On the Adoption of the Elliptic Curve Digital Signature Algorithm (ECDSA) in DNSSEC

Roland van Rijswijk-Deij*†, Mattijs Jonker* and Anna Sperotto*
*University of Twente, Enschede, the Netherlands
†SURFnet bv, Utrecht, the Netherlands
e-mail: {r.m.vanrijswijk, m.jonker, a.sperotto}@utwente.nl

***Abstract*—The Domain Name System Security Extensions (DNSSEC) are steadily being deployed across the Internet. DNSSEC extends the DNS protocol with two vital security properties, authenticity and integrity, using digital signatures. While DNSSEC is meant to solve security issues in the DNS, it also introduces a new one: the digital signatures significantly increase DNS packet sizes, making DNSSEC an attractive vector to abuse in amplification denial-of-service attacks. By default, DNSSEC uses RSA for digital signatures. Earlier work has shown that alternative signature schemes, based on elliptic curve cryptography, can significantly reduce the impact of signatures on DNS response sizes. In this paper we study the actual adoption of ECDSA by DNSSEC operators, based on longitudinal datasets covering over 50% of the global DNS namespace over a period of 1.5 years. Adoption is still marginal, with just 2.3% of DNSSEC-signed domains in the `.com` TLD using ECDSA. Nevertheless, use of ECDSA is growing, with at least one large operator leading the pack. And adoption could be up to 42% higher. As we demonstrate, there are barriers to deployment that hamper adoption. Operators wishing to deploy DNSSEC using current recommendations (with ECDSA as signing algorithm) must be mindful of this when planning their deployment.**

I. Introduction

The Domain Name System (DNS) is a vital part of the Internet's infrastructure. It maps names to machine-readable information, e.g., mapping `www.example.com` to the IP address `93.184.216.34`. The original DNS has a critical vulnerability, called cache poisoning [1], that allows skilled attackers to falsify information in the DNS and potentially redirect thousands of Internet users to malicious sites.

The DNS Security Extensions (DNSSEC) were introduced to address this vulnerability. Using digital signatures, DNSSEC guarantees the authenticity and integrity of DNS data, thus thwarting attackers that seek to falsify DNS responses. However, while DNSSEC solves this flaw in the DNS, it introduces a serious new vulnerability. The digital signatures DNSSEC adds to the protocol make DNS responses much larger. This makes DNSSEC an attractive vector to abuse in amplification denial-of-service attacks [2], [3]. The root cause of why DNSSEC makes responses so much larger, is the use of RSA for digital signatures. Current official recommendations [4], [5] suggest using 2048-bit RSA keys. If followed, this means every signature added to a DNS response requires 256 octets. Earlier work showed there are attractive alternatives to RSA [6]. In particular, Elliptic Curve Cryptography (ECC) offers better security with smaller signatures[1], with only minor drawbacks [7]. Thus, use of ECC can vastly reduce the attack potential in DNSSEC. Two algorithms, ECDSA P-256 and P-384, were standardised for use in DNSSEC in 2012 [8]. Yet when [6] was published, in 2015, there was next to no adoption of these algorithms, with 99.99% of signed domains in `.com`, `.net` and `.org` still using RSA.

There is increasing interest in the use of ECC for DNSSEC. At least one large operator, CloudFlare [9], has thrown its weight behind deployment of ECC in DNSSEC. Second, the IETF is standardising additional ECC algorithms for DNSSEC [10]. Finally, there has been active evangelisation of the use of ECC in DNSSEC in recent conferences frequented by operators, such as ICANN meetings, the IETF and NANOG. This raises the question whether these efforts are paying off.

In this paper we study the adoption of ECC by DNS operators. Our main contributions are that we:

- provide the first detailed insight into operational adoption of a new cryptographic algorithm in DNSSEC;
- show how adoption of ECC in DNSSEC grows, based on longitudinal datasets that span up to 1.5 years;
- show evidence of hurdles to deployment in our datasets;
- illustrate how adoption by a single operator can potentially be a game changer for the use of ECC in DNSSEC.

II. Methodology and Data

A. Methodology

To study the adoption of ECC, we search for domains that use the currently standardised ECC algorithms, ECDSA P-256 and P-384 [8]. Algorithm identifiers in three DNSSEC-specific resource record (RR) types signal the use of these algorithms:

- `RRSIG` – the record type for digital signatures; the signature in an `RRSIG` covers a so-called *RRset*, which consists of all records of a single type for a single name (e.g. all `A` records for `www.example.com`).
- `DNSKEY` – contains information on the public keys that are required to validate the signatures in `RRSIG` records.
- `DS` – the *delegation signer* record resides in the parent zone and signals a *secure delegation* from the parent to the signed zone. A properly DNSSEC-signed domain has a *trust chain* from the root of the DNS all the way down[2].

[1] ECDSA P-256 signatures are 4 times smaller than RSA 2048.

[2] More on DNSSEC trust chains can be found in [6], [11].

978-3-901882-85-2 © 2016 IFIP

Dataset#	TLD	start date	end date	#domains*	#signed*	(%*)
1	.com .net .org	Mar. 1, 2015	Aug. 31, 2016	127.0M 15.6M 10.8M	0.58M 0.10M 0.07M	(0.46%) (0.64%) (0.67%)
2	.nl	Feb. 9, 2016	Aug. 31, 2016	5.6M	2.54M	(44.95%)
3	.gov	August 31, 2016		1151	1023	(88.88%)

*on August 31, 2016

TABLE I
DATASETS

Based on these records, we identify two levels of adoption:

- ***Full deployment*** – there are signatures (RRSIG records), keys (DNSKEY records) and a secure delegation (DS record(s)) for one or more ECC algorithms.
- ***Partial deployment*** – there are signatures and possibly keys for one or more ECC algorithms, but no secure delegation (DS record(s)).

B. Datasets

The data used for this study comes from a large-scale active DNS measurement platform [12][3]. Table I shows which data we used from this platform. The datasets used cover around 50% of the global DNS namespace. The first dataset was selected because it covers the longest time period, and includes the point in time when the statistics for [6] were collected (which show virtually no adoption of ECDSA). The second dataset covers the .nl ccTLD. This ccTLD has the largest DNSSEC deployment worldwide, and enabled support for ECDSA secure delegations only recently (on Mar. 1, 2016). The third dataset is a one-day snapshot of the .gov TLD reserved for US Government use. The snapshot is based on a publicly available list of .gov domains [13]. Studying .gov is of interest as DNSSEC-signing is mandatory and there are specific guidelines that recommend a switch to ECDSA signing by 2015 [4].

III. RESULTS

A. Adoption of ECDSA in .com, .net and .org

First, we look at adoption of ECDSA in .com, .net and .org. These TLDs supported secure delegations for domains signed using ECDSA P-256 and P-384 over the entire period covered by the dataset. From here on, the analysis exclusively focuses on ECDSA P-256, as adoption of ECDSA P-384 is negligible[4] (< 0.01%). Figure 1 shows adoption of ECDSA P-256 from October 1, 2015 until the end of the dataset. Adoption of ECDSA P-256 is virtually non-existent until November 10, 2015, when CloudFlare introduces its DNSSEC service [9]. Until April 2016, the use of ECDSA P-256 for DNSSEC-signed domains is almost exclusively limited to domains that use CloudFlare's DNSSEC service. From early April, however, this changes as the first domains using ECDSA P-256 not operated by CloudFlare start appearing (the distinction is shown using darker and lighter colours, as the legend shows). Almost all of these domains are operated by one company (a media venture).

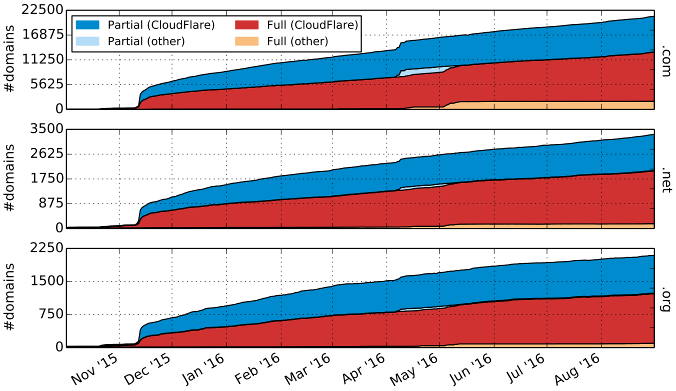

Fig. 1. ECDSA P-256 adoption in .com, .net and .org

A second observation, that stands out, is that there are a significant number of partial deployments of DNSSEC with ECDSA P-256. Section II-A defined a partial deployment as having signatures and keys, but no secure delegation. Effectively, this means that the domain is DNSSEC-signed, but that the signatures cannot be validated by DNS resolvers, as no chain of trust exists. Conversely, almost 39% of signed domains that use ECDSA P-256 in the .com TLD cannot be validated at present (for .net this is also almost 39%, for .org it is almost 42%). While this is not an operational problem (DNS resolution for these domains will still function correctly), it does signal a potential barrier to adoption. The cause of this problem is the way in which secure delegations are currently created in the DNS. While DNSSEC signing can be done independently by a DNS operator, the creation of a secure delegation has to go through the so-called RRR (Registrant, Registrar, Registry) channel, which is primarily used for domain-name registration. This has two implications. First, registrants (domain name owners) need to request a secure delegation through their domain name registrar if they or their DNS operator signs a domain. Second, registrars need to support the creation of secure delegations for domains signed using ECDSA P-256. If either one of these conditions is not fulfilled, then deployment can only be partial. DNS and TLD registry operators recognise the existence of this problem. RFC 7344 [14] provides a technical means to signal information for the creation and maintenance of secure delegations directly through the DNS, and several parties, including CloudFlare and the ccTLD registry operator for .ca (CIRA), currently have an active Internet draft describing a means to bootstrap the creation of secure delegations [15].

While this problem clearly is a barrier to deployment of ECDSA P-256 for DNSSEC signing, it also exists for other DNSSEC algorithms. Figure 2 shows the adoption state of two variants of RSA signing over the full 18-month dataset. The figure shows that while deployments for one of these (RSA-SHA1-NSEC3, left-hand side of the figure) are almost entirely full deployments, for the other one (RSA-SHA256-NSEC3) partial deployments outnumber full deployments for all three TLDs. Further analysis of these partial deployments shows that they occur for at least 15 DNS operators that sign more than

[3] http://www.openintel.nl/

[4] While ECDSA P-384 is cryptographically stronger, there is not much incentive to use it over ECDSA P-256. Recommendations in [4], [5] indicate that ECDSA P-256 is sufficiently strong for 30+ year use. And as [6] illustrates, gains in reduction of amplification are far less for ECDSA P-384.

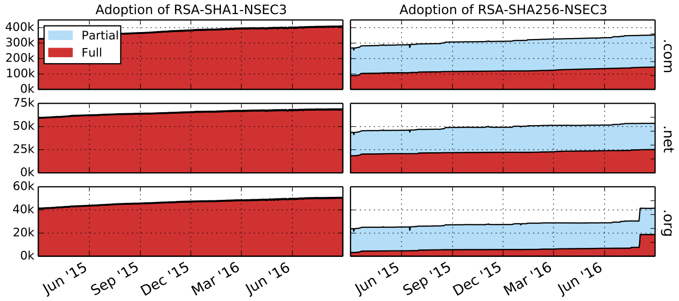

Fig. 2. Adoption of RSA variants in `.com`, `.net` and `.org`

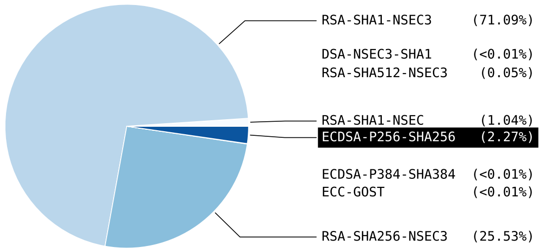

Fig. 3. Use of DNSSEC algorithms in `.com` on August 31, 2016

1000 domains. While a detailed analysis of the causes of these partial deployments is outside the scope of this paper, an initial assessment shows the most likely cause again is either a lack of action by the registrant (to create the secure delegation), or a lack of support for secure delegations by the registrar.

Finally, we mapped the distribution of signing algorithms used in `.com` (which has the largest ECDSA deployment). As Figure 3 shows, ECDSA P-256 use is still modest.

B. *CloudFlare-specific metrics*

Given that CloudFlare operates the largest deployment of ECDSA P-256 in `.com`, `.net` and `.org`, we specifically looked at developments in this deployment. CloudFlare's DNSSEC service is an optional feature of its DNS DDoS protection service, which allows customers to protect the name servers for their domain. To use this service, domain owners configure CloudFlare name servers as authoritative name servers for their domain. This means that use of CloudFlare's DNS service can be detected in the dataset by looking for `NS` records that point to authoritative name servers operated by CloudFlare [16]. Figure 4 shows the percentage of domains operated by CloudFlare that enable DNSSEC on a given day and indicates if these are new or existing CloudFlare customers. In other words: is DNSSEC something that only new customers enable, or do existing customers also turn it on? As a detection criterion, we label domains that were using CloudFlare name servers four weeks prior to DNSSEC signing as 'existing' customers, and all other domains as 'new'. Figure 4 covers the time period from CloudFlare announcing the service [9] until the end of the dataset. As the figure shows, during the initial weeks of the service being offered, enablements are dominated by existing customers (75%). After that phase, though, the majority of enablements come from new customers.

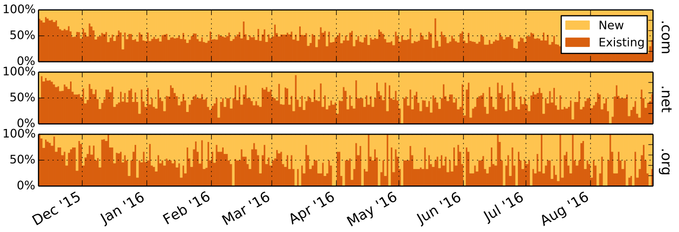

Fig. 4. New vs. existing CloudFlare customers activating DNSSEC

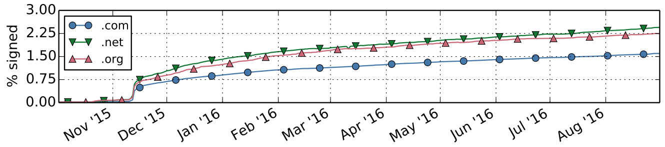

Fig. 5. Percentage of CloudFlare-operated domains that are signed

TLD	#domains	#signed	(%)	%ECDSA	#CloudFlare	%signed⋆	%ECDSA⋆
`.com`	127.0M	0.58M	(0.46%)	2.27%	1.20M	1.40%	67.9%
`.net`	15.6M	0.10M	(0.64%)	2.08%	0.13M	1.45%	56.9%
`.org`	10.8M	0.07M	(0.67%)	1.70%	0.09M	1.48%	55.3%

⋆potential deployment including CloudFlare

TABLE II
CLOUDFLARE'S DNSSEC POTENTIAL IN .COM, .NET AND .ORG

As discussed in Section III-A, there are barriers to adoption of DNSSEC-signing using ECDSA P-256. For instance, Figure 1 showed that up to 42% of signed domains do not have a full secure delegation. This is not the entire story, however. Using the analysis previously discussed, we have also tracked the total number of CloudFlare users over time. The analysis shows that only a fraction of these users have enabled DNSSEC. Figure 5 shows the percentage of domains operated by CloudFlare that are DNSSEC-signed. As the figure shows, while there is growth, the percentage is still small ($< 2.5\%$). If all CloudFlare users were to fully deploy its DNSSEC service, however, the picture would change dramatically. In fact, as Table II illustrates, if all domains operated by CloudFlare fully deploy DNSSEC, the number of signed domains more than doubles in all three TLDs and ECDSA P-256 would become the dominant signing algorithm in these TLDs overnight.

C. *Adoption of ECDSA in .nl*

The second dataset selected for this study covers the `.nl` ccTLD, which – unlike `.com`, `.net` and `.org` – did not support secure delegations with ECDSA at the start of the dataset. This allows us to study ECDSA adoption before and after the ccTLD started supporting secure delegations for this algorithm. Figure 6 shows partial and full adoption of ECDSA in the `.nl` ccTLD. Three things stand out. First, initial ECDSA deployment is dominated by CloudFlare, just like in `.com`, `.net` and `.org`. From the middle of June, however, the first domains signed with ECDSA from other operators appear, and toward the end of the dataset these outnumber domains operated by CloudFlare. These domains are mostly operated by two hosting companies, one who enabled ECDSA signing from June 16th, the other from August 18th. This growth coincides with the release of PowerDNS 4.0, an authoritative DNS server implementation popular among

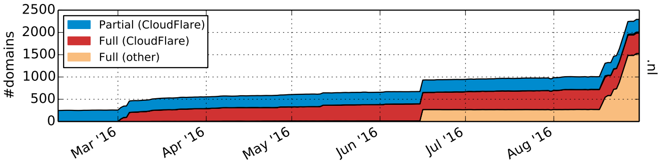

Fig. 6. ECDSA P-256 adoption in .nl

Dutch hosting companies. In this PowerDNS release, the default signing algorithm was changed to ECDSA P-256 [17].

Second, the deployment of ECDSA for signing is quite modest in .nl, especially compared to the total number of signed domains, at just 0.08%. As we will discuss in Section IV, this is unlikely to change in the near future.

Finally, 8.4% of domains (192 in total) that were signed using ECDSA P-256 at the end of the dataset were already signed at the start of the dataset (all through CloudFlare), when the .nl ccTLD did not yet support secure delegations for this algorithm. Remarkably, only 37 of these domains have gone from having a partial deployment to a full deployment (i.e. now have a secure delegation). We performed a closer examination, to see if those domains that still have a partial deployment encountered the barriers discussed in Section III-A. To do this, we determined the domain name registrars for these domains and checked if these registrars support secure delegations for ECDSA P-256. It turns out that over half of these domains are registered through companies that support ECDSA P-256 secure delegations. While we cannot be certain, we speculate that the registrants of these domains enabled CloudFlare's DNSSEC service at a (much) earlier point in time and simply forgot to request a secure delegation when that became possible for .nl. For the other domains, either the registrar does not support ECDSA P-256 secure delegations or the registrant did not request a secure delegation.

D. Adoption of ECDSA in .gov

As Section II-B mentions, we also measured adoption for the .gov TLD, specifically because NIST recommends switching to ECDSA [4]. While .gov has a very high use of DNSSEC (88.9% of domains deploy DNSSEC), not a single domain is signed using ECDSA.

IV. Conclusions

In this paper we analysed the deployment of elliptic curve digital signature algorithms for DNSSEC in five top-level domains. In general, deployments of ECDSA are still scarce. The largest deployment, in .com, covers about 2.3% of signed domains. Rather poignantly, despite guidance from NIST, not a single domain in the US Government's .gov TLD has deployed ECDSA so far. Furthermore, roll-out is mostly driven by a single operator, CloudFlare, with little uptake by others.

Nevertheless, there are opportunities. First, if current barriers to adoption – registrants failing or forgetting to create secure delegations and/or registrars and registries failing to support secure delegations – can be overcome, universal deployment of DNSSEC for CloudFlare users alone can more than double the number of DNSSEC-signed domains in .com, .net and .org, and make ECDSA P-256 the dominant signing algorithm overnight. Second, while certainly not a niche technology, DNSSEC deployment is far from ubiquitous, with recent estimates setting deployment at around 3% [6]. This means – given the benefits in terms of security and stability that ECC algorithms offer – that there is also an opportunity to 'do it right', and use ECC, for the 97% of domains that have not yet deployed DNSSEC.

Lessons for operators – The most important takeaway is that the adoption of new algorithms in the complex DNSSEC ecosystem takes a lot of time. The uptake of ECDSA is disappointing, especially given that it was already standardised in 2012 [8] and there has been active evangelisation for at least two years. This is true throughout the DNSSEC ecosystem; in related work, Huston and Michaelson [18] show that support for ECDSA among DNS resolver operators is also not yet universal. It is much higher than on the signing side, though, with 82% of validating resolvers supporting ECDSA. We note that the Internet community is trying to learn from this slow deployment as input for the roll-out of future standards [19].

Domain name operators wishing to secure their domains with DNSSEC should be mindful of deployment hurdles. If they want to follow current advice to sign using ECDSA [6], [7], they need to take care when selecting a DNS operator and domain name registrar. These need to support DNSSEC in full, including the newly standardised ECC algorithms. Finally, there may also be hard times ahead for those 3% of domain name owners that have already fully deployed DNSSEC using RSA. The transition from RSA to ECC signing algorithms is very complex. This so-called algorithm rollover [20] requires concurrently signing a zone with both algorithms. It is highly likely that this will require a manual intervention by operators, since only one recently released DNSSEC implementation supports automated algorithm rollovers [21]. If it indeed becomes best practice to use ECC algorithms, then these operators are in for a hard and potentially costly transition. This is especially true for .nl, with over 2.5M signed domains using RSA. The Dutch may once again be confronted with their own *'law of the handicap of a headstart'* [22].

Future work – as mentioned in the introduction, there are ongoing efforts to standardise additional ECC algorithms for DNSSEC [10] and we intend to monitor adoption of these as well. Furthermore, we plan to study the complex 'algorithm rollover' discussed above. We will both experiment with such rollovers as well as observe if operators actually put them into practice, and whether or not this is done correctly.

Acknowledgments – this work was supported by the EU-FP7 FLAMINGO Network of Excellence Project (318488) and by SURF, the Netherlands collaborative organisation for ICT in higher education and research institutes. The research leading to these results was made possible by OpenINTEL[3], a joint project of SURFnet, the University of Twente and SIDN. The authors would like to thank the anonymous reviewers for their valuable input to this work.

REFERENCES

[1] D. Kaminsky, “Black Ops 2008: It’s the End of the Cache As We Know It,” in *Black Hat USA*, 2008. [Online]. Available: http://www.slideshare.net/dakami/dmk-bo2-k8

[2] R. van Rijswijk-Deij, A. Sperotto, and A. Pras, “DNSSEC and its potential for DDoS attacks,” in *Proceedings of ACM IMC 2014*. Vancouver, BC, Canada: ACM Press, 2014.

[3] Akamai, “Security Bulletin: DNSSEC Amplification DDoS,” Akamai, Tech. Rep., 2016. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/dnssec-amplification-ddos-security-bulletin.pdf

[4] E. Barker and Q. Dang, “Recommendation for Key Management - Part 3: Application-Specific Key Management Guidance (rev. 1),” *NIST SP 800-57*, 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

[5] N. Smart, “ECRYPT II Yearly Report on Algorithms and Keysizes 2011-2012,” European Commission, Tech. Rep., 2012. [Online]. Available: http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf

[6] R. van Rijswijk-Deij, A. Sperotto, and A. Pras, “Making the Case for Elliptic Curves in DNSSEC,” *ACM Computer Communication Review (CCR)*, vol. 45, no. 5, 2015.

[7] R. van Rijswijk-Deij, K. Hageman, A. Sperotto, and A. Pras, “The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation,” *To appear in IEEE/ACM Transactions on Networking*, 2016.

[8] P. Hoffman and W. Wijngaards, “RFC6605 - Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC,” 2012. [Online]. Available: http://tools.ietf.org/html/rfc6605

[9] CloudFlare, “Announcing Universal DNSSEC: Secure DNS for Every Domain.” [Online]. Available: https://blog.cloudflare.com/introducing-universal-dnssec/

[10] O. Surý and R. Edmonds, “(draft) EdDSA for DNSSEC,” 2016. [Online]. Available: https://tools.ietf.org/html/draft-ietf-curdle-dnskey-eddsa-00

[11] H. Yang, E. Osterweil, D. Massey, S. Lu, and L. Zhang, “Deploying cryptography in internet-scale systems: A case study on DNSSEC,” *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 656–669, 2011.

[12] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, “A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 7, 2016.

[13] NIST, “Estimating USG IPv6 and DNSSEC External Service Deployment Status.” [Online]. Available: http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov

[14] W. Kumari, Ó. Guðmundsson, and G. Barwood, “RFC 7344 - Automating DNSSEC Delegation Trust Maintenance,” 2014. [Online]. Available: https://tools.ietf.org/html/rfc7344

[15] J. Latour, Ó. Guðmundsson, P. Wouters, and M. Pounsett, “(draft) Third Party DNS operator to Registrars/Registries Protocol,” Tech. Rep., 2016. [Online]. Available: https://tools.ietf.org/html/draft-ietf-regext-dnsoperator-to-rrr-protocol-00

[16] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, “Measuring the Adoption of DDoS Protection Services,” in *To appear in Proceedings of ACM IMC 2016*. Santa Monica, CA, USA: ACM Press, 2016.

[17] P. Lexis, “PowerDNS Authoritative Server 4.0.0 Released,” 2016. [Online]. Available: https://blog.powerdns.com/2016/07/11/powerdns-authoritative-server-4-0-0-released/

[18] G. Huston and G. Michaelson, “ECDSA P-256 Support in DNSSEC-Validation Resolvers,” ICANN DNSSEC Workshop, Marrakech, Morocco, Tech. Rep., 2016. [Online]. Available: https://meetings.icann.org/en/marrakech55/schedule/wed-dnssec/presentation-dnssec-validating-resolvers-09mar16-en.pdf

[19] D. York, O. Surý, P. Wouters, and Ó. Guðmundsson, “(draft) Observations on Deploying New DNSSEC Cryptographic Algorithms,” 2016. [Online]. Available: https://tools.ietf.org/html/draft-york-dnsop-deploying-dnssec-crypto-algs-00

[20] O. Kolkman, W. Mekking, and R. Gieben, “RFC 6781 - DNSSEC Operational Practices, Version 2,” 2012. [Online]. Available: http://tools.ietf.org/html/rfc6781

[21] “OpenDNSSEC 2.0 Release Notes,” 2016. [Online]. Available: https://www.opendnssec.org/2016/07/opendnssec-2-0-0/

[22] “The Law of the Handicap of a Head Start,” 2016. [Online]. Available: https://en.wikipedia.org/wiki/Law_of_the_handicap_of_a_head_start