ISSN 1831-9424

JRC TECHNICAL REPORT

Internet Standards

Web communication standards: an analysis of uptake in the EU

March 2023

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

EUR 31552 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

JRC133219

EUR 31552 EN

PDF ISBN 978-92-68-04290-8 ISSN 1831-9424 doi:10.2760/546086 KJ-NA-31-552-EN-N

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: Kouliaridis, V., Karopoulos, G., Spigolon, R. and Sanchez Martin, J.I., *Web communication standards: an analysis of uptake in the EU, March 2023*, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/546086, JRC133219.

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

The broad deployment of Hypertext Transfer Protocol (HTTP)-related standards (such as, HTTPS, HTTP/3 and HTTP security response headers) is imperative for ensuring the interoperability, security, scalability and stability of the Internet. This report studies the adoption rate of modern HTTP-related technologies, namely HTTP Secure (HTTPS), the latest version of HTTP, i.e., HTTP/3, and HTTP Strict Transport Security (HSTS) response header in Q1 2023 across EU Member States, as well as globally. The analysis of the level of uptake of web communication standards has been carried out using publicly available data, as well as data collected from measurements conducted by the European Commission's Joint Research Centre.

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 Commission is exploring mechanisms to systematically monitor the evolution of standards used in web browsing for identifying gaps and barriers for their adoption, and evaluate the need for regulatory measures to promote their uptake.

The Hypertext Transfer Protocol (HTTP) provides the foundation of web browsing. However, given that HTTP does not provide any kind of security, it is easy for an attacker to get access to sensitive data exchanged over the web, such as credit card numbers. The most widely used standard for secure HTTP communications is Hypertext Transfer Protocol Secure (HTTPS). In addition, HTTP/3 is designed to improve the performance of HTTPS traffic, as well as imposing the use of HTTPS by default. A further measure for secure communications over HTTP is HSTS, which requests the web browser to access the web site over HTTPS for mitigating attacks and security vulnerabilities.

This report provides an analysis of the adoption rate of modern web communication technologies (that is, HTTPS, HTTP/3 and HSTS) in the EU Member States (MSs), as well as globally. The data stem from publicly available data sources.

In the EU MSs, the current results for Q1 2023 show a similar trend to Q3 2022 with a very high HTTPS adoption in average (80.98%), which is almost the same as the global adoption rate (81.7%). Looking at each country individually, the adoption rates are quite homogeneous as shown in Figure 1, ranging approximately from 68 to 94%. This means that, in every MS, at least two thirds of the websites support secure web browsing. Globally, even though the adoption rate is already high, it is still steadily growing with time.

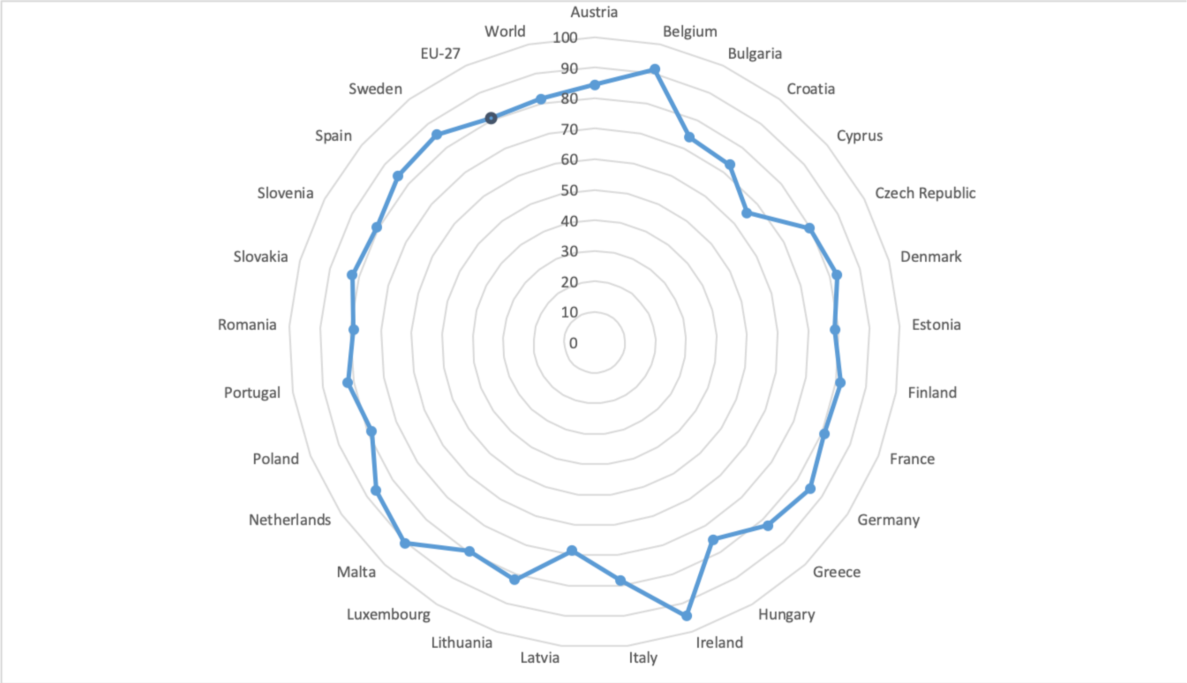

Figure 1: Usage of HTTPS in the top websites situated in EU MSs (Q-Success)

The adoption rate of HTTP/3 in EU MSs is low on average (10.5%), while also being significantly lower than the global average (25.2%). While the world average is the same as it was in Q3 2022, for EU MSs a slight decrease of 0.5%, was observed between Q3 2022 and Q1 2023. The adoption rates in MSs are quite heterogeneous as shown in Figure 2, ranging approximately from 1.5 to 42.3%.

Regarding HTTP security response headers, global results suggest that overall adoption is still low, at 25%. Data for the EU MSs are available for HSTS only; these data confirm the low adoption of this header in the vast majority of EU MSs with an average of less than 17%, as shown in Figure 3. The results of the study show that globally there is a slow positive trend of HTTP security response headers adoption.

Overall, it is argued that HTTPS is a mature and well-supported technology, both in the EU and globally. On

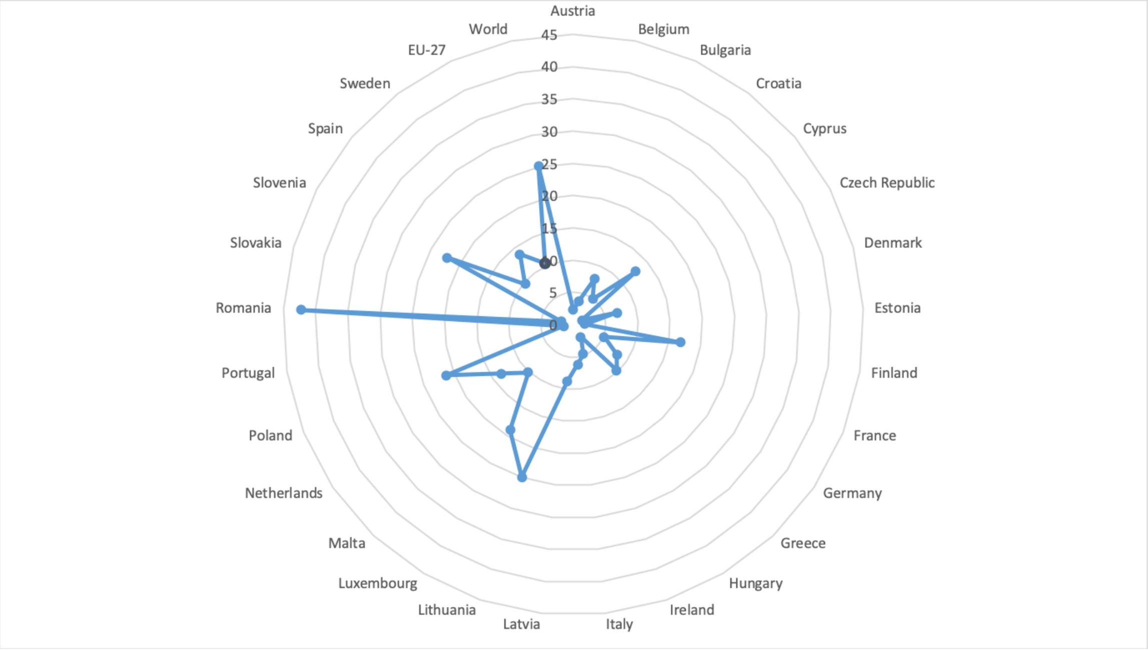

Figure 2: Usage of HTTP/3 in the top websites situated in EU MSs (Q-Success)

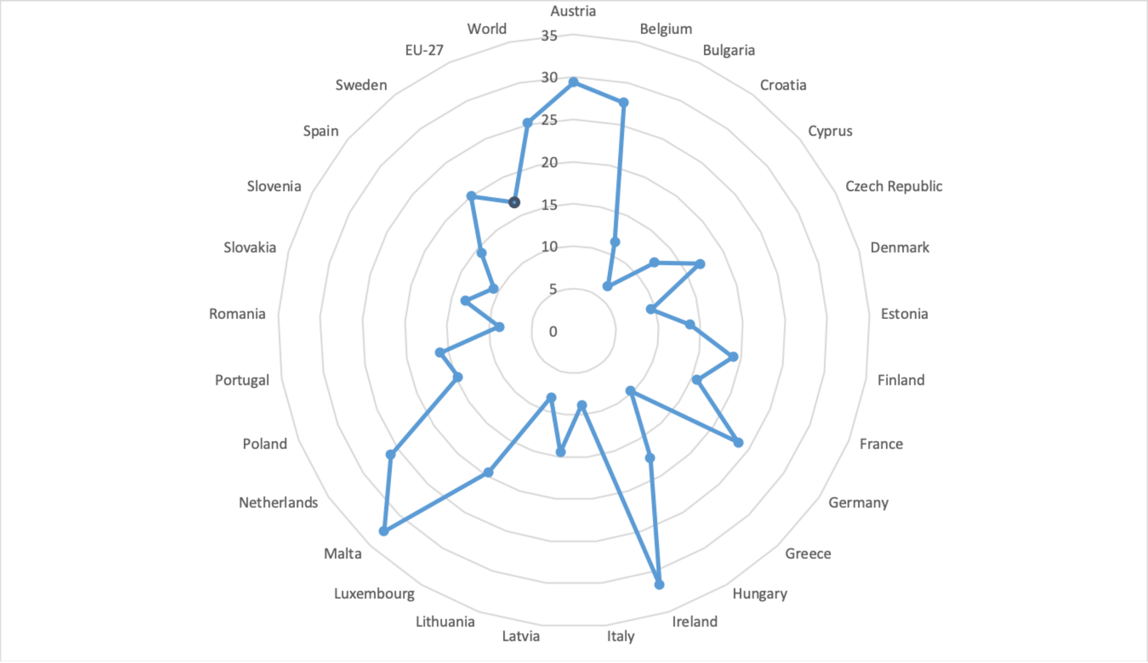

Figure 3: Usage of HSTS in the top websites situated in EU MSs (Q-Success)

the other hand, HTTP/3 and HSTS adoption rates lag behind in the EU, with the former being almost half of the global average and the latter being close to the global average. In the case of HTTP/3, this could be attributed to it being a relatively new standard (its first stable version was published in June 2022).

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.”*

To that end, this report concentrates on web communication standards used for browsing. The initial versions of Hypertext Transfer Protocol (HTTP) did not provide robust security protection; considering, however, the increasing exchange of sensitive data over the World Wide Web (WWW), the adoption of modern web security standards is necessary. Such standards include Transport Layer Security (TLS), HTTP version 3 or HTTP/3, and HTTP security headers like HTTP Strict Transport Security (HSTS); the wide adoption of these standards would offer a secure and efficient browsing experience to end users.

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 web communication standards used for browsing in the European Union (EU) and globally. The first report concerned Q1 2022 (G et al., 2022) whereas this one presents results for Q3 2022. Similarly as the previous version, this report is based on open data and presents results and analysis of the adoption rates of Hypertext Transfer Protocol Secure (HTTPS)/TLS, HTTP/3 and HSTS. The key observations from Q3 2022 were that HTTPS shows a very high adoption rate, both in the EU and globally. On the contrary, HTTP/3 adoption is very low, especially in EU Member States (MSs) where it is half than the global rate. HSTS and HTTP security headers in general have a low adoption rate in the EU, a trend that is also observed globally. Current measurements for Q1 2023 report similar figures; the average adoption rates for HTTPS and HSTS have slightly increased. In contrast, HTTP/3 adoption rates for EU MSs report a small increase (0.5%).

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 divided into subsections for HTTPS, HTTP/3 and HSTS/HTTP security headers. 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 15/02/2023. Overall, the remarks and recommendations of the previous report (Karopoulos et al., 2022), and especially the analysis and conclusions sections, still apply here given the minor differences in the deployment results. Next, an overview of the data sources and methodology followed by each source entity to collect the respective dataset is given; these are the same as in the previous version of the report but are repeated here for convenience.

Table 1: Data sources used for estimating the adoption rate of web technologies

Source	Description
Q-Success (Q-Success, n.d.h)	Daily statistics of web technologies usage, total and by country, among others for: HTTPS (Q-Success, n.d.c, Q-Success, n.d.a), HSTS (Q-Success, n.d.e, Q-Success, n.d.b) and HTTP/3 (Q-Success, n.d.f, Q-Success, a)
Crawler.Ninja (Helme, n.d.)	Daily statistics of website security metrics, including HTTP security response headers
Related work	Academic peer-reviewed and individual works measuring the adoption of HTTP security response headers
Our results	Our measurements on the adoption rates of HTTPS, HSTS, and HTTP/3 on the Tranco Top 1M domains

Q-Success – The data are provided by the company's W3Techs division (Q-Success, n.d.h) that reports the adoption rates of several web technologies by the top 10M million websites worldwide. Among the metrics reported are HTTPS and HTTP/3 worldwide, as well as by country. This list is based on the Tranco (Tranco, n.d.) list, as well as other sources, excluding unused websites; for example, sites with only a default web server page. When there are subdomains and redirected domains of a main domain they are counted only as a single website, that is, the main domain. Regarding the collected data, each website is visited approximately once a month, while the reports are updated daily.

Crawler.Ninja – This source hosts data reported by a crawler on website security-related metrics. It uses the Tranco top 1M list and provides free access to the raw data collected daily. The metrics provided are adoption rates of HTTP security headers, such as HSTS, CSP, XFO, and XCTO. Results are also provided for HTTPS redirection, Let's Encrypt certificate usage, TLS versions employed, cipher suites used and key sizes.

Our results – This round of reports also includes our results on the adoption rates of HTTPS, HSTS, and HTTP/3 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 for HTTPS support of each domain and also extracted HSTS response header, when available. Additionally, we check each domain for HTTP/3 support, by using a custom version of CURL (curl.se, n.d.).

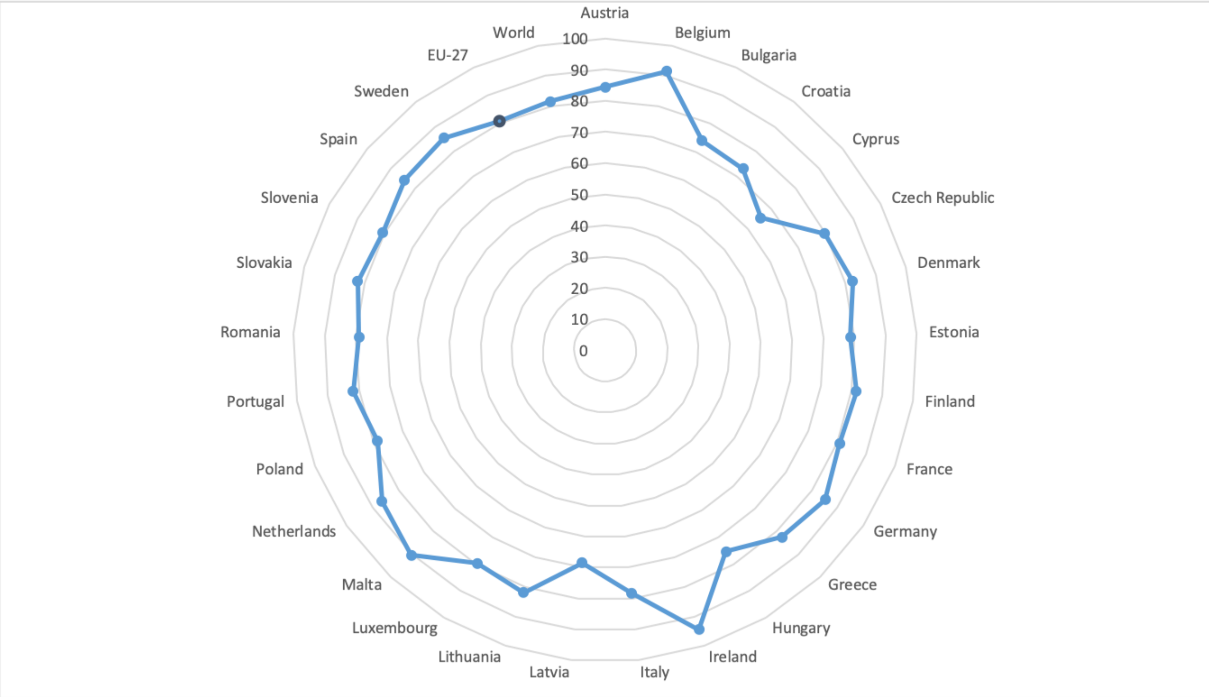

Figure 4: Usage of HTTPS in the top websites situated in EU countries (Q-Success)

3 Data analysis

Overall, the collected results for Q1 2023 show a slight increase in the adoption of the HTTP-related standards, which is steady when observing 1-year long data. It is interesting to note that, while a few countries showed some significant differences in the adoption rates of different standards between 10 and 20%. Having said that, the remarks and recommendations of the previous report (Karopoulos et al., 2022), and especially the analysis and conclusions sections, still apply here given the minor differences in the rest of the deployment results.

3.1 HTTPS

Public data from Q-Success on the adoption rates of HTTPS on websites situated in the EU MSs and a selection of other countries worldwide is shown in Tables 2. The EU average has increased by 1.77%, reaching 80.98% and being in line with the global rise, whereas the standard deviation is similar to the previous data from Q3 2022. In the vast majority of EU countries there is an augmentation in the HTTPS adoption rate with only a few countries, namely Croatia, Cyprus, and Czech republic, having a slightly lower rate. The EU data are also graphically represented in Figure 4.

Additionally, for Q1 2023, this report presents our results on the adoption rate of HTTPS in the EU MSs, which are shown in Table 3. Precisely, our results are almost similar to those of Q-Success, with an average adoption rate of 80.67% (0.31% lower than reported by Q-Success). By looking at individual MSs, the only major difference (>10%) is with Bulgaria, where our results report a 12% higher update. This believe that this is the result of the different methodology used to map domains to countries, i.e., in our results, we map domains to countries based on their TLD, while Q-Success maps domains to countries based on the server/host location. Nevertheless, we believe that measuring the adoption of indicators with both mapping methods results in a more thorough analysis.

Regarding the selected non-EU countries, Figure 5 gives a graphical overview of the data presented in Table 2. Also in this case, the vast majority of countries has an improved adoption rate, whereas two countries (Argentina, Japan, and South Korea) have a lower rate than Q3 2022.

The rate of the top 10M websites globally that use HTTPS by default in Q1 2023 is 81.7%, according to the Q-Success website (Q-Success, n.d.c). These data demonstrate an increase of 2.2% since Q3 2022. Figure 6 shows this increasing trend in the last year; the total increase in this last year is less than 10%.

Table 2: HTTPS adoption rate in the EU-27 MS and worldwide (Q-Success)

EU-27 MS	%	Country	%
Austria	84.4	Argentina	65.0
Belgium	91.5	Australia	88.3
Bulgaria	74.0	Bangladesh	59.1
Croatia	73.0	Belarus	73.9
Cyprus	65.5	Brazil	75.4
Czech Republic	79.7	Canada	78.5
Denmark	82.3	China	42.5
Estonia	78.7	India	74.4
Finland	81.6	Indonesia	69.5
France	80.9	Iran	67.9
Germany	85.3	Israel	97.6
Greece	82.5	Japan	70.5
Hungary	75.3	Kazakhstan	79.3
Ireland	94.4	Malaysia	73.8
Italy	78.3	Norway	87.8
Latvia	68.6	Russian Federation	72.6
Lithuania	81.9	Saudi Arabia	74.7
Luxembourg	79.7	Singapore	76.3
Malta	90.4	South Africa	80.9
Netherlands	86.4	South Korea	48.0
Poland	78.6	Switzerland	87.1
Portugal	81.9	Taiwan	62.1
Romania	79.0	Thailand	63.4
Slovakia	82.3	Turkey	67.9
Slovenia	80.6	Ukraine	77.4
Spain	84.4	United Kingdom	85.9
Sweden	85.4	United States	83.1
Average EU-27	80.98		
StDev EU-27	6.3		
World	81.7		

Table 3: HTTPS adoption rate in the EU-27 MS (Our results)

EU-27 MS	%	EU-27 MS	%
Austria	85.32	Italy	78.50
Belgium	82.53	Latvia	74.83
Bulgaria	86.13	Lithuania	78.58
Croatia	79.93	Luxembourg	81.16
Cyprus	50.00	Malta	90.91
Czech Republic	77.58	Netherlands	86.03
Denmark	84.21	Poland	77.64
Estonia	85.78	Portugal	82.42
Finland	84.66	Romania	83.29
France	80.82	Slovakia	77.47
Germany	83.86	Slovenia	79.96
Greece	83.08	Spain	79.89
Hungary	72.25	Sweden	85.99
Ireland	85.38		
Average EU-27	80.67		
StDev EU-27	7.35		

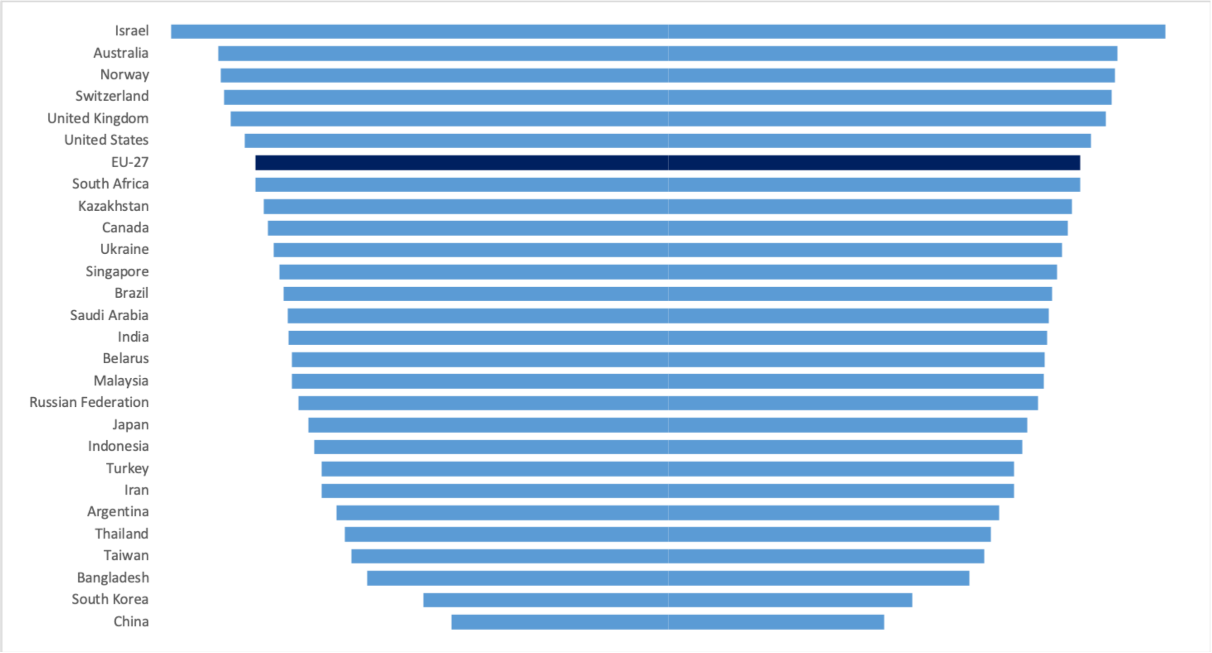

Figure 5: Usage of HTTPS on the top websites situated in selected countries (Q-Success)

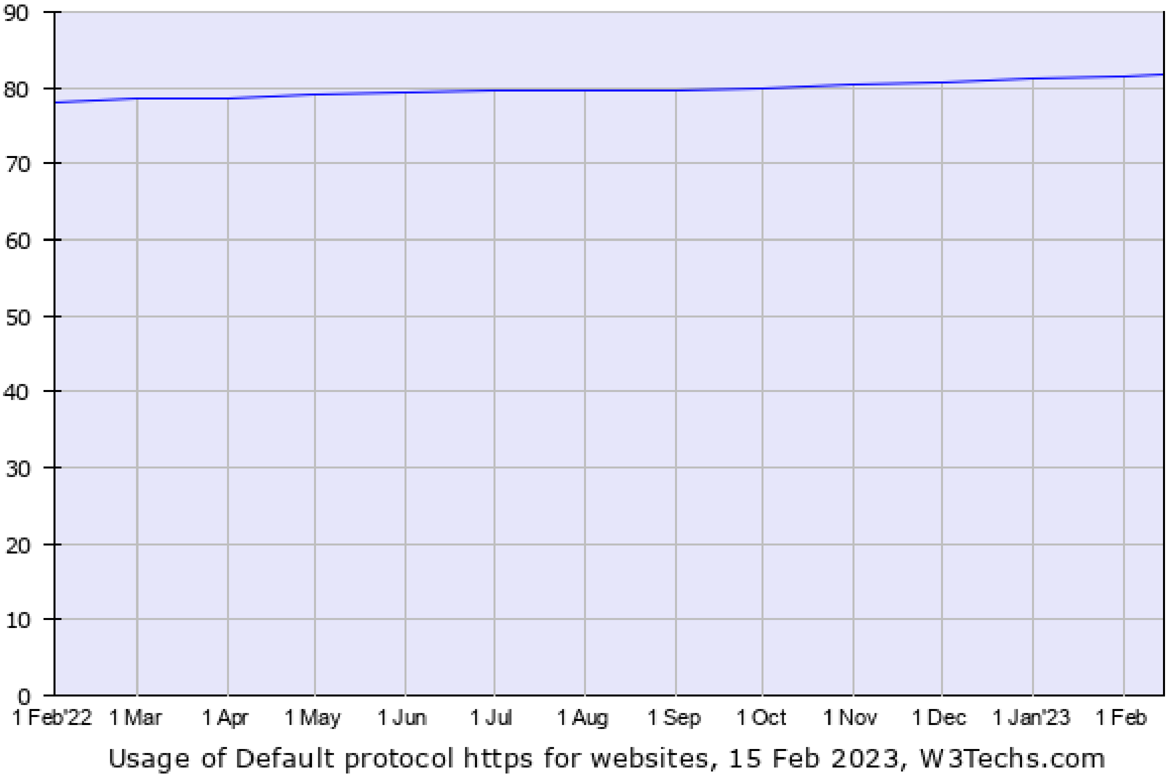

Figure 6: Usage of HTTPS in the top 10M websites (Q-Success, n.d.c)

3.2 HTTP/3

The adoption rates of HTTP/3 in the EU and a selection of non-EU countries are presented in detail in Table 4; the same data were used for the graphs in Figures 7 and 8 for EU and non-EU countries respectively. In total, the average adoption rate decreased in the EU countries by 0.79% dropping at 10.5%. What is interesting is that Romania saw a major rise from 35.5% in Q3 2022 to 42.3% in Q1 2023. The world average showed no difference since Q3 2022.

Similar to HTTPS, this round of reports also includes our own results on the adoption rate of HTTP/3. Precisely, Table 5 reports our results, which again are similar to those reported by Q-Sucess. Specifically, our results report a 10.93% rate for EU MSs, which is 0.43 percentage points (pp) higher than the rate reported by Q-Success. Compared to the data reported by Q-Success, the only major differences (>10pp) are in Romania (-20.6pp in our results), Cyprus (-12.7pp in our results), Greece (+10.8pp in our results), and Slovenia(-10.3pp in our results). It is also noteworthy that our data show 0% uptake for Malta and Cyprus.

According to Q-Success, the global adoption rate of HTTP/3 in the top 10M websites increased from 23.3% in Q1 2022 to 25.2% in Q1 2023, as shown in Figure 9. Compared to Q3 2022, the vast majority had a slight increase in HTTP/3 adoption. Nevertheless, the global adoption rate reported by Q-Success for Q1 2023 is still the same. However, it is important to note that Q-Success also measures the rate of adoption of many other countries that are not included in this report.

3.3 HTTP security response headers

The updated adoption rates for HSTS in EU and a selection of non-EU countries are presented in Table 6. The same data are also graphically depicted in Figures 10 and 11. Generally, the average HSTS uptake in the EU is at 16.76%, which is lower by 0.08pp compared to Q3 2022, whereas globally it is higher by 0.8pp, reaching 25.2%. In more detail, about half of the EU countries, precisely 16, have slightly lower adoption rates compared to the previous data; in non-EU countries the vast majority has an increased adoption rate with only two of them showing a decrease.

On the other hand, our results shown in Table 7 report an average HSTS uptake of 27.7% in the EU, which is 10.94pp higher than the average reported by Q-Success. Compared to the data reported by Q-Success, the major differences (>+10pp) in our data are noted in 17 MSs. We believe that the reason behind this difference

Table 4: HTTP/3 adoption rate in the EU-27 MS and worldwide (Q-Success)

EU-27 MS	%	Country	%
Austria	2.3	Argentina	1.9
Belgium	3.7	Australia	28.4
Bulgaria	7.8	Bangladesh	41.6
Croatia	5.0	Belarus	4.1
Cyprus	12.7	Brazil	11.4
Czech Republic	1.5	Canada	17.8
Denmark	7.0	China	2.3
Estonia	1.8	India	15.6
Finland	16.9	Indonesia	40.1
France	5.1	Iran	33.8
Germany	8.2	Israel	86.1
Greece	9.7	Japan	2.8
Hungary	2.2	Kazakhstan	0.2
Ireland	4.8	Malaysia	27.9
Italy	6.2	Norway	10.1
Latvia	8.8	Russian Federation	1.5
Lithuania	24.9	Saudi Arabia	1.4
Luxembourg	19.0	Singapore	23.2
Malta	10.2	South Africa	9.5
Netherlands	13.5	South Korea	0.4
Poland	21.2	Switzerland	9.7
Portugal	1.5	Taiwan	5.2
Romania	42.3	Thailand	1.7
Slovakia	1.9	Turkey	37.8
Slovenia	22.1	Ukraine	4.4
Spain	9.8	United Kingdom	15.9
Sweden	13.7	United States	14.4
Average EU-27	10.5		
StDev EU-27	9.27		
World	25.2		

Table 5: HTTP/3 adoption rate in the EU-27 MS (Our results)

EU-27 MS	%	EU-27 MS	%
Austria	6.08	Italy	11.42
Belgium	6.99	Latvia	11.36
Bulgaria	14.48	Lithuania	19.84
Croatia	13.75	Luxembourg	9.66
Cyprus	0	Malta	0
Czech Republic	5.24	Netherlands	10.75
Denmark	16.92	Poland	16.49
Estonia	7.5	Portugal	10.59
Finland	12.24	Romania	21.68
France	10.2	Slovakia	6.55
Germany	6.28	Slovenia	11.78
Greece	20.58	Spain	12.35
Hungary	8.19	Sweden	11.33
Ireland	12.95		
Average EU-27	10.93		
StDev EU-27	5.40		

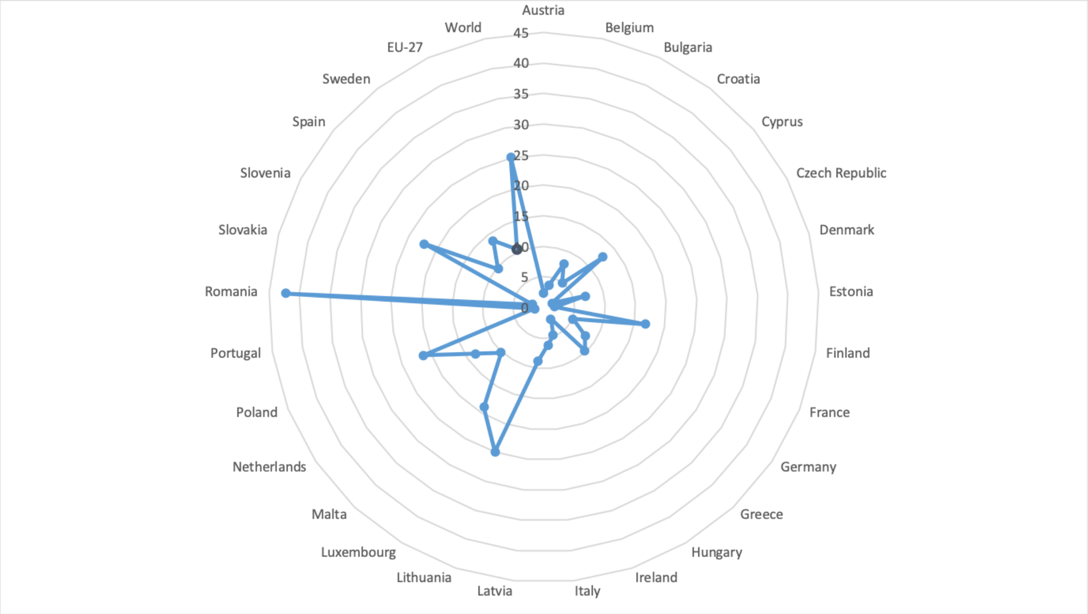

Figure 7: Usage of HTTP/3 on the top websites situated in EU countries (Q-Success)

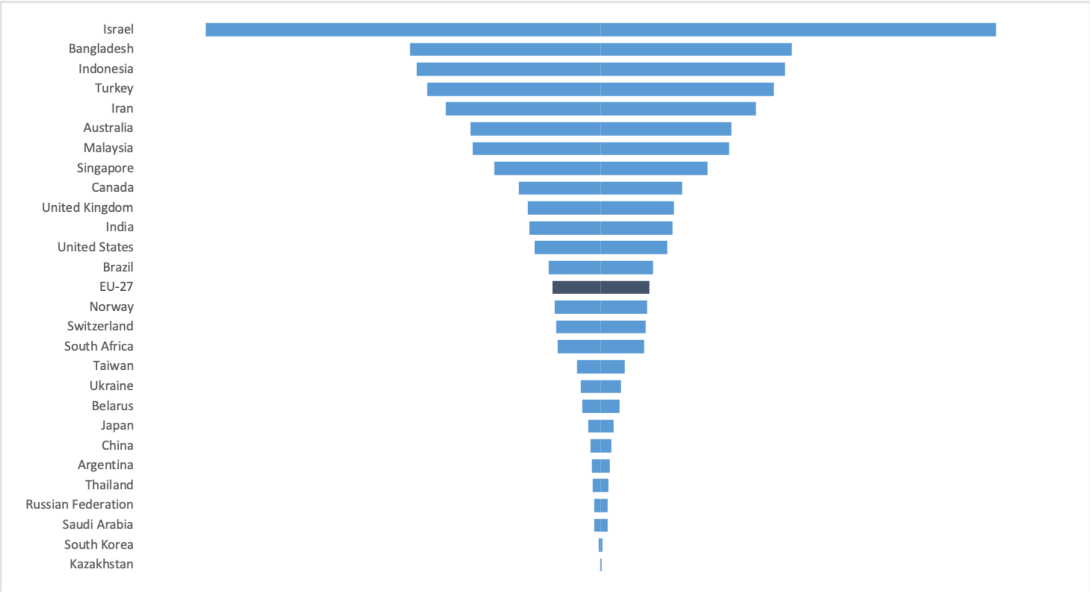

Figure 8: Usage of HTTP/3 on the top websites situated in selected countries (Q-Success)

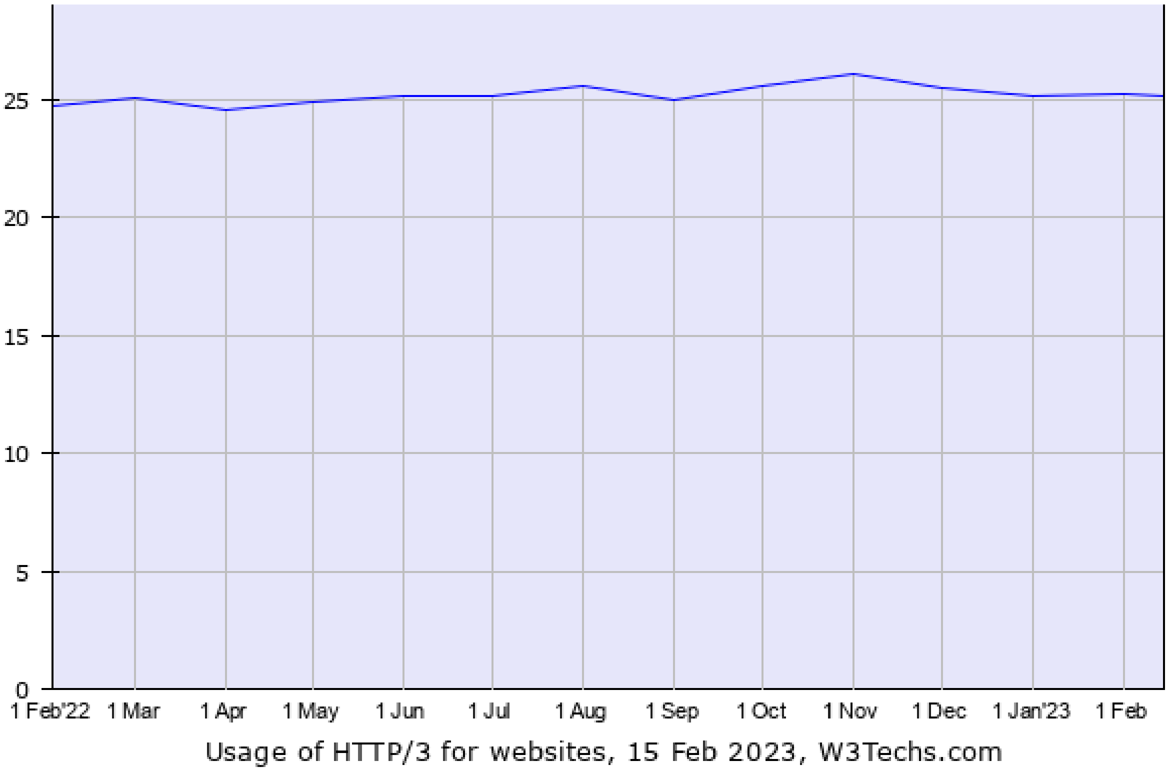

Figure 9: Usage of HTTP/3 for websites (Q-Success, n.d.f)

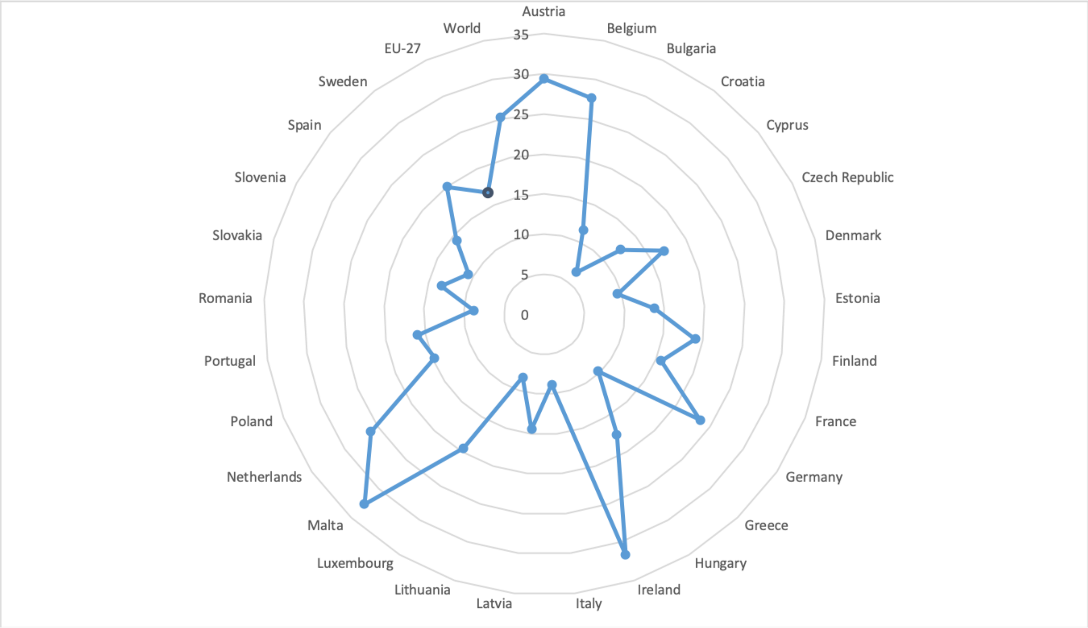

Figure 10: Usage of HSTS in the top websites situated in EU countries (Q-Success)

could be the number of domains used by Q-Success. More specifically, Q-Success measure the adoption rates for the Top 10M domains, whereas our results concern the Top 1M domains of the Tranco list.

The global adoption rate of the HSTS security header in the top 10M websites is 25.2% in Q1 2023, as presented in Figure 12. This is an increase of about 2.4pp compared to Q1 2022. Overall, the HSTS support is still low globally but with a slow, increasing trend.

Table 8 provides an historical overview of the adoption rate of the six most common HTTP security headers in the top 1M websites since 2014; it is an updated version of the relevant table from Q1 2022 with the addition of data for all HTTP security headers from Crawler.Ninja for 2022. In most headers there is a slight increase in the adoption rate from Q1 to Q3 2022, ranging from 0.03pp to 1.29pp The exceptions are XCTO with a rather insignificant decrease of 0.21pp and XXP with 0.37pp. It should be noted here that the XXP header has been deprecated in favor of CSP; more precisely, Edge abandoned the XSS Filter in July 2018([1]), Google retired XXP since Chrome 78 in 2019 ([2]), and Firefox does not support this header([3]). This indicates that XXP support is expected to further decrease in the coming years. Overall, these results suggest that in the last months the adoption of HTTP security headers is relatively stable.

[1] https://blogs.windows.com/windows-insider/2018/07/25/announcing-windows-10-insider-preview-build-17723-and-build-18204/
[2] https://developers.google.com/web/updates/2019/09/chrome-78-deps-rems
[3] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection

Table 6: HSTS adoption rate in the EU-27 MS and worldwide (Q-Success)

EU-27 MS	%	Country	%
Austria	29.4	Argentina	4.4
Belgium	27.6	Australia	17.4
Bulgaria	11.6	Bangladesh	9
Croatia	6.6	Belarus	18
Cyprus	12.5	Brazil	10.8
Czech Republic	16.9	Canada	17.9
Denmark	9.5	China	15.9
Estonia	13.8	India	8.8
Finland	19.1	Indonesia	17.4
France	15.7	Iran	5.4
Germany	23.5	Israel	87.3
Greece	9.8	Japan	8.3
Hungary	17.5	Kazakhstan	20.3
Ireland	31.7	Malaysia	10.4
Italy	8.8	Norway	36.5
Latvia	14.4	Russian Federation	15.8
Lithuania	8.3	Saudi Arabia	23
Luxembourg	19.5	Singapore	22.6
Malta	32.6	South Africa	8.5
Netherlands	26.1	South Korea	14.6
Poland	14.7	Switzerland	40.1
Portugal	16	Taiwan	20.8
Romania	8.8	Thailand	17.5
Slovakia	13.3	Turkey	5.3
Slovenia	10.7	Ukraine	25.8
Spain	14.3	United Kingdom	16.6
Sweden	20	United States	32.1
Average EU-27	16.76		
StDev EU-27	7.4		
World	25.2		

Table 7: HSTS adoption rate in the EU-27 MS (Our results)

EU-27 MS	%	EU-27 MS	%
Austria	34.58	Italy	20.6
Belgium	31.94	Latvia	23.25
Bulgaria	29.74	Lithuania	21.42
Croatia	21.00	Luxembourg	37.68
Cyprus	25.00	Malta	27.27
Czech Republic	24.45	Netherlands	40.21
Denmark	25.19	Poland	20.45
Estonia	34.84	Portugal	30.91
Finland	39.63	Romania	16.98
France	31.25	Slovakia	24.45
Germany	34.01	Slovenia	25
Greece	18.03	Spain	26.81
Hungary	19.19	Sweden	31.15
Ireland	32.97		
Average EU-27	27.70		
StDev EU-27	6.65		

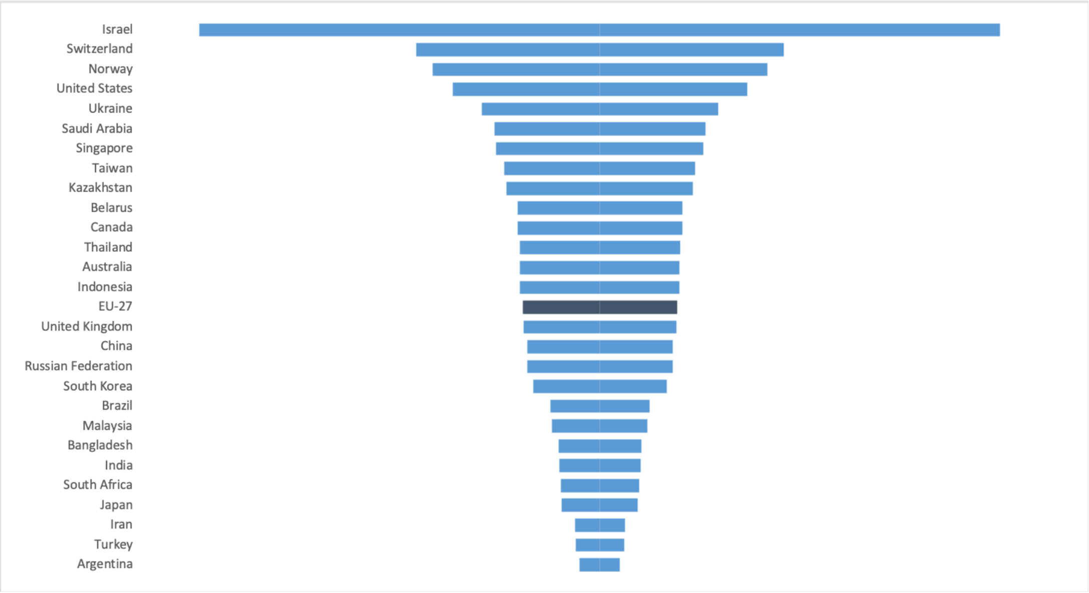

Figure 11: Usage of HSTS in the top websites situated in selected countries (Q-Success)

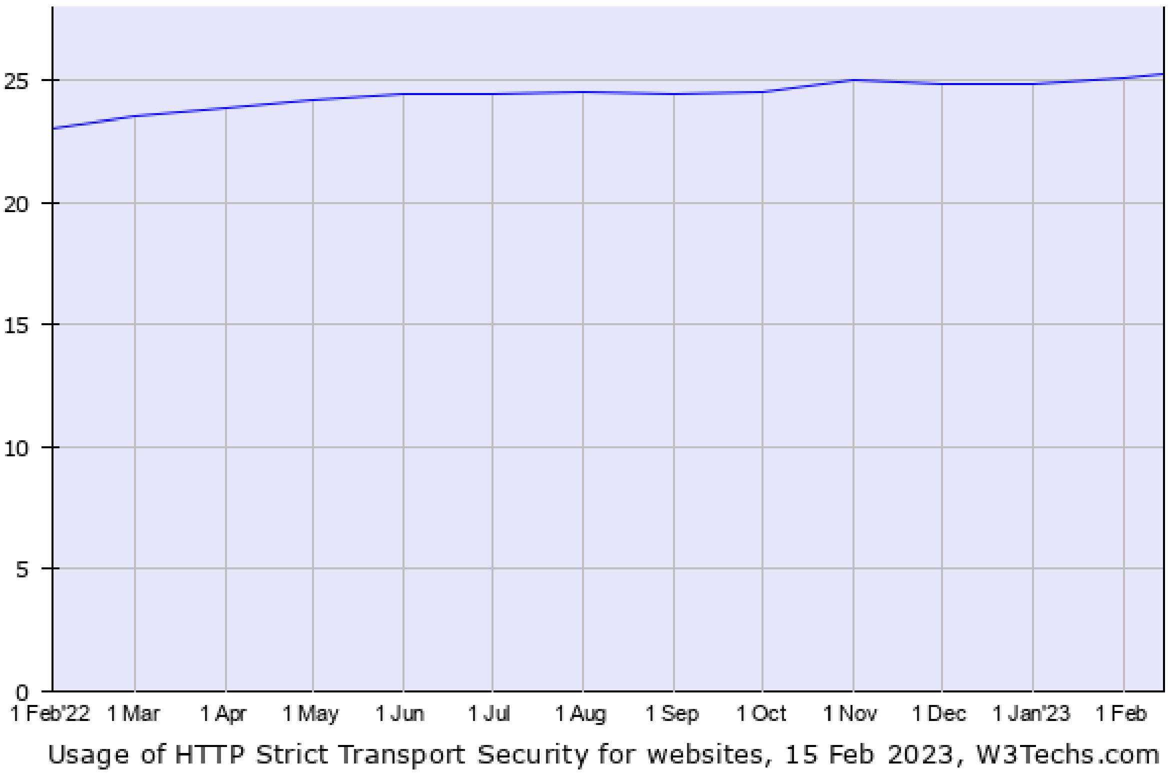

Figure 12: Usage statistics (%) of HSTS for the top 10M websites (Q-Success, n.d.e)

		HTTP security headers support (%)					
Year	**Work**	XFO	XCTO	HSTS	XXP	CSP	RP
2014	Weissbacher et. al (Weissbacher et al., 2014)	2.5	4.4	0.2	4.5	0.08	-
2015	Kranch et. al (Kranch and Bonneau, 2015)	-	-	0.51	-	-	-
2017	Buchanan et. al (Buchanan et al., 2017)	9.3	8	4	-	1.3	-
2018	Lavrenovs et. al (Lavrenovs and Melón, 2018)§	11.44	11.2	7	8.4	1.6	0.16
2018	Petrov et. al (Petrov et al., 2017)	-	-	4.12	-	-	-
2019	King (April King, 2019)	16.42	16.27	8.68	11.74	0.03*	-
2020	Helme (Helme, 2020)	13.49	12.71	11.28	9.98	4.54	3.9
2021	Karopoulos et. al (Karopoulos et al., 2021)	15.5	14.95	13.36	11.71	5.5	4.37
2021	Crawler.Ninja (Helme, n.d.)	19	18.84	17.86	14.15	7.98	6.52
2022	Crawler.Ninja (Helme, n.d.)	20.29	18.63	18.99	13.78	8.01	7.20

Table 8: Related work on the usage of HTTP security headers in the top 1M websites (Alexa list used up to 2019 and Tranco list afterwards, §approximate results calculated from data in (Lavrenovs and Melón, 2018), *A site is counted only if the respective header is implemented correctly)

4 Conclusions

The following concluding remarks are drawn from the analysis of the adoption rates of the different web technologies covered in this report. 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 (Karopoulos et al., 2022) still apply.

1. Overall, the adoption rates of HTTPS in both the EU countries and globally are still very high with a small increase since Q3 2022. This shows that HTTPS is a well-supported and mature technology, and is already considered the default for web services.
2. On the other hand, HTTP/3 shows a low adoption rate in the EU, which is less than half of the global one. Furthermore, the HSTS adoption rate in the EU slightly dropped in Q1 2023.
3. Country-wise, there were no major differences in individual country adoption rates between Q3 and Q1 2023 and the vast majority of countries saw minor increases or decreases in all standards. The exceptions in the EU are Luxembourg with 14.9pp increase in HTTPS, and Bulgaria with 29.2pp decrease in HTTP/3.
4. A security-related remark from the Q1 2022 report was that, even though gQUIC is insecure due to QUIC Crypto (Langley and Chang, 2016), it was still adopted in some of the top 10M websites ($\sim$7%). According to Q-Success data (Q-Success, n.d.g), this support rate actually increased in Q1 2023 to $\sim$8.7%, exposing more websites and end-users to known vulnerabilities.
5. For the first time, we present our data on the adoption rates in EU MSs, which coincide with those reported by Q-Success for HTTPS and HTTP/3. On the contrary, for HSTS, our results show a higher adoption rate in the EU of around 11pp.

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.

Abu-Nimeh, S. and Nair, S., ‘Bypassing security toolbars and phishing filters via dns poisoning’, In ‘IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference’, IEEE. ISSN 1930-529X, pp. 1–6. .

Adams, C., Farrell, S., Kause, T. and Mononen, T., ‘Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)’. RFC 4210 (Proposed Standard), Sep. 2005. URL http://www.ietf.org/rfc/rfc4210.txt. Updated by RFC 6712.

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.

Alexa, ‘Top sites’. n.d. URL https://www.alexa.com/topsites. Last visited 20/09/2021.

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

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

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

APNIC, ‘Use of DNSSEC Validation for World’. b. 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.

April King, ‘Analysis of the Alexa Top 1M sites (April 2019)’. 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.

Atkins, D. and Austein, R., ‘Threat Analysis of the Domain Name System (DNS)’. RFC 3833, Aug. 2004. . URL https://rfc-editor.org/rfc/rfc3833.txt.

Barnes, R., Thomson, M., Pironti, A. and Langley, A., ‘Deprecating Secure Sockets Layer Version 3.0’. RFC 7568, Jun. 2015. . URL https://rfc-editor.org/rfc/rfc7568.txt.

Bishop, M., ‘HTTP/3 and QUIC: Past, Present, and Future’. 2021a. URL https://www.akamai.com/blog/performance/http3-and-quic-past-present-and-future. Last visited 03/11/2021.

Bishop, M., ‘Hypertext Transfer Protocol Version 3 (HTTP/3)’, Internet-Draft draft-ietf-quic-http-34, Internet Engineering Task Force, Feb. 2021b. URL https://datatracker.ietf.org/doc/html/draft-ietf-quic-http-34. Work in Progress.

Buchanan, W. J., Helme, S. and Woodward, A., ‘Analysis of the adoption of security headers in HTTP’, *IET Information Security*, Vol. 12, No 2, Oct. 2017, pp. 118–126. ISSN 1751-8717. Publisher: IET Digital Library.

Can I use, ‘HTTP/3 protocol’. n.d.a. URL https://caniuse.com/http3. Last visited 26/11/2021.

Can I use, ‘Strict Transport Security’. n.d.b. URL https://caniuse.com/stricttransportsecurity. Last visited 26/11/2021.

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

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W., ‘Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile’. RFC 5280 (Proposed Standard), May 2008. URL http://www.ietf.org/rfc/rfc5280.txt. Updated by RFC 6818.

Crispin, M., ‘INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1’. RFC 3501 (Proposed Standard), Mar. 2003. URL http://www.ietf.org/rfc/rfc3501.txt. Updated by RFCs 4466, 4469, 4551, 5032, 5182, 5738, 6186, 6858, 7817.

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.

curl.se, ‘HTTP3 (and QUIC) ’. n.d. URL https://curl.se/docs/http3.html. Last visited 16/02/2023.

Decker, L., ‘QUIC & The Dead: Which of the Most Common IDS/IPS Tools Can Best Identify QUIC Traffic?’, White paper, SANS Institute, 05 2020. URL https://sansorg.egnyte.com/dl/pmKFA7vozH. Accessed on 04.10.2021.

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.

Dierks, T. and Rescorla, E., ‘The Transport Layer Security (TLS) Protocol Version 1.2’. RFC 5246 (Proposed Standard), Aug. 2008. URL http://www.ietf.org/rfc/rfc5246.txt. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685, 7905.

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

Dukhovni, V. and Hardaker, W., ‘The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance’. RFC 7671 (Proposed Standard), Oct. 2015. URL http://www.ietf.org/rfc/rfc7671.txt.

Elkins, M., Torto, D. D., Levien, R. and Roessler, T., ‘MIME Security with OpenPGP’. RFC 3156 (Proposed Standard), Aug. 2001. URL http://www.ietf.org/rfc/rfc3156.txt.

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.

F5, ‘K60235402: Overview of the BIG-IP HTTP/3 and QUIC profiles’. 2020. URL https://support.f5.com/csp/article/K60235402. Last visited 30/11/2021.

Farrell, S. and Tschofenig, H., ‘Pervasive Monitoring Is an Attack’. RFC 7258, May 2014. . URL https://rfc-editor.org/rfc/rfc7258.txt.

Fenton, J., ‘SMTP Require TLS Option’, Internet-Draft draft-fenton-smtp-require-tls-02, Internet Engineering Task Force, Aug. 2016. URL https://tools.ietf.org/html/draft-fenton-smtp-require-tls-02. Work in Progress.

Freed, N. and Borenstein, N., ‘Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples’. RFC 2049 (Draft Standard), Nov. 1996a. URL http://www.ietf.org/rfc/rfc2049.txt.

Freed, N. and Borenstein, N., ‘Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies’. RFC 2045 (Draft Standard), Nov. 1996b. URL http://www.ietf.org/rfc/rfc2045.txt. Updated by RFCs 2184, 2231, 5335, 6532.

Freed, N. and Borenstein, N., ‘Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types’. RFC 2046 (Draft Standard), Nov. 1996c. URL http://www.ietf.org/rfc/rfc2046.txt. Updated by RFCs 2646, 3798, 5147, 6657.

Freed, N., Klensin, J. and Postel, J., ‘Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures’. RFC 2048 (Best Current Practice), Nov. 1996. URL http://www.ietf.org/rfc/rfc2048.txt. Obsoleted by RFCs 4288, 4289, updated by RFC 3023.

Freier, A. O., Karlton, P. and Kocher, P. C., ‘The Secure Sockets Layer (SSL) Protocol Version 3.0’. RFC 6101, Aug. 2011. . URL https://rfc-editor.org/rfc/rfc6101.txt.

G, K., G, K. and JI, S. M., 'Web communication standards: an analysis of uptake in the eu - march 2022', , No KJ-NA-31-276-EN-N (online), 2022. ISSN 1831-9424 (online). .

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

Ghedini, A. and Lalkaka, R., 'HTTP/3: the past, the present, and the future'. 2019. URL https://blog.cloudflare.com/http3-the-past-present-and-future/. Last visited 03/11/2021.

Google, 'Chrome User Experience Report'. URL https://developers.google.com/web/tools/chrome-user-experience-report. Last visited 04/11/2021.

Grigorik, I., 'High performance browser networking: What every web developer should know about networking and web performance', " O'Reilly Media, Inc.", 2013.

Gudmundsson, O., 'Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)'. RFC 7218 (Proposed Standard), Apr. 2014. URL http://www.ietf.org/rfc/rfc7218.txt.

Helme, S., 'Top 1 Million Analysis - March 2020'. 2020. URL https://scotthelme.co.uk/top-1-million-analysis-march-2020/. Last visited 23/11/2021.

Helme, S., 'Top 1 Million Sites Security Analysis'. n.d. URL https://crawler.ninja/. Last visited 23/11/2021.

Hodges, J., Jackson, C. and Barth, A., 'HTTP Strict Transport Security (HSTS)'. RFC 6797, Nov. 2012. . URL https://rfc-editor.org/rfc/rfc6797.txt.

Hoffman, P., 'SMTP Service Extension for Secure SMTP over Transport Layer Security'. RFC 3207 (Proposed Standard), Feb. 2002. URL http://www.ietf.org/rfc/rfc3207.txt. Updated by RFC 7817.

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

Hoffman, P. and Schlyter, J., 'The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA'. RFC 6698 (Proposed Standard), Aug. 2012. URL http://www.ietf.org/rfc/rfc6698.txt. Updated by RFCs 7218, 7671.

Hong, J., 'The state of phishing attacks', *Communications of the ACM*, Vol. 55, No 1, 2012, pp. 74–81. ISSN 0001-0782. . URL http://doi.acm.org/10.1145/2063176.2063197.

HTTP Archive, 'Getting Started Accessing the HTTP Archive with BigQuery'. a. URL https://github.com/HTTPArchive/httparchive.org/blob/main/docs/gettingstarted_bigquery.md. Last visited 05/11/2021.

HTTP Archive, 'Report: State of the Web - HTTP/3 Support'. b. URL https://httparchive.org/reports/state-of-the-web#h3.

HTTP Archive, 'Web Almanac - HTTP Archive's annual state of the web report'. c. URL https://almanac.httparchive.org/en/2020/. Last visited 04/11/2021.

IETF, 'Innovative New Technology for Sending Data Over the Internet Published as Open Standard'. URL https://www.ietf.org/blog/innovative-new-technology-for-sending-data/. Last visited 03/11/2021.

Internet Architecture Board, 'IAB Statement on Internet Confidentiality'. 2014. URL https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/. Last visited 23/11/2021.

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.

Joras, M. and Chi, Y., 'How Facebook is bringing QUIC to billions'. 2020. URL https://engineering.fb.com/2020/10/21/networking-traffic/how-facebook-is-bringing-quic-to-billions/. Last visited 03/11/2021.

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.

Karopoulos, G., Geneiatakis, D. and Kambourakis, G., 'Neither good nor bad: A large-scale empirical analysis of http security response headers', In 'Trust, Privacy and Security in Digital Business', , edited by S. Fischer-Hübner, C. Lambrinoudakis, G. Kotsis, A. M. Tjoa, and I. KhalilSpringer International Publishing, Cham. ISBN 978-3-030-86586-3, pp. 83–95.

Karopoulos, G., Kambourakis, G., Spigolon, R. and Sanchez, I., 'Web communication standards: an analysis of uptake in the eu - september 2022', *Publications Office of the European Union*, 2022.

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.

Klensin, J., 'Simple Mail Transfer Protocol'. RFC 5321 (Draft Standard), Oct. 2008. URL `http://www.ietf.org/rfc/rfc5321.txt`. Updated by RFC 7504.

Kranch, M. and Bonneau, J., 'Upgrading HTTPS in mid-air: An Empirical Study of Strict Transport Security and Key Pinning', In 'Proceedings 2015 Network and Distributed System Security Symposium', Internet Society, San Diego, CA. ISBN 978-1-891562-38-9.

Kucherawy, M., 'Email Authentication Status Codes'. RFC 7372 (Proposed Standard), Sep. 2014. URL `http://www.ietf.org/rfc/rfc7372.txt`.

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`.

Langley, A. and Chang, W.-T., 'QUIC Crypto'. 2016. URL `https://docs.google.com/document/d/1g5nIXAIkN_Y-7XJW5K45IblHd_L2f5LTaDUDwvZ5L6g/edit#`. Last visited 25/11/2021.

Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., Yang, F., Kouranov, F., Swett, I., Iyengar, J., Bailey, J., Dorfman, J., Roskind, J., Kulik, J., Westin, P., Tenneti, R., Shade, R., Hamilton, R., Vasiliev, V., Chang, W.-T. and Shi, Z., 'The quic transport protocol: Design and internet-scale deployment', In 'Proceedings of the Conference of the ACM Special Interest Group on Data Communication', SIGCOMM '17. Association for Computing Machinery, New York, NY, USA. ISBN 9781450346535, p. 183–196. . URL `https://doi.org/10.1145/3098822.3098842`.

Lavrenovs, A. and Melón, F. J. R., 'HTTP security headers analysis of top one million websites', In '2018 10th International Conference on Cyber Conflict (CyCon)', pp. 345–370.

Margolis, D., Risher, M., Lidzborski, N., Chuang, W., Long, B., Ramakrishnan, B., Brotman, A., Jones, J., Martin, F., Umbach, K. and Laber, M., 'SMTP MTA Strict Transport Security', Internet-Draft draft-ietf-uta-mta-sts-01, Internet Engineering Task Force, Jul. 2016a. URL `https://tools.ietf.org/html/draft-ietf-uta-mta-sts-01`. Work in Progress.

Margolis, D., Risher, M., Lidzborski, N., Chuang, W., Long, B., Ramakrishnan, B., Brotman, A., Jones, J., Martin, F., Umbach, K. and Laber, M., 'SMTP Strict Transport Security', Internet-Draft draft-margolis-smtp-sts-00, Internet Engineering Task Force, Mar. 2016b. URL `https://tools.ietf.org/html/draft-margolis-smtp-sts-00`. Work in Progress.

Mayzin Han, 'Google, Microsoft, Apple and Mozilla deprecate support of TLS 1.0 and 1.1: What this means for your CRM'. 2020. URL `https://www.columbusglobal.com/en-gb/blog/google-microsoft-apple-and-mozilla-deprecate-support-of-tls-what-this-means-for-your-crm`. Last visited 19/11/2021.

Melnikov, A., 'Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols'. RFC 7817 (Proposed Standard), Mar. 2016. URL `http://www.ietf.org/rfc/rfc7817.txt`.

Microsoft, 'Disabling TLS 1.0 and 1.1 for Microsoft 365'. 2021. URL `https://docs.microsoft.com/en-us/microsoft-365/compliance/tls-1.0-and-1.1-deprecation-for-office-365?view=o365-worldwide`. Last visited 19/11/2021.

Moore, K., 'MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text'. RFC 2047 (Draft Standard), Nov. 1996. URL `http://www.ietf.org/rfc/rfc2047.txt`. Updated by RFCs 2184, 2231.

Moore, K. and Newman, C., 'Mail User Agent Strict Transport Security (MUA-STS)', Internet-Draft draft-ietf-uta-email-deep-05, Internet Engineering Task Force, Jul. 2016. URL `https://tools.ietf.org/html/draft-ietf-uta-email-deep-05`. Work in Progress.

Myers, J. and Rose, M., 'Post Office Protocol - Version 3'. RFC 1939 (INTERNET STANDARD), May 1996. URL `http://www.ietf.org/rfc/rfc1939.txt`. Updated by RFCs 1957, 2449, 6186.

Nielsen, H., Mogul, J., Masinter, L. M., Fielding, R. T., Gettys, J., Leach, P. J. and Berners-Lee, T., 'Hypertext Transfer Protocol – HTTP/1.1'. RFC 2616, Jun. 1999. . URL https://rfc-editor.org/rfc/rfc2616.txt.

Nordström, O. and Dovrolis, C., 'Beware of bgp attacks', *SIGCOMM Computer Communication Review*, Vol. 34, No 2, 2004, pp. 1–8. ISSN 0146-4833. . URL http://doi.acm.org/10.1145/997150.997152.

OWASP, 'OWASP Top Ten'. n.d.a. URL https://owasp.org/www-project-top-ten/. Last visited 19/11/2021.

OWASP, 'Secure Headers Project'. n.d.b. URL https://owasp.org/www-project-secure-headers/. Last visited 19/11/2021.

Patrick Nohe, 'Twitter will deprecate support for TLS 1.0, TLS 1.1 on July 15'. 2015. URL https://www.thesslstore.com/blog/twitter-will-deprecate-support-for-tls-1-0-tls-1-1-on-july-15/. Last visited 22/11/2021.

Petrov, I., Peskov, D., Coard, G., Chung, T., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A. and Wilson, C., 'Measuring the Rapid Growth of HSTS and HPKP Deployments', 2017, p. 7.

Q-Success, 'Usage of HTTP/3 broken down by server locations'. a. URL https://w3techs.com/technologies/breakdown/ce-http3/server_location. Last visited 23/11/2021.

Q-Success, 'Usage statistics of HTTP/3 for websites'. b. URL https://w3techs.com/technologies/details/ce-http3. Last visited 04/11/2021.

Q-Success, 'Usage of Default protocol https broken down by server locations'. n.d.a. URL https://w3techs.com/technologies/breakdown/ce-httpsdefault/server_location. Last visited 23/11/2021.

Q-Success, 'Usage of HTTP Strict Transport Security broken down by server locations'. n.d.b. URL https://w3techs.com/technologies/breakdown/ce-hsts/server_location. Last visited 24/11/2021.

Q-Success, 'Usage statistics of Default protocol https for websites'. n.d.c. URL https://w3techs.com/technologies/details/ce-httpsdefault. Last visited 23/11/2021.

Q-Success, 'Usage statistics of Default protocol https for websites'. n.d.d. URL https://w3techs.com/technologies/details/ce-httpsdefault. Last visited 03/11/2021.

Q-Success, 'Usage statistics of HTTP Strict Transport Security for websites'. n.d.e. URL https://w3techs.com/technologies/details/ce-hsts. Last visited 24/11/2021.

Q-Success, 'Usage statistics of HTTP/3 for websites'. n.d.f. URL https://w3techs.com/technologies/details/ce-http3. Last visited 23/11/2021.

Q-Success, 'Usage statistics of QUIC for websites'. n.d.g. URL https://w3techs.com/technologies/details/ce-quic. Last visited 25/11/2021.

Q-Success, 'W3Techs - World Wide Web Technology Surveys'. n.d.h. URL https://w3techs.com/. Last visited 23/11/2021.

Qualys, 'SSL Pulse'. n.d. URL https://www.ssllabs.com/ssl-pulse/. Last visited 26/11/2021.

QUIC WG, 'Charter for Working Group'. n.d. URL https://datatracker.ietf.org/wg/quic/about/.

Ramsdell, B. and Turner, S., 'Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling'. RFC 5750 (Proposed Standard), Jan. 2010. URL http://www.ietf.org/rfc/rfc5750.txt.

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. and Modadugu, N., 'Datagram Transport Layer Security Version 1.2'. RFC 6347, Jan. 2012. . URL https://www.rfc-editor.org/info/rfc6347.

Risher, M., Jones, J., Ramakrishnan, B., Brotman, A. and Margolis, D., 'SMTP TLS Reporting', Internet-Draft draft-ietf-uta-smtp-tlsrpt-02, Internet Engineering Task Force, Dec. 2016a. URL https://tools.ietf.org/html/draft-ietf-uta-smtp-tlsrpt-02. Work in Progress.

Risher, M., Margolis, D., Ramakrishnan, B., Brotman, A. and Jones, J., 'SMTP MTA Strict Transport Security (MTA-STS)', Internet-Draft draft-ietf-uta-mta-sts-02, Internet Engineering Task Force, Dec. 2016b. URL https://tools.ietf.org/html/draft-ietf-uta-mta-sts-02. Work in Progress.

Santesson, S., Nystrom, M. and Polk, T., 'Internet X.509 Public Key Infrastructure: Qualified Certificates Profile'. RFC 3739 (Proposed Standard), Mar. 2004. URL http://www.ietf.org/rfc/rfc3739.txt.

Shodan, 'TLS 1.0/ 1.1 Usage Report'. URL https://beta.shodan.io/search/report?query=http%20ssl.version%3Atlsv1.0%2Ctlsv1.1&title=TLS%201.0/%201.1%20Usage%20Report. Last visited 22/11/2021.

Tranco, 'A Research-Oriented Top Sites Ranking Hardened Against Manipulation'. n.d. URL https://tranco-list.eu. Last visited 20/09/2021.

Trevisan, M., Giordano, D., Drago, I. and Khatouni, A. S., 'Measuring http/3: Adoption and performance'. 2021.

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.

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.

White House Office of Management and Budget, 'The HTTPS-Only Standard'. n.d. URL https://https.cio.gov/. Last visited 23/11/2021.

Wireshark, 'Wireshark 3.4.9 Release Notes'. 2021. URL https://www.wireshark.org/docs/relnotes/wireshark-3.4.9.html. Last visited 30/11/2021.

Yee, P., 'Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile'. RFC 6818 (Proposed Standard), Jan. 2013. URL http://www.ietf.org/rfc/rfc6818.txt.

Yoshibumi Suematsu, 'APNIC - Why has DNSSEC increased in some economies and not others?' 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'. 2020. URL https://www.zdnet.com/article/china-is-now-blocking-all-encrypted-https-traffic-using-tls-1-3-and-esni/. Last visited 26/11/2021.

List of abbreviations and definitions

DNS Domain Name System

EC European Commission

EU European Union

HSTS HTTP Strict Transport Security

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

MS Member State

TLS Transport Layer Security

WWW World Wide Web

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.

Publications Office
of the European Union