulties, as many customers are unlikely to understand the meaning of such a notification, or its implications, causing them not to take any action to deploy DNSSEC.

Accept after Delay where the registrar installs the new DS RRs after seeing no changes to the CDS RRs for a period of time, from different Internet vantage points. This offers some protection against hijacking to install malicious DS RRs, but is not a perfect guarantee.

Accept with Challenge in which a registrar gives a challenge token to the customer (via the registrar) to insert into zone, to prove intent to bootstrap DNSSEC. This presents the operational difficulties of both **Accept via an Authenticated Channel** and **Accept with Extra Checks**, as there is no standard for such a token, its communication between different entities, nor is the customer likely to be aware what to do with such a token.

Accept from Inception where the registrar checks the CDS RRs as the time of domain registration. This requires the DNS operator to configure the zone and serve CDS RRs before registration, which is often not the case.

D Feasibility of registries deploying AB

In total, our scans generated 6.5TiB of data over a scan duration of just over a month. For an average zone, we needed to send approximately 20 queries to each nameserver, of which most had 2. At first, this might appear like an insurmountably large amount of data required to assess child zones for AB, especially in larger zones like `.com`. However, our scan collected far more data than is required for a registry to adequately implement AB.

Firstly, we stored the whole DNS message for every query made; this allowed us to assess the causes of errors/mistakes, but in the context of a registry's deployment they need not consider the whole DNS message after parsing it. Secondly, we scanned every single domain in our dataset exhaustively; this is not what a registry would do. A registry could exclude, at a minimum, those domains with extant DS records. It can also 'short-circuit' in its implementation, abandonment future queries after discovering an unsigned zone, or at the first sign of a configuration mistake.

On the number of individual DNS queries required, a registry implementing AB need not query as extensively as us, as they are not looking for the reasons behind possible inconsistencies, merely enough records to form the cryptographic chain required to bootstrap.

Per our results, this would leave only 1.2 M of the total 287.6 M domains that need to be scanned to a similar extent that we did here — a far more manageable amount for a registry.