ECC support in DNS resolvers as seen by RIPE Atlas

Maciej Andzinski
NASK
maciej.andzinski@nask.pl

February 2016

Abstract

Whereas the elliptic curve cryptography (ECC) is sometimes considered to be a remedy for low DNSSEC adoption rate [1], there is also a lot of controversy around it. One of the main concerns is that DNSSEC-validating resolvers not always make use of ECC [1, 2, 3]. The goal of this study was to assess the extent of ECC support in DNS resolvers and to determine the impact of ECC deployment on domain name availability and security.

1 Introduction

At the time of writing this article, there were three ECC algorithms registered by IANA[1] for DNSKEY records. These were: number 12, 13 and 14, as presented in the table below.

Table 1: ECC algorithms registered by IANA for DNSKEY RRs

number	description
12	GOST R 34.10-2001
13	ECDSA Curve P-256 with SHA-256
14	ECDSA Curve P-384 with SHA-384

There were also four key digest algorithms[2] specified for DS records.

Table 2: Digest algorithms registered by IANA for DS RRs

number	description
1	SHA-1
2	SHA-256
3	GOST R 34.11-94
4	SHA-384

As the SHA-1 algorithm had been deprecated it was not considered in this study. In order to compare ECC and RSA support, DNSKEY algorithm number 8 (RSA/SHA-256)[3] was chosen. Ultimately, a set of four DNSKEY algorithms (8, 12, 13, 14) and a set of three DS digest algorithms (2, 3, 4) were selected to be the subject of analysis in this study. Thereby, there were twelve combinations of these two sets of values:

```
 (8,2)  (8,3)  (8,4)
(12,2) (12,3) (12,4)
(13,2) (13,3) (13,4)
(14,2) (14,3) (14,4)
```

A DNS zone was created for each combination above. It was signed using the appropriate DNSKEY algorithm and a specific DS record was generated and placed in the parent zone. Moreover, for each combination above a zone with bogus DNSSEC delegation was forged (key digest in DS record was malformed). For instance, for DNSKEY algorithm number 13 and DS digest algorithm number 2 there was a pair of zones:

```
key13-ds2-nsec3.lab.dnssec.pl.
key13-ds2-nsec3-bogus.lab.dnssec.pl.
```

Such a pair of zones existed for each of the twelve combinations above, thus there were twenty four unique domain names.

Once the DNS zones had been configured, the next step was to force as many recursive resolvers as possible to query for the considered domain names. For this purpose advantage of the RIPE Atlas system[4] was taken. Each RIPE Atlas probe with `system-ipv4-works` and `system-resolves-a-correctly` tags was employed to query its local resolver(s) for each of the twenty four domain names. For example, for DNSKEY algorithm number 13 and DS digest algorithm number 2 two DNS queries were issued:

```
test.key13-ds2-nsec3.lab.dnssec.pl.  IN TXT ?
test.key13-ds2-nsec3-bogus.lab.dnssec.pl.  IN TXT ?
```

For non-bogus DNSSEC delegation an answer was classified as correct if it contained a TXT record with "hello" text. For bogus DNSSEC delegation the SERVFAIL RCODE was also allowed. To determine whether a DNS resolver was DNSSEC-validating and supported a particular type of cryptography, the DO (*"DNSSEC OK"*) bit was set a in DNS query. A DNSSEC-validating resolver was expected to set AD (*"authenticated data"*) bit in an answer to such a query. Furthermore, it was supposed to answer with SERVFAIL RCODE when asked for a domain name with a bogus delegation.

[1] http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

[2] http://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml

[3] It was the most common non-deprecated algorithm [4]. 2048-bit KSK and 1024-bit ZSK were used.

[4] https://atlas.ripe.net/

2 Results

The data for analysis were collected at the end of December 2015 and in January 2016. The RIPE Atlas system yielded results from 8316 probes distributed over 3085 autonomous systems and 175 countries.

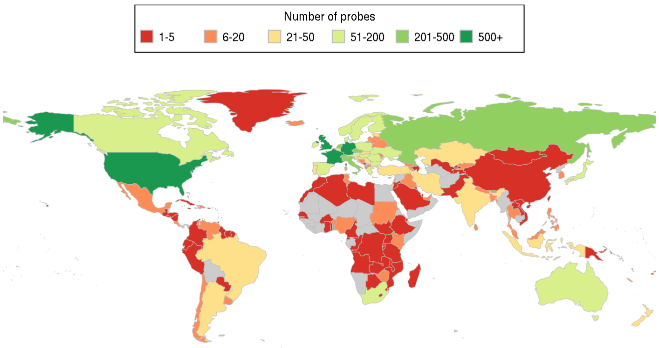

Figure 1: Distribution of RIPE Atlas probes involved in the measurements.

The total number of resolvers configured on the probes was 14501. 13744 (95%) of them were classified as working[5]. Each probe had up to 3 resolvers configured, but in most cases only one was working.

Table 3: Number of working resolvers configured on a probe

working resolvers	% of probes[6]
one	42.6%
two	40.4%
three	17.0%

Out of all working resolvers, 1370 (10%) were using IPv6 and 12374 (90%) were using IPv4. In the latter group the number of loop-back or private IP addresses[7] was 4417 (36%). The most popular resolver IP addresses were presented in Table 4.

Table 4: Top 10 resolver IP addresses

	IP address	count	% of total
1	8.8.8.8	1540	11.2 %
2	192.168.1.1	979	7.1 %
3	8.8.4.4	599	4.4 %
4	192.168.0.1	316	2.3 %
5	2001:4860:4860::8888	301	2.2 %
6	192.168.1.254	220	1.6 %
7	127.0.0.1	147	1.1 %
8	192.168.2.1	141	1.0 %
9	208.67.222.222	116	0.8 %
10	208.67.220.220	96	0.7 %

Google public DNS service[8] (IP addresses: 8.8.8.8, 8.8.4.4, 2001:4860:4860::8888 and 2001:4860:4860::8844) was far more popular than any other open DNS service. Its share constituted 24.7% of the total number of IPv6 resolvers and 17.2% of IPv4 resolvers. Such popularity significantly influenced the results.

It should be noted that IP address was not the attribute that indicated the resolver's uniqueness. Even if the same resolver IP address (for instance 8.8.8.8) was configured on many probes, all results were treated as if they came from individual sources. Such approach was adopted because the goal of this study was to assess the support for DNSSEC algorithms "as seen" from user perspective, not to investigate the behaviour of distinct resolvers. Furthermore, the IP address-based distinction was not reasonable due to the large number of resolvers with loop-back/private IP address.

2.1 ECC and RSA support comparison

Comparison of answers for different combinations of DS and DNSKEY algorithms was presented in Figure 2.

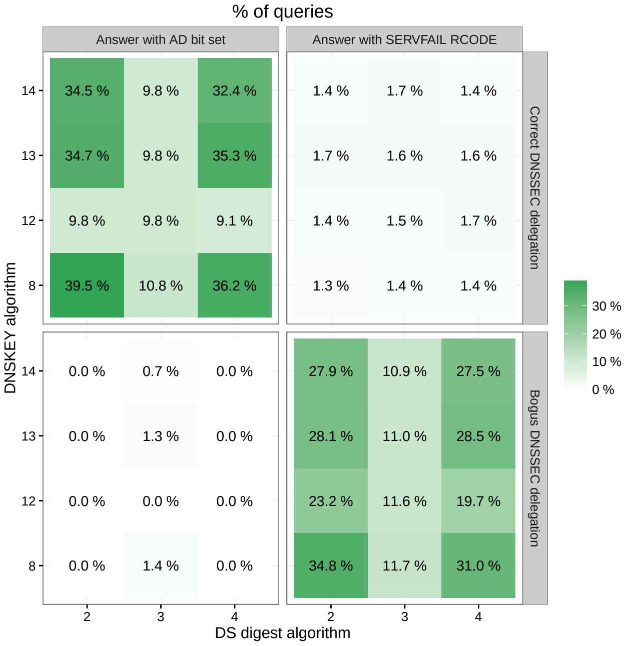

Figure 2: Answer statistics in relation to zone's DNSSEC delegation for various combinations of DS and DNSKEY algorithms.

Correct DNSSEC delegation

About 39.5% of resolvers answered with AD bit set for a query for a domain name secured using RSA cryptography. This value was slightly lower in case of ECDSA keys used with SHA-256/SHA-384 DS digest (34%-35%), but significantly decreased in the GOST-only case (9%-10%).

Whereas the difference between SHA-256 and SHA-384 support was minor (for all considered DNSKEY algorithms it was 29.6% and 28.3%, respectively), the GOST R 34.11-94 DS digest algorithm was much less frequently supported (10%).

Regardless of the algorithm, there was an almost constant overhead (about 1.5%) of SERVFAIL answers. However, the lowest value was observed in the RSA-only scenario, this issue was described in greater detail in Section 2.2.

[5] A resolver was classified as working if it had received a correct answer for at least one query in each of the two scenarios (correct/bogus DNSSEC delegation).

[6] Only probes which had at least one working resolver were taken into consideration.

[7] IPv4 loop-back: 127.0.0.0/8, IPv4 private addresses: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 (see RFC1918 [6]).

[8] `https://developers.google.com/speed/public-dns/`

Bogus DNSSEC delegation

The results were expected to be approximate to those for correct DNSSEC delegation, however some differences were observed.

One of the findings was that for some zones with bogus DNSSEC delegation certain resolvers returned answers with AD bit set (see Figure 2: lower left area). Another unusual observation was related to increased SERVFAIL answer rate for bogus DNSSEC delegation (comparing to the number of the answers with AD bit for correct DNSSEC delegation) when DNSKEY algorithm number 12 and DS digest algorithms number 2 or 4 were used. In-depth analysis showed that these curious phenomena concerned Google public DNS servers which, under certain circumstances, demonstrated a peculiar behaviour. This issue was discussed in more detail in Section 2.3.

IPv4 vs IPv6

In order to asses the difference in DNSSEC support on IPv4 and IPv6 resolvers, the answers for queries for domain names with correct DNSSEC delegation were studied. It was noticeable that the DNSSEC support rate was considerably higher in IPv6 resolvers (by 98% for ECC GOST algorithm, by 75% for ECDSA and by 67% for RSA). Furthermore, in these resolvers the differences in support rates of various algorithms were smaller. The comparison of answers from IPv4 and IPv6 resolvers was presented in Figure 3.

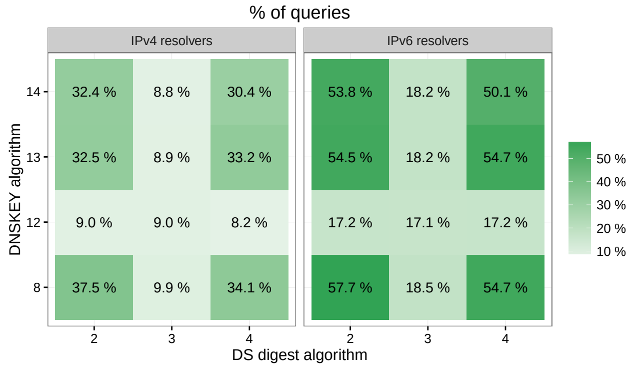

Figure 3: Answers with AD bit set in relation to resolver address family for various combinations of DS and DNSKEY algorithms.

Resolvers' behaviour comparison

Properly functioning DNSSEC-validating resolver was expected to answer with AD bit set for a query for a domain name with correct DNSSEC delegation and with a SERVFAIL RCODE in case of a bogus DNSSEC delegation. Resolvers' behaviour in these two scenarios was investigated.

As remarked in Section 2, each working resolver configured on a probe was treated as a unique data source, regardless of its IP address.

As illustrated in Figure 4, the majority of resolvers did not perform DNSSEC validation at all. The most frequently supported DNSKEY algorithm was RSA/SHA-256 along with SHA-256 as DS digest algorithm (30.9%).

The curious observation was that for the combinations of RSA or ECDSA DNSKEY algorithms (number 8, 13, 14) and SHA-256 or SHA-386 DS digest algorithms (number 2, 4) some resolvers did not perform DNSSEC validation for a domain name with bogus DNSSEC delegation, while the validation took place for correct DNSSEC delegation. Further investigation revealed that, again, it was an issue with Google public DNS (more details in Section 2.3).

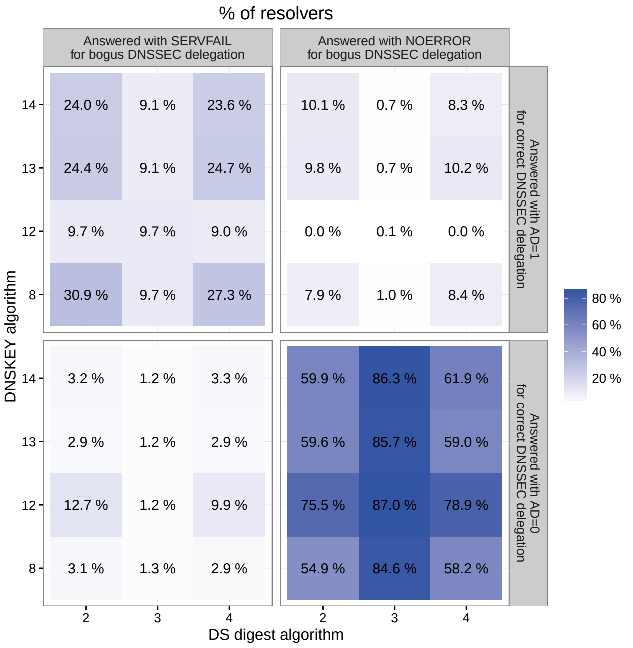

Figure 4: Resolvers' behaviour for various combinations of DS and DNSKEY algorithms.

2.2 ECC impact on domain name availability

The answers for queries for domain names with correct DNSSEC delegation were investigated in order to determine whether any correlations between the DS/DNSKEY algorithms and domain name availability existed. The percentages of correct answers[9] for various combinations of DS and DNSKEY algorithms were presented in Figure 5.

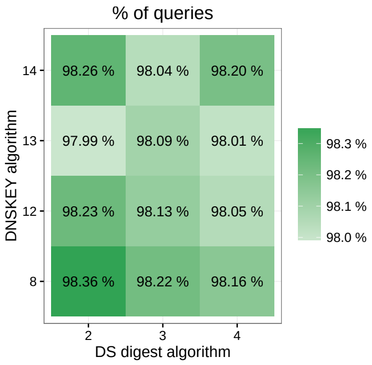

Figure 5: Correct answers for various combinations of DS and DNSKEY algorithms.

[9] The definition of "correct answer" was given in Section 1

Very slight differences were observed, however, it was noticeable that the highest answer rate (98.36%) was for the combination of DNSKEY algorithm number 8 and DS digest algorithm number 2, i.e. for very common RSA-only scenario. Moreover, as presented in Figure 6, for such a combination of algorithms also the lowest SERVFAIL answer rate was observed (1.27 %).

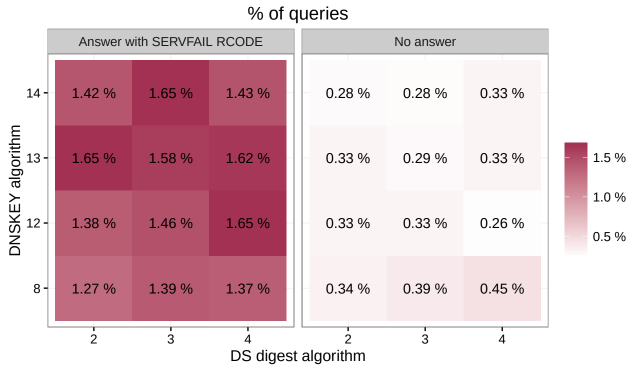

Figure 6: Unanswered queries and SERVFAIL answers for various combinations of DS and DNSKEY algorithms.

An interesting finding was that for RSA algorithms a slightly higher number of unanswered queries was noticed. Such an observation could have led to conclusion that a correlation between the DNS message size (much bigger in case of RSA) and the packet loss rate existed. Nevertheless, it should be taken into account that the parent zones (`.`, `pl.`,`dnssec.pl.`, `lab.dnssec.pl.`) were secured using the RSA cryptography (see Section 4.2), and thus for ECC-secured zones, the domain name resolution process also involved a transmission of large DNS packets.

2.3 Google public DNS issues

The study revealed several cases of unusual behaviour of Google public DNS servers. Because of the popularity of this service and its influence on the results, it was considered appropriate to discuss the encountered issues.

First observation was that under certain circumstances Google public DNS servers had answered with AD bit set for bogus DNSSEC delegation (see Figure 2). This phenomenon concerned only zones which were using DNSKEY algorithms number 8, 13 or 14 and DS digest algorithm number 3. The problem occurred for about 4% of queries for such bogus zones.

Another issue concerned unusual DNSSEC validation outcome when an unsupported DNSKEY algorithm[10] was used to sign the zone. As it was presented in Figure 2, for DNSKEY algorithm number 12 and DS digest algorithms number 2 and 4 there were many SERVFAIL answers for bogus DNSSEC delegation (about twice as many as the answers with AD bit set for correct DNSSEC delegation). This anomaly concerned Google public DNS servers which seemed to verify the key digest even when the key algorithm specified in DS RR was unsupported. Of course, it was desired to get a SERVFAIL answer for bogus DNSSEC delegation, however, a DNS resolver was also expected to abstain from DNSSEC validation when encountered an unsupported DNSKEY algorithm. According to RFC4035 [5], Section 5.2: *"If the resolver does not support any of the algorithms listed in an authenticated DS RRset, then the resolver will not be able to verify the authentication path to the child zone. In this case, the resolver SHOULD treat the child zone as if it were unsigned."* As the above RFC quote contained *"SHOULD"* not *"MUST"*, the recommendations were not actually violated, however, the Google servers demonstrated a behaviour which was uncommon among other DNS resolvers.

Lastly, it was observed that Google servers did not perform DNSSEC validation for about 25% of queries for domain names with bogus DNSSSEC delegation. Such queries resulted in answers with NOERROR RCODE, while it should have been SERVFAIL. This anomaly was visible in Figures 2 and 4.

Google had been advised of these issues, but it remained unknown whether any steps were subsequently taken to modify DNSSEC validation processes.

3 Conclusions

It was demonstrated that elliptic curve cryptography was not as widely supported as RSA. However, the differences between the RSA and ECDSA support rates were not very big. In contrast, the resolvers making use of Russian GOST algorithm were not too common. A similar observation was made for DS digest algorithms. SHA-384 was, unlike GOST R 34.11-94, almost as frequently supported as SHA-256. The results led to conclusion that the transition from RSA to ECC would narrow the group of the Internet users who benefit from DNSSEC. Nevertheless, for ECDSA algorithms this loss would not be very big. It should also be mentioned that, as claimed in [1], ECC might eliminate many issues which discourage people from using DNSSEC. Hence, in the long term, ECC deployment could increase DNSSEC adoption rate and thereby broaden the group of the Internet users who benefit from secure DNS.

The study showed that DNSSEC was more popular in IPv6 Internet and that the less common algorithms were more frequently supported by IPv6 resolvers.

It was not proved that ECC deployment had an impact on domain name availability but such possibility was not ruled out. It was demonstrated that in the RSA-only scenario domain name availability was slightly higher and also a slightly lower SERVFAIL answer rate was observed. This issue could have been investigated more thoroughly if more data had been collected, but such a far-reaching study was out of scope of this paper.

The fact that RIPE Atlas probes were not evenly distributed over the Internet[11] should be taken into consid-

[10] No clear information about algorithm support had been found, however relying on the results of this study it was justified to assume that DNSKEY algorithm 12 was not supported by Google public DNS.

[11] `https://atlas.ripe.net/results/maps/network-coverage/`

eration. As shown in Figure 1, European countries along with US and Canada were the most popular locations.

4 Remarks

4.1 Measurement parameters

Default timeout for a DNS query sent by RIPE Atlas probe was 5 seconds. All the measurements were created with `RETRY` parameter[12] set to value 2.

4.2 DNSSEC in the parent zones

In order to validate a DNSSEC-signed domain name, all the DS digest/DNSKEY algorithms within the chain of trust had to be supported in a DNS resolver. DNSSEC configuration of the parent zones was presented in Table 5.

Table 5: DNSSEC configuration of the parent zones

zone	DS digest / DNSKEY algorithm number	KSK/ZSK size (bits)
.	-/8	2048/1024
pl.	2/8	2048/1024
dnssec.pl.	2/10	4096/2048
lab.dnssec.pl.	2/8	2048/1024

5 Acknowledgements

The author thanks Michał Kępień and Piotr Studziński-Raczyński for their feedback.

References

[1] R. van Rijswijk-Deij, Sperotto A., Pras A.: Making the Case fo Elliptic Curves in DNSSEC[13], *ACM SIGCOMM Computer Communication Review*, volume 45, number 5, pages 14-19, October 2015

[2] Guðmundsson Ó.: ECDSA is your friend[14], *RIPE 70*, May 2015

[3] Huston G., Michaelson G.: ECDSA and DNSSEC [15], *Potaroo blog, The ISP Column* , October 2014

[4] Lewis E.: DNSSEC Cryptographic Demographics – One Level Down[16], *CENTR Jamboree 2015*, June 2015

[5] Arends R., Austein R., Larson M., Massey D., Rose S.: RFC4035 (Protocol Modifications for the DNS Security Extensions)[17], *IETF Network Working Group*, March 2005

[6] Rekhter Y., Moskowitz B., Karrenberg D., G. J. de Groot: RFC1918 (Address Allocation for Private Internets)[18], *IETF Network Working Group*, February 1996

[12] https://atlas.ripe.net/docs/measurement-creation-api/

[13] http://www.sigcomm.org/sites/default/files/ccr/papers/2015/October/0000000-0000002.pdf

[14] https://ripe70.ripe.net/wp-content/uploads/presentations/85-Alg-13-support.pdf

[15] http://www.potaroo.net/ispcol/2014-10/ecdsa.pdf

[16] https://centr.org/system/files/agenda/attachment/rd7-lewis-dnssec_cryptographic_demographics-20150603.pdf

[17] https://www.ietf.org/rfc/rfc4035.txt

[18] https://tools.ietf.org/rfc/rfc1918.txt