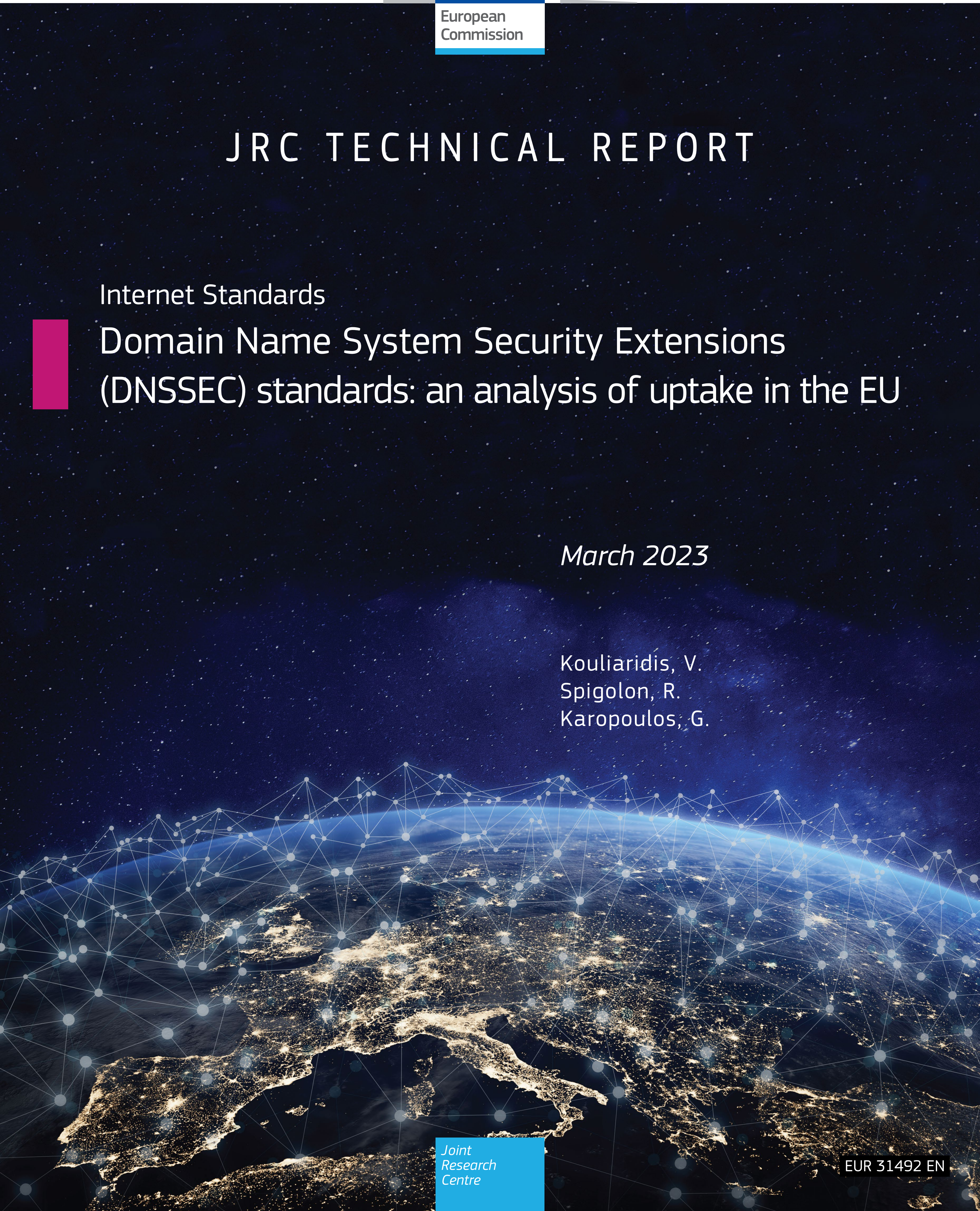
ISSN: 1831-9424

European Commission



JRC TECHNICAL REPORT

Internet Standards

Domain Name System Security Extensions (DNSSEC) standards: an analysis of uptake in the EU

March 2023

Kouliaridis, V.
Spigolon, R.
Karopoulos, G.

Joint Research Centre

EUR 31492 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission’s science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information
Name: Ignacio SANCHEZ
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 581, 21027 Ispra (VA), Italy
Email: Ignacio.SANCHEZ@ec.europa.eu
Tel.: +39 033278-5998

EU Science Hub
https://joint-research-centre.ec.europa.eu

JRC133218

EUR 31492 EN

PDF ISBN 978-92-68-03005-9 ISSN 1831-9424 doi:10.2760/565767 KJ-NA-31-492-EN-N

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: Kouliaridis, V., Spigolon, R. and Karopoulos, G., *Domain Name System Security Extensions (DNSSEC) standards: an analysis of uptake in the EU, March 2023*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/565767, JRC133218.

Contents

Acknowledgements

The authors would like to acknowledge Ms. Gillian O'NEILL (JRC) for reviewing parts of this report, and Mr. Massimiliano GUSMINI (JRC) for creating the front cover.

Abstract

A high level of adoption of Domain Name System Security Extensions (DNSSEC) is essential to protect the integrity of the Domain Name System (DNS) Internet infrastructure to ensure the interoperability and security of the global cyberspace. This report provides an analysis of the level of adoption of DNSSEC in Q1 2023 across EU Member States and globally. The report also presents an analysis of the usage of DNS resolvers in the EU and globally. Overall, the average DNSSEC validation rate in the EU is still low (46.3%), but is superior to the global one (31.4%).

Executive summary

In the joint Communication "The EU's Cybersecurity Strategy for the Digital Decade" published on 16/12/2020, the European Commission (EC) announced a set of actions to maintain an open, secure, and resilient global Internet. One of these actions focuses on identifying, monitoring and fostering the uptake of key Internet communication and security standards, as well as best practices for Domain Name System (DNS), routing, browsing and e-mail security. Following up on this, the EC is exploring mechanisms to systematically monitor the evolution of secure DNS deployment for identifying gaps and barriers for its adoption, and evaluate the need for regulatory measures to promote its uptake.

The DNS service is well known to provide the mapping of domain names to their corresponding IP addresses. Less known is the key role that DNS plays supporting the operation of other key Internet security standards, particularly security standards used in email and web communications. The wide deployment of DNSSEC is essential for protecting the integrity of the DNS service, which is crucial to ensure the effectiveness of other key Internet security standards and increase the resilience of the Internet.

This report provides an analysis of DNSSEC validation rates in Q1 2023 across EU Member States (MSs) and globally. Moreover, an analysis of the usage of DNS resolvers is provided, distinguishing between resolvers belonging to the Internet Service Provider of the end–user and open resolvers. This report also includes our own analysis of DNSSEC adoption rates of the top domains across EU MSs. The analysis is based on third–party publicly available data. Additionally, this report also includes our own results on the DNSSEC support of the top domains in the EU, i.e., the Top-1M domains of the Tranco list.

In the EU MSs, the current results for Q1 2023 show a similar trend to Q3 2022 with a medium degree of users validating DNSSEC-signed responses in the EU MSs (around 46%), which is slightly increased (+3 percentage points) since Q3 2022. A closer look at each country individually, reveals that the validation rates are not homogeneous as shown in Figure 1, ranging approximately from 4 to 95%. Czech Republic, Denmark, Finland, Luxembourg and Sweden lead the way with rates above 70%, followed by Belgium, Cyprus, Estonia, Germany, Netherlands, Poland, and Slovenia with percentages between 50 and 70%. On the other end, Hungary and Romania have adoption rates lower than 10%, whereas Austria, Croatia, Greece, Italy, Slovakia, and Spain are between 10 and 30%. The remaining MSs, namely Bulgaria, France, Ireland, Latvia, Lithuania, Malta, and Portugal have rates between 30 and 50%.

Globally, the average DNSSEC validation rate in Q1 2023 is significantly lower (31.4%) than the EU average, showing an increase of around 1% since Q3 2022. Overall this shows that, the global average adoption of DNSSEC lags behind compared to the EU, and is developing faster in the EU.

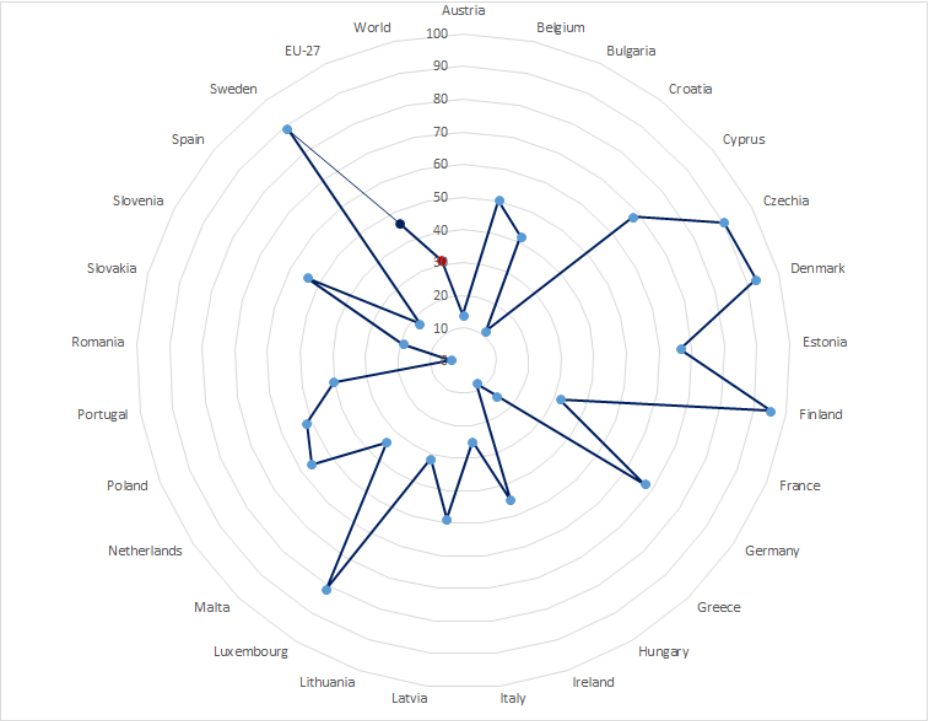


Figure 1: DNSSEC validation rate per MS. The EU average is marked with a blue dot, whereas global average is marked with a red dot.

1 Introduction

As described in the Joint Communication 'The EU's Cybersecurity Strategy for the Digital Decade' published on Dec. 2020 (European Commission, 2020), the European Commission (EC) announced a set of actions to maintain an open, secure, and resilient Internet. One of the actions of this strategy concentrates on identifying, monitoring and promoting the adoption of key Internet standards and best practices for Domain Name System (DNS), routing, browsing, and e-mail security. Moreover, the recent EU Strategy on Standardisation states (European Commission, 2022): *"The Commission will monitor the deployment of internationally agreed key internet standards and make this data and related good practices available on an EU internet standards monitoring website. [...] The Commission will: [...] Foster the development and deployment of international standards for a free, open, accessible and secure global internet and establish an EU internet standards monitoring website."*

As a product of the aforementioned initiatives, this report concentrates on DNS and more in particular DNS Security Extensions (DNSSEC). As the base DNS service does not provide any security mechanisms its integrity is not warranted; moreover, other security-focused standards, such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC), depend on the secure operation of DNS to provide their services. To that end, DNSSEC (Arends et al., 2005,Hoffman, 2010,Weiler and Blacka, 2013) comprise a suite of Internet Engineering Task Force (IETF) specifications for ensuring that DNS responses are valid, increasing the level of trust. For this reason, it is considered that the wide deployment of DNSSEC contributes to a safer, more secure and resilient Internet.

This report is part of the Internet Standards series of reports aiming at monitoring the adoption of key Internet standards in the EU Member States. This periodic review of key Internet standards is performed every six months and the first round of reports was launched in March 2022. An overview of the results is also available in the associated *EU Internet Standards Deployment Monitoring Website* (European Commission, n.d.). The present report focuses on the adoption of DNSSEC in the European Union (EU) and globally. The first report concerned Q1 2022 (Kampourakis and Karopoulos, 2022) whereas this one presents results for Q1 2023. Contrary to the previous version, this report is based both on third–party open data and our own measurements and presents results and analysis of the DNSSEC validation rate of DNS requests. The key observations from Q3 2022 were that in the EU there is a medium DNSSEC validation rate, which is, however, significantly higher than the global rate. Moreover, while overall there is a slowly increasing trend, the rates vary significantly from Member State (MS) to MS. Current measurements for Q1 2023 report similar figures, showing a slight increase in DNSSEC validation in the EU that is higher to the one observed globally.

The rest of the report is organised as follows. Section 2 describes the data sources and methodology used in each source to collect their measurements. Section 3 presents the data analysis on the current DNSSEC validation rate and use of DNS resolvers worldwide. Finally, Section 4 concludes the report.

2 Data sources and methodology

The data used in this report come from the sources shown in Table 1. The data freeze date is set to 21/02/2023. Overall, the remarks and recommendations of the previous report (Kambourakis et al., 2022) still apply here given the minor differences in the deployment results. The provided results focus is on the DNSSEC validation rate by resolvers and pertain to (i) the global rate of DNSSEC uptake, (ii) the DNSSEC deployment status across EU, and (iii) the DNSSEC deployment status across a set of selected countries worldwide. Regarding encrypted DNS, i.e., DNS queries over HTTPS (DoH), DNS over TLS (DoT), and DNS over QUIC (DoQ), no updated results are provided, given that there are no sources providing periodical adoption statistics and no new relevant studies have been published since the previous measurement period.

This round of reports also includes our results on the support rate of DNSSEC on the Tranco Top 1M domains, only for EU MSs. Specifically, we mapped each domain to an EU MS based on their TLD and checked the DNSSEC support of each domain.

Table 1: Data sources used in the context of this report.

Source	**Short description**
APNIC I (APNIC, n.d.c, APNIC, n.d.a)	DNSSEC 30-day average validation rates by region, sub-region, and country worldwide
APNIC II (APNIC, n.d.b)	Frequently updated statistics about the percentages of the top utilized DNS resolvers by region, sub-region, and country worldwide.
Our results	Our measurements on the support rate of DNSSEC on the Tranco Top 1M domains

3 Data collection and analysis

Overall, the collected results for Q1 2023 show a slight increase in DNSSEC validation rate in the EU as well as globally, which is steady in the long–term when observing 1-year long data but with ups and downs in shorter periods. Having said that, the remarks and recommendations of the previous report (Kambourakis et al., 2022) still apply here given the minor differences in the results.

In Figures 2 and 3 we can observe the trends related to the DNSSEC validation rate globally and the growth of DS record sets over time, based on APNIC data (APNIC, n.d.a). As observed, in both cases, the trend is following the path already set in the previous version of this report, with global DNSSEC validation rate at around 31%, which is slightly higher (+1 percentage points) than the previous measurement period).

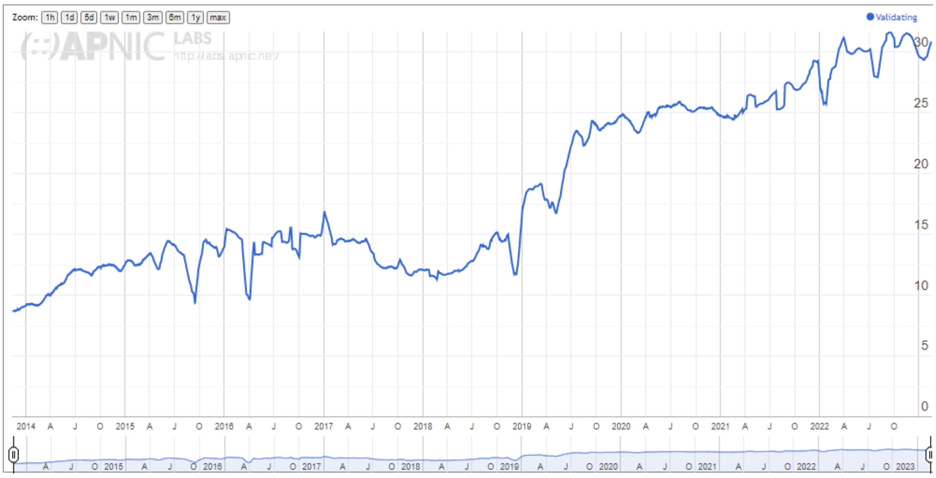


Figure 2: A projection of DNSSEC validation rate for world (APNIC, n.d.c)

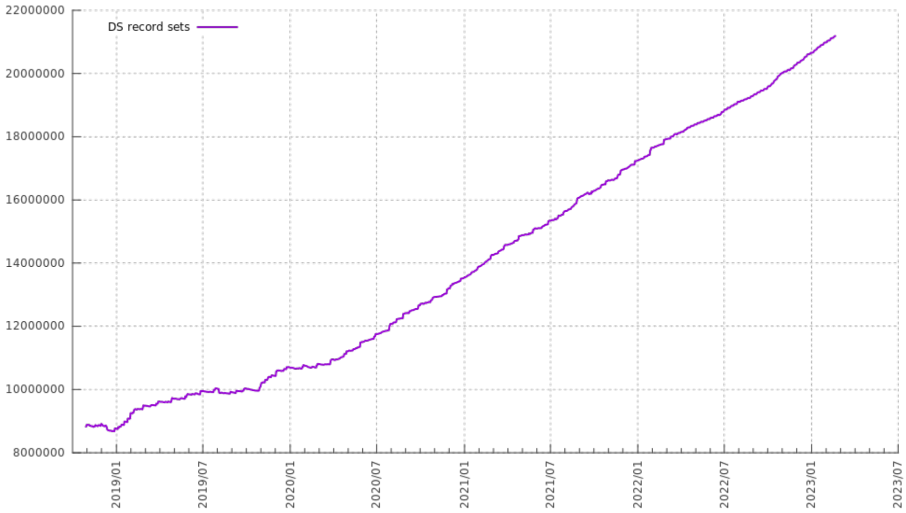


Figure 3: Growth of DS record sets over time, i.e., the number of signed zones Internet-wide (15/06/2022) (DNSSEC-Tools, n.d.)

The specific DNS validation rate indicator for each EU MS and for a selection of non-EU countries is reported in Table 2.

It is observed that also the EU average had an increase, which is higher than the world average (+3.1 percentage points). Looking closely at each MS, and rebuilding the classification table used in Section 3 of the previous report (Kambourakis et al., 2022), we can see in Table 3 that several countries passed to a higher category based on the achieved improvement: Croatia, Bulgaria, Ireland, Lithuania, Malta, Poland,

Table 2: DNSSEC validation rate in EU-27 Member States and a selection of non EU-27 countries (%)

MS	%	Country	%
Austria	14.02	Argentina	35.40
Belgium	50.18	Australia	26.74
Bulgaria	41.98	Bangladesh	73.87
Croatia	11.35	Belarus	30.10
Cyprus	68.00	Brazil	50.72
Czech Republic	90.23	Canada	15.33
Denmark	92.79	China	0.03
Estonia	66.49	India	59.54
Finland	95.14	Indonesia	16.11
France	31.83	Iran	88.11
Germany	67.09	Israel	42.21
Greece	14.81	Japan	15.77
Hungary	7.98	Kazakhstan	31.62
Ireland	44.80	Malaysia	20.19
Italy	24.74	Norway	90.21
Latvia	48.56	Russian Federation	33.18
Lithuania	31.50	Saudi Arabia	95.52
Luxembourg	81.33	Singapore	62.04
Malta	34.19	South Africa	43.82
Netherlands	56.21	South Korea	3.35
Poland	51.60	Switzerland	68.58
Portugal	40.30	Taiwan	5.85
Romania	3.90	Thailand	11.64
Slovakia	19.24	Turkey	32.39
Slovenia	54.15	Ukraine	39.98
Spain	17.65	United Kingdom	9.64
Sweden	89.29	United States	35.44
Average EU-27	**46.30**	Average	**38.70**
StDev EU-27	**27.90**	StDev	**26.78**
Average World (APNIC, n.d.c)	**31.42**	–	–

Table 3: Categorization of MSs based on DNSSEC validation score

Percentage	MSs
≤ 10	Hungary, Romania
$> 10 \ \& \leq 30$	Austria, Croatia, Greece, Italy, Slovakia, Spain
$> 30 \ \& \leq 50$	Bulgaria, France, Ireland, Latvia, Lithuania, Malta, Portugal
$> 50 \ \& \leq 70$	Belgium, Cyprus, Estonia, Germany, Netherlands, Poland, Slovenia
$> 70 \ \& \leq 95$	Czech Republic, Denmark, Finland, Luxembourg, Sweden

Slovenia; the highest improvement is achieved by Malta (+20.65 percentage points). On the other hand, France has a decreased rate of around 22 percentage points, with respect to the last measurement period. In our opinion, this is caused by an increase of around +100% in the sample size provided by APNIC (APNIC, n.d.a).

Regarding the 27 non-EU countries taken as reference, a general decrease of DNSSEC validation score can be observed. Specifically, 16 countries show a decreased validaction score, namely Australia, Belarus, Brazil, Canada, China, Israel, Japan, Malaysia, Russia, Singapore, South Korea, Taiwan, Turkey, Ukraine, United Kingdom, and United states. On the other hand, Iran, had an increase of around 70%

A graphical comparison of the DNSSEC validation rate within the EU is depicted in Figure 4, while Figure 5 shows how the EU stands vis-à-vis the selected third countries.

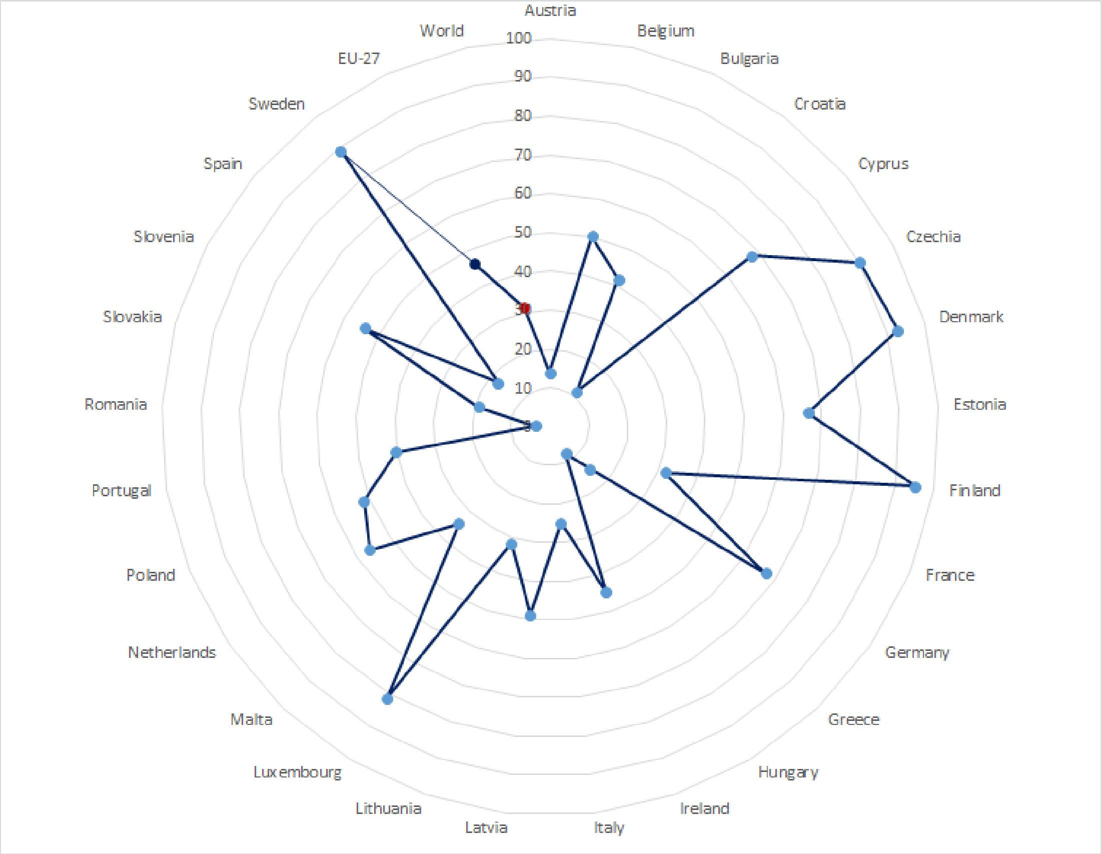


Figure 4: DNSSEC validation rate per MS. EU and world averages are shown by a larger dot.

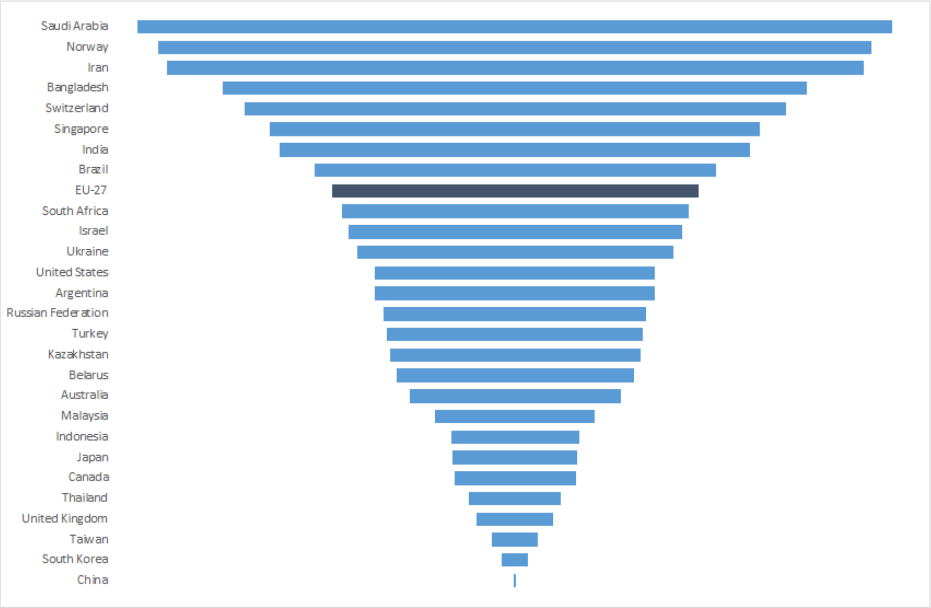


Figure 5: A funnel representation of DNSSEC validation rate per non-EU country. The EU average score resides at the top one-third of the funnel.

Table 4 Shows our results on DNSSEC support for EU MSs, on the Top-1M domains of the Tranco list. Consequently, the results on Table 4 concern the server-side adoption of DNSSEC, whereas APNIC's data refer to end–user adoption, i.e., users validating DNSSEC-signed responses. As shown in Table 4, Czech Republic, Denmark and Netherlands have the highest adoption rate ($>$ 45%), which also appear to have high DNSSEC validation rates in Table 3. Next is Sweden (31%), followed by Slovakia (29%), Estonia (19%), Belgium (16%), and Cyprus (12%). The rest 19 MSs have an adoption rate of $<$ 10%.

Table 5 shows the updated data regarding the utilisation of major DNS resolvers in the EU MSs. As in the last measurement period, the sum of the relative usage of DNS resolvers located in the same Autonomous System (AS) as the user, i.e., the Internet Service Provider (ISP) resolver (sameas), the Google open resolver at 8.8.8.8 & 8.8.4.4 (googlepdns), and Cloudflare's open DNS service at 1.1.1.1 & 1.0.0.1 (cloudflare), is very high, i.e., above 80%.

Moreover, a notable reduction of the employment of Google's DNS resolvers is noticed from the last measurement period (-4%), and a small reduction in the utilisation of Cloudflare's (-1.3%). Regarding the single countries, there is one highlight from France, Germany, and the Netherlands, where the percentage related to Google's DNS resolver has decreased by more than 13%.

Table 4: DNSSEC Support of the Top-1M domains (Our results)(%)

MS	%
Austria	3,99
Belgium	16,39
Bulgaria	5,23
Croatia	0,92
Cyprus	12,5
Czech Republic	49,73
Denmark	47,78
Estonia	19,21
Finland	9,47
France	9,67
Germany	3,60
Greece	1,99
Hungary	9,75
Ireland	1,27
Italy	1,52
Latvia	6,29
Lithuania	2,04
Luxembourg	8,69
Malta	0,00
Netherlands	45,42
Poland	8,49
Portugal	8,79
Romania	3,63
Slovakia	28,99
Slovenia	6,61
Spain	5,35
Sweden	31,36
Average EU-27	14,73
StDev EU-27	14,71

Table 5: Usage of resolvers (%) in EU: AS (ISPs) vs. the two most utilized open resolvers.

MS	**sameas**	**googledns**	**cloudflare**
Austria	73.421	6.564	0.074
Belgium	95.745	1.642	0.071
Bulgaria	59.455	10.549	2.135
Croatia	74.701	2.598	0.839
Cyprus	50.723	7.595	0.248
Czech Republic	73.421	6.564	0.074
Denmark	79.613	6.444	2.217
Estonia	92.321	2.779	1.599
Finland	89.706	5.094	2.45
France	85.010	3.382	1.796
Germany	88.783	5.537	2.914
Greece	68.619	3.448	1.186
Hungary	87.344	2.643	0.82
Ireland	85.534	5.116	1.867
Italy	91.452	4.041	0.898
Latvia	76.553	3.710	2.365
Lithuania	88.635	6.293	1.134
Luxembourg	86.156	6.292	2.797
Malta	30.460	4.600	1.251
Netherlands	42.500	5.506	3.237
Poland	72.481	6.435	2.075
Portugal	90.272	2.543	0.807
Romania	91.634	2.031	0.971
Slovakia	83.673	7.450	2.289
Slovenia	94.489	2.706	0.746
Spain	78.713	10.947	1.486
Sweden	90.370	3.421	0.469
Average EU-27	78.58	5.03	1.44
StDev EU-27	16.29	2.40	0.92
Average World	66.88	10.42	0.98

4 Conclusions

This report provides an up-to-date review of the DNSSEC validation rate in the EU and globally. The main outcomes of this study can be summarized as follows. Please note that, mainly due to the minor differences in the results of the present and the previous measurement periods, the observations described in the previous report (Kambourakis et al., 2022) still apply.

1. The global DNSSEC validation rate by resolvers presents a steady increase, especially since 2019. Based on Q1 2023 data, this score is approximately 31.4%. The increasing trend observed in Q3 2022 is similar in Q1 2023 but still develops at a slow pace.
2. The average DNSSEC validation rate in the EU is quite high, reaching 46.3%, hence being superior to the global average percentage by around 15% and to that of several other countries, including Japan, United Kingdom, United States, Russia, and China; The MSs individual scores are less fragmented, with the most populous groups of countries lying in the (30,70] range.
3. Compared to Q3 2022, in Q1 2023 it seems that the use of DNS resolvers as-a-service remained somewhat stable. In the EU, the use of the most popular open resolver (*googledns*) decreased by 4%, and *cloudflare* decreased by 1.3%. Globally, the use of *googledns* also decreased by 4% and that of *cloudflare* decreased by 1.35%.

References

Abley, J., Gudmundsson, O., Majkowski, M. and Hunt, E., 'RFC 8482: Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY', Tech. rep., IETF, 2019. URL https://tools.ietf.org/html/rfc8482.

AdGuard, 'AdGuard DNS-over-QUIC'. 2020. URL https://adguard.com/en/blog/dns-over-quic.html. Last visited 21/11/2021.

Adrichem, N. L. M., Blenn, N., Lúa, A. R., Wang, X., Wasif, M., Fatturrahman, F. and Kuipers, F. A., 'A measurement study of dnssec misconfigurations', *Security Informatics*, Vol. 4, No 1, 2015, pp. 1–14. .

Albright, S., Leach, P. J., Gu, Y., Goland, Y. Y. and Cai, T., 'Simple Service Discovery Protocol/1.0', Internet-Draft draft-cai-ssdp-v1-03, Internet Engineering Task Force, Nov. 1999. URL https://datatracker.ietf.org/doc/html/draft-cai-ssdp-v1-03. Work in Progress.

Alec Muffett, 'DoHoT: making practical use of DNS over HTTPS over Tor'. 2021. URL https://github.com/alecmuffett/dohot. Last visited 15/02/2022.

Anagnostopoulos, M., Georgios, K., Elisavet, K. and Stefanos, G., 'Dnssec vs. dnscurve: A side-by-side comparison"', In 'Situational Awareness in Computer Network Defense: Principles, Methods and Applications', IGI Global.

Anagnostopoulos, M., Kambourakis, G., Gritzalis, S. and Yau, D. K. Y., 'Never say never: Authoritative TLD nameserver-powered DNS amplification', In '2018 IEEE/IFIP Network Operations and Management Symposium, NOMS 2018, Taipei, Taiwan, April 23-27, 2018', IEEE, pp. 1–9. . URL https://doi.org/10.1109/NOMS.2018.8406224.

Anagnostopoulos, M., Kambourakis, G., Konstantinou, E. and Gritzalis, S. *DNSSEC vs. DNSCurve: A Side-by-Side Comparison*, IGI Global, 2012b. pp. 201–220.

Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G. and Gritzalis, S., 'DNS Amplification Attack Revisited', *Computers & Security*, Vol. 39, Part B, 2013a, pp. 475 – 485.

Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G. and Gritzalis, S., 'Dns amplification attack revisited', *Comput. Secur.*, Vol. 39, Nov. 2013b, p. 475–485. ISSN 0167-4048. . URL https://doi.org/10.1016/j.cose.2013.10.001.

APNIC, 'Opinion: Centralized DoH is bad for privacy, in 2019 and beyond'. 2019. URL https://blog.apnic.net/2019/10/03/opinion-centralized-doh-is-bad-for-privacy-in-2019-and-beyond/. Last visited 24/11/2021.

APNIC, 'DNSSEC Validation Rate by country'. n.d.a. URL https://stats.labs.apnic.net/dnssec. Last visited 25/10/2021.

APNIC, 'Use of DNS Resolvers for World'. n.d.b. URL https://stats.labs.apnic.net/rvrs/XA?hc=XA&hl=1&hs=0&ht=10&w=1&t=10&x2=1. Last visited 29/10/2021.

APNIC, 'Use of DNSSEC Validation for World'. n.d.c. URL https://stats.labs.apnic.net/dnssec/XA?hc=XA&hx=0&hv=1&hp=1&hr=1&w=30&p=0. Last visited 25/10/2021.

Apple, 'Enable encrypted DNS'. 2020. URL https://developer.apple.com/videos/play/wwdc2020/10047. Last visited 22/11/2021.

April King, 'Analysis of the Alexa Top 1M sites (April 2019)'. URL https://pokeinthe.io.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S., 'DNS Security Introduction and Requirements'. RFC 4033 (Proposed Standard), Mar. 2005. URL http://www.ietf.org/rfc/rfc4033.txt. Updated by RFCs 6014, 6840.

Belshe, M., Peon, R. and Thomson, M., 'Hypertext Transfer Protocol Version 2 (HTTP/2)'. RFC 7540, May 2015. . URL https://rfc-editor.org/rfc/rfc7540.txt.

CDNetworks, 'State of the Web Security, H1 2020'. URL https://www.cdnetworks.com.

Chung, T., van Rijswijk-Deij, R., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A. and Wilson, C., 'A longitudinal, end-to-end view of the DNSSEC ecosystem', In '26th USENIX Security Symposium (USENIX Security 17)', USENIX Association, Vancouver, BC. ISBN 978-1-931971-40-9, pp. 1307–1322. URL https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/chung.

Chung, T., van Rijswijk-Deij, R., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A. and Wilson, C., 'Understanding the role of registrars in dnssec deployment', In 'Proceedings of the 2017 Internet Measurement Conference', IMC '17. Association for Computing Machinery, New York, NY, USA. ISBN 9781450351188, p. 369–383. . URL https://doi.org/10.1145/3131365.3131373.

Consumer Reports, Electronic Frontier Foundation, and the National Consumers League, 'But see Letter from Consumer Reports, Electronic Frontier Foundation, and the National Consumers League to Senate and House Committee Chairmen and Ranking Members'. 2019. URL https://www.eff.org/files/2019/10/22/effcr_and_ncl_letter_on_doh_to_congress.pdf. Last visited 21/02/2022.

Crocker, D., Hansen, T. and Kucherawy, M., 'DomainKeys Identified Mail (DKIM) Signatures'. RFC 6376 (INTERNET STANDARD), Sep. 2011. URL http://www.ietf.org/rfc/rfc6376.txt.

Csikor, L., Singh, H., Kang, M. S. and Divakaran, D. M., 'Privacy of dns-over-https: Requiem for a dream?', In 'IEEE European Symposium on Security and Privacy, EuroS&P 2021, Vienna, Austria, September 6-10, 2021', IEEE, pp. 252–271. . URL https://doi.org/10.1109/EuroSP51992.2021.00026.

Darren Anstee, 'Disappearing DNS: DoT and DoH, Where one Letter Makes a Great Difference'. 2020. URL https://www.securitymagazine.com/articles/91674-disappearing-dns-dot-and-doh-where-one-letter-makes-a-great-difference. Last visited 23/11/2021.

Dickinson, J., Dickinson, S., Bellis, R., Mankin, A. and Wessels, D., 'DNS Transport over TCP - Implementation Requirements'. RFC 7766, Mar. 2016. . URL https://rfc-editor.org/rfc/rfc7766.txt.

Digineo, 'Public DNS Server List'. n.d. URL https://public-dns.info/. Last visited 28/10/2021.

DNSSEC-Tools, 'DNSSEC and DANE Deployment Statistics - DNSSEC deployment growth'. n.d. URL https://stats.dnssec-tools.org/. Last visited 25/10/2021.

Doan, T. V., Tsareva, I. and Bajpai, V., 'Measuring DNS over TLS from the edge: Adoption, reliability, and response times', In 'Passive and Active Measurement - 22nd International Conference, PAM 2021, Virtual Event, March 29 - April 1, 2021, Proceedings', , edited by O. Hohlfeld, A. Lutu, and D. Levin*Lecture Notes in Computer Science*, Vol. 12671. Springer, pp. 192–209. . URL https://doi.org/10.1007/978-3-030-72582-2_12.

Dukhovni, V. and Hardaker, W., 'The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance'. RFC 7671, Oct. 2015. . URL https://rfc-editor.org/rfc/rfc7671.txt.

Eastlake 3rd, D. E., 'Transport Layer Security (TLS) Extensions: Extension Definitions'. RFC 6066, Jan. 2011. . URL https://www.rfc-editor.org/info/rfc6066.

European Commission, 'Join(2020) 18 final. joint communication to the european parliament and the council - the eu's cybersecurity strategy for the digital decade'. 2020. URL https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&rid=5. Last visited 21/09/2021.

European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market – COM/2022/31 final'. 2022. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0031.

European Commission, 'EU Internet Standards Deployment Monitoring Website'. n.d. URL https://ec.europa.eu/internet-standards/index.html.

Executive office of the President, 'Memo-18-23'. URL https://www.whitehouse.gov/wp-content/uploads/2018/08/M-18-23.pdf. Last visited 19/11/2021.

Executive office of the President, ‘Memo M-08-23’. 2008. URL https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-23.pdf. Last visited 19/11/2021.

Executive office of the President, ‘Memo-18-23’. 2018. URL https://www.whitehouse.gov/wp-content/uploads/2018/08/M-18-23.pdf. Last visited 19/11/2021.

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S. and Levchenko, K., ‘Security by any other name: On the effectiveness of provider based email security’, In ‘Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security’, CCS’15. Association for Computing Machinery, New York, NY, USA. ISBN 9781450338325, p. 450–464. . URL https://doi.org/10.1145/2810103.2813607.

Friedl, S., Popov, A., Langley, A. and Emile, S., ‘Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension’. RFC 7301, Jul. 2014. . URL https://www.rfc-editor.org/info/rfc7301.

García, S., Hynek, K., Vekshin, D., Cejka, T. and Wasicek, A., ‘Large scale measurement on the adoption of encrypted DNS’, *CoRR*, Vol. abs/2107.04436, 2021. URL https://arxiv.org/abs/2107.04436.

Geoff Huston, ‘APNIC - DNSSEC validation revisited’. 2020. URL https://blog.apnic.net/2020/03/02/dnssec-validation-revisited/. Last visited 25/10/2021.

Hoang, N. P., Polychronakis, M. and Gill, P., ‘Measuring the accessibility of domain name encryption and its impact on internet filtering’, *CoRR*, Vol. abs/2202.00663, 2022. URL https://arxiv.org/abs/2202.00663.

Hoffman, P., ‘Cryptographic Algorithm Identifier Allocation for DNSSEC’. RFC 6014 (Proposed Standard), Nov. 2010. URL http://www.ietf.org/rfc/rfc6014.txt.

Hoffman, P. E. and McManus, P., ‘DNS Queries over HTTPS (DoH)’. RFC 8484, Oct. 2018. . URL https://rfc-editor.org/rfc/rfc8484.txt.

Hounsel, A., Borgolte, K., Schmitt, P., Holland, J. and Feamster, N., ‘Analyzing the costs (and benefits) of dns, dot, and doh for the modern web’, In ‘Proceedings of the Applied Networking Research Workshop, ANRW 2019, Montreal, Quebec, Canada, July 22, 2019’, , edited by P. Gill and J. IyengarACM, pp. 20–22. . URL https://doi.org/10.1145/3340301.3341129.

Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D. and Hoffman, P. E., ‘Specification for DNS over Transport Layer Security (TLS)’. RFC 7858, May 2016. . URL https://rfc-editor.org/rfc/rfc7858.txt.

Huitema, C., Dickinson, S. and Mankin, A., ‘DNS over Dedicated QUIC Connections’, Internet-Draft draft-ietf-dprive-dnsoquic-09, Internet Engineering Task Force, Feb. 2022. URL https://datatracker.ietf.org/doc/html/draft-ietf-dprive-dnsoquic-09. Work in Progress.

Huitema, C., Mankin, A. and Dickinson, S., ‘Specification of DNS over Dedicated QUIC Connections’, Internet-Draft draft-huitema-dprive-dnsoquic-00, Internet Engineering Task Force, Mar. 2020. URL https://datatracker.ietf.org/doc/html/draft-huitema-dprive-dnsoquic-00. Work in Progress.

Huitema, C., Mankin, A. and Dickinson, S., ‘Specification of DNS over Dedicated QUIC Connections’, Internet-Draft draft-ietf-dprive-dnsoquic-02, Internet Engineering Task Force, 2 2021. URL https://datatracker.ietf.org/doc/html/draft-ietf-dprive-dnsoquic-02. Work in Progress.

Huston, G. and Damas, J., ‘Measuring recursive resolver centrality’. 2021. URL https://www.icann.org/en/system/files/files/presentation-day1b-resolver-centrality-huston-25may21-en.pdf. Last visited 02/11/2021.

ICANN Research, ‘TLD DNSSEC Report’. n.d. URL http://stats.research.icann.org/dns/tld_report/. Last visited 28/10/2021.

Internet Society, ‘DNSSEC Deployment Maps’. 2021. URL https://www.internetsociety.org/deploy360/dnssec/maps/. Last visited 28/10/2021.

Iyengar, J. and Thomson, M., ‘QUIC: A UDP-Based Multiplexed and Secure Transport’. RFC 9000, May 2021. . URL https://rfc-editor.org/rfc/rfc9000.txt.

Kambourakis, G., Draper-Gil, G. and Sanchez, I., 'What email servers can tell to johnny: An empirical study of provider-to-provider email security', *IEEE Access*, Vol. 8, 2020, pp. 130066–130081. . URL https://doi.org/10.1109/ACCESS.2020.3009122.

Kambourakis, G., Moschos, T., Geneiatakis, D. and Gritzalis, S., 'Detecting dns amplification attacks', In 'Critical Information Infrastructures Security', , edited by J. Lopez and B. M. HämmerliSpringer Berlin Heidelberg, Berlin, Heidelberg, pp. 185–196.

Kambourakis, G., Spigolon, R. and Karopoulos, G., 'Domain name system security extensions (dnssec) standards: an analysis of uptake in the eu - september 2022', *Publications Office of the European Union*, 2022.

Kampourakis, G. and Karopoulos, G., 'Domain name system security extensions (dnssec) standards: an analysis of uptake in the eu - march 2022', , No KJ-NA-31-273-EN-N (online), 2022. ISSN 1831-9424 (online). .

Karel Hynek, 'The prevalence of DNS over HTTPS'. 2021. URL https://blog.apnic.net/2021/09/13/the-prevalence-of-dns-over-https/. Last visited 22/11/2021.

Kinnear, E., McManus, P., Pauly, T., Verma, T. and Wood, C. A., 'Oblivious DNS Over HTTPS', Internet-Draft draft-pauly-dprive-oblivious-doh-10, Internet Engineering Task Force, Sep. 2021. URL https://datatracker.ietf.org/doc/html/draft-pauly-dprive-oblivious-doh-10. Work in Progress.

Kitterman, S., 'Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1'. RFC 7208 (Proposed Standard), Apr. 2014. URL http://www.ietf.org/rfc/rfc7208.txt. Updated by RFC 7372.

Kosek, M., Doan, T. V., Granderath, M. and Bajpai, V., 'One to rule them all? a first look at dns over quic'. 2022.

Kucherawy, M. and Zwicky, E., 'Domain-based Message Authentication, Reporting, and Conformance (DMARC)'. RFC 7489 (Informational), Mar. 2015. URL http://www.ietf.org/rfc/rfc7489.txt.

Lamb, Rick, 'DNSSEC Deployment Report'. n.d. URL https://rick.eng.br/dnssecstat/. Last visited 28/10/2021.

Mayrhofer, A., 'The EDNS(0) Padding Option'. RFC 7830, May 2016. . URL https://rfc-editor.org/rfc/rfc7830.txt.

Mozilla, 'Letter from Mozilla about DoH to Senate and House Committee Chairmen and Ranking Members'. 2019. URL https://www.ncta.com/sites/default/files/2019-09/Final%20DOH%20LETTER%209-19-19.pdf. Last visited 21/02/2022.

Mozilla, 'Firefox extends privacy and security of Canadian internet users with by-default DNS-over-HTTPS rollout in Canada'. 2021. URL https://blog.mozilla.org/en/mozilla/news/firefox-by-default-dns-over-https-rollout-in-canada/. Last visited 24/11/2021.

NCTA, CTIA, USTELECOM, 'Letter from major US telecommunications associations to Senate and House Committee Chairmen and Ranking Members'. 2019. URL https://www.ncta.com/sites/default/files/2019-09/Final%20DOH%20LETTER%209-19-19.pdf. Last visited 21/02/2022.

OWASP, 'OWASP Top Ten'. URL https://owasp.org/www-project-top-ten/.

Radu, R. and Hausding, M., 'Consolidation in the dns resolver market – how much, how fast, how dangerous?', *Journal of Cyber Policy*, Vol. 5, No 1, 2020, pp. 46–64. .

Ramaswamy Chandramouli and Scott Rose, 'Secure Domain Name System (DNS) Deployment Guide'. 2013. URL https://csrc.nist.gov/publications/detail/sp/800-81/2/final. Last visited 15/02/2022.

Rescorla, E., 'The Transport Layer Security (TLS) Protocol Version 1.3'. RFC 8446, Aug. 2018. . URL https://rfc-editor.org/rfc/rfc8446.txt.

Rescorla, E., Oku, K., Sullivan, N. and Wood, C. A., 'TLS Encrypted Client Hello', Internet-Draft draft-ietf-tls-esni-13, Internet Engineering Task Force, Aug. 2021. URL https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-13. Work in Progress.

Schwartz, B. M., Bishop, M. and Nygren, E., ‘Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)’, Internet-Draft draft-ietf-dnsop-svcb-https-08, Internet Engineering Task Force, Oct. 2021. URL https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-08. Work in Progress.

Scott Helme, ‘Top 1 Million Analysis - March 2020’. a. URL https://scotthelme.co.uk/top-1-million-analysis-march-2020/.

Scott Helme, ‘Top 1 Million Sites Security Analysis’. b. URL https://crawler.ninja/.

Shulman, H. and Waidner, M., ‘One key to sign them all considered vulnerable: Evaluation of DNSSEC in the internet’, In ‘14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)’, USENIX Association, Boston, MA. ISBN 978-1-931971-37-9, pp. 131–144. URL https://www.usenix.org/conference/nsdi17/technical-sessions/presentation/shulman.

Siby, S., Juárez, M., Díaz, C., Vallina-Rodriguez, N. and Troncoso, C., ‘Encrypted DNS -> privacy? A traffic analysis perspective’, In ‘27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020’, The Internet Society.

Singanamalla, S., Chunhapanya, S., Hoyland, J., Vavrusa, M., Verma, T., Wu, P., Fayed, M., Heimerl, K., Sullivan, N. and Wood, C. A., ‘Oblivious DNS over HTTPS (odoh): A practical privacy enhancement to DNS’, *Proc. Priv. Enhancing Technol.*, Vol. 2021, No 4, 2021, pp. 575–592. . URL https://doi.org/10.2478/popets-2021-0085.

StatDNS, ‘List of ccTLDs – Country Code Top-Level Domains’. n.d.a. URL https://www.statdns.com/cctlds/. Last visited 28/10/2021.

StatDNS, ‘Zone File Statistics’. n.d.b. URL https://www.statdns.com/. Last visited 29/10/2021.

The Register, ‘DoH! Mozilla assures UK minister that DNS-over-HTTPS won’t be default in Firefox for Britons’. 2019. URL https://www.theregister.com/2019/09/24/mozilla_backtracks_doh_for_uk_users/. Last visited 24/11/2021.

The Shadow Server Foundation, ‘The Open Resolver Scanning Project’. URL https://indico.dns-oarc.net/event/0/contributions/1/attachments/19/125/201305-dnsoarc-mauch-openresolver.pdf. Last visited 28/10/2021.

The Shadow Server Foundation, ‘The Open Resolver Scanning Project’. n.d. URL https://scan.shadowserver.org/dns/. Last visited 28/10/2021.

Timothy B. Lee, ‘Why big ISPs aren’t happy about Google’s plans for encrypted DNS’. 2019. URL https://arstechnica.com/tech-policy/2019/09/isps-worry-a-new-chrome-feature-will-stop-them-from-spying-on-you/. Last visited 21/02/2022.

van Rijswijk-Deij, R., Sperotto, A. and Pras, A., ‘DNSSEC and Its Potential for DDoS Attacks: A Comprehensive Measurement Study’, In ‘Proceedings of the 2014 Conference on Internet Measurement Conference’, IMC ’14. ACM, New York, NY, USA, pp. 449–460.

Wander, M., ‘Measurement survey of server-side DNSSEC adoption’, In ‘Network Traffic Measurement and Analysis Conference, TMA 2017, Dublin, Ireland, June 21-23, 2017’, IEEE, pp. 1–9. . URL https://doi.org/10.23919/TMA.2017.8002913.

Wang, Z., ‘A revisit of DNS kaminsky cache poisoning attacks’, In ‘2015 IEEE Global Communications Conference, GLOBECOM 2015, San Diego, CA, USA, December 6-10, 2015’, IEEE, pp. 1–6. . URL https://doi.org/10.1109/GLOCOM.2014.7417017.

Weiler, S. and Blacka, D., ‘Clarifications and Implementation Notes for DNS Security (DNSSEC)’. RFC 6840 (Proposed Standard), Feb. 2013. URL http://www.ietf.org/rfc/rfc6840.txt.

Weissbacher, M., Lauinger, T. and Robertson, W., ‘Why is csp failing? trends and challenges in csp adoption’, In ‘International Workshop on Recent Advances in Intrusion Detection’, Springer, pp. 212–233.

XDA, ‘BraveDNS is an open-source DNS-over-HTTPS client, firewall, and adblocker for Android’. 2020. URL https://www.xda-developers.com/bravedns-open-source-dns-over-https-client-firewall-adblocker-android/. Last visited 22/11/2021.

Yoshibumi Suematsu, ‘APNIC - Why has DNSSEC increased in some economies and not others?’ 2020. URL https://blog.apnic.net/2020/07/10/why-has-dnssec-increased-in-some-economies-and-not-others/. Last visited 25/10/2021.

ZDNet, ‘China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI’. URL https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/. Last visited 24/11/2021.

ZDNet, ‘China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI’. 2020a. URL https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/. Last visited 24/11/2021.

ZDNet, ‘Russia wants to ban the use of secure protocols such as TLS 1.3, DoH, DoT, ESNI’. 2020b. URL https://www.zdnet.com/article/russia-wants-to-ban-the-use-of-secure-protocols-such-as-tls-1-3-doh-dot-esni/. Last visited 24/11/2021.

List of abbreviations and definitions

AS Autonomous System

DKIM Domain Keys Identified Mail

DMARC Domain-based Message Authentication, Reporting and Conformance

DNS Domain Name System

DNSSEC DNS Security Extensions

DoH DNS queries over HTTPS

DoQ DNS over QUIC

DoT DNS over TLS

EC European Commission

EU European Union

IETF Internet Engineering Task Force

ISP Internet Service Provider

MS Member State

SPF Sender Policy Framework

List of figures

List of tables

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

— at the following standard number: +32 22999696,

— via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
joint-research-centre.ec.europa.eu

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

@eu_science

Publications Office
of the European Union