ISSN 1831-9424

European Commission

JRC TECHNICAL REPORT

Internet Standards: Email communication security standards - an analysis of uptake in the EU

Kouliaridis, V.
Sanchez, I.

September 2023

Joint Research Centre

EUR 31722 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

JRC135301

EUR 31722 EN

PDF ISBN 978-92-68-08763-3 ISSN 1831-9424 doi:10.2760/032699 KJ-NA-31-722-EN-N

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: Kouliaridis, V. and Sanchez Martin, J.I., *Internet Standards: Email communication security standards - an analysis of uptake in the EU*, September 2023, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/032699, JRC135301.

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

Ensuring the interoperability and security of email communications is one of the cornerstones of a resilient and open Internet. In this context, the wide adoption of key Internet security standards, such as StartTLS, SPF, DKIM, DMARC, DANE and DNSSEC, is essential for a safe cyberspace for everyone. This report assesses the level of uptake of the above set of standards in Q3 2023 across EU Member States, comparing it to the global status. The analysis uses data from publicly available data sources and assessment tools, as well as from measurements conducted by the European Commission's Joint Research Centre. Our findings show that the average level of adoption of all standards is similar to the previous measurement period (Q1 2023), with StartTLS, SPF and DKIM having high adoption rates in the EU (ranging from around 84 to 97%), DMARC following with medium adoption (around 66%), and DANE with DNSSEC showing very low uptake, between 1 and 5% respectively.

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 ways to systematically monitor the deployment evolution of email communications security standards to identify gaps and barriers for their adoption, and evaluate the need for regulatory measures to promote their uptake.

Email communications need to be protected because of the vast number of email messages exchanged daily and also the sensitivity of the information frequently contained in them. Moreover, the email system often plays a central role in the processes linked to the online identity of users (e.g., email addresses used as usernames, email-based password resets or second factor authentication via email). The adoption of Internet standards designed to secure email communications is therefore an important step to protect Internet users and contribute to ensure the scalability, stability, and security of the Internet.

The aim of this report is to assess the level of uptake of the set of Internet standards relevant for the protection of email communications, analysing their level of adoption across EU Member States (MSs) as well as globally. This analysis is based both on publicly available data and a set of measurements carried out with a variety of tools, namely, the My Email Communications Security Assessment (MECSA) and its standalone, open source version 'mecsa-st' both developed by the Joint Research Centre. The analysis is complemented by an additional third-party, open-source measurement tool, namely the 'internet.nl' platform.

Figure 1 provides an overview of the adoption of email security standards in the EU using mecsa-st and internet.nl in Q3 2023, showing similar trends to Q1 2023, with a small increase in the case of StartTLS, DMARC, and DKIM. This figure presents a selection of the indicators that can be found in the report, where further analysis is provided.

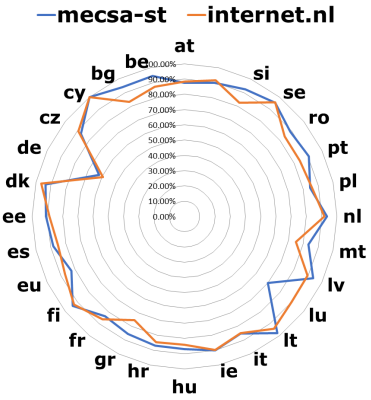
The results show a very high adoption for Sender Policy Framework (SPF), as presented in Figure 1b, where almost all EU MSs have a rate of above 85%. In addition, almost all of them implement a strict SPF policy. These figures are slightly higher than that of non-EU countries; also they are slightly higher compared to Q1 and Q3 2023.

DomainKeys Identified Mail (DKIM) is also well supported both in the EU and globally with support rates of above 87% and 81% for all countries in EU and non-EU countries, respectively, showing a +14 percentage point increase in the EU average since Q1 2023. Figure 1c depicts the DKIM support rates per EU MS. Even though there are slight differences from one measurement tool to the other, the trend is increasing and similar to Q1 2023.

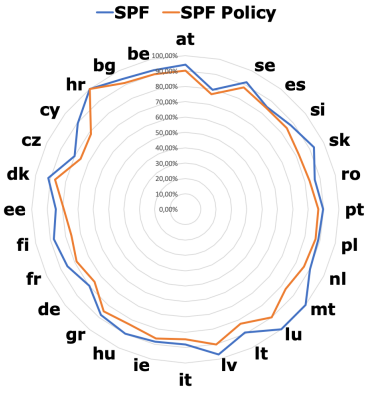
Regarding Domain-based Message Authentication, Reporting and Conformance (DMARC), its adoption is medium with an average of around 63% in the EU and 59% in non-EU countries. Compared to Q1 2023 there is a noteworthy increase of 14 percentage points in the EU average and an increase of 5 percentage points in the non-EU average. It is also evident that the support of DMARC strict policies is very far from the support of the DMARC protocol itself. The support rates for each EU MS are presented in Figure 1d.

The support of DNS-based Authentication of Named Entities (DANE) is almost 0% most of the EU Member States. Similarly, low support rates are also observed in non-EU countries. These results follow the low adoption rates of Domain Name System Security Extensions (DNSSEC), since the latter is a prerequisite for implementing DANE. Figure 1e depicts the adoption rates of both DANE and DNSSEC in the EU MSs. These results are similar to those reported in Q1 2023.

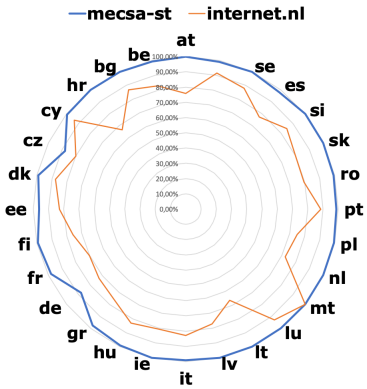
A summary of the average adoption rates of the reviewed email communication standards in EU and non-EU countries is presented in Figure 2. Here all three measurement tools were used as follows: MECSA for measuring global standards adoption, mecsa-st for EU and non-EU average adoption, and internet.nl for EU and non-EU average adoption.



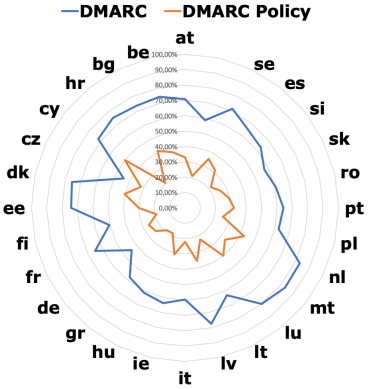
(a) StartTLS support



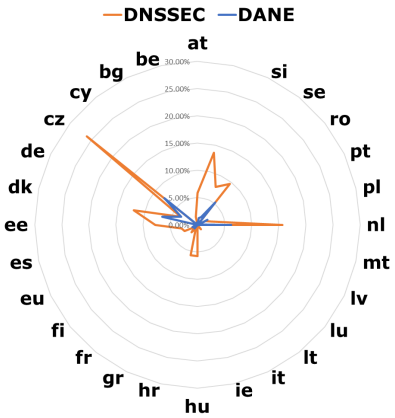
(b) SPF support using the mecsa-st tool



(c) DKIM support



(d) DMARC support using the mecsa-st tool



(e) DANE and DNSSEC support using the mecsa-st tools

Figure 1: Email security standards adoption in the EU in Q3 2023 using mecsa-st and internet.nl measurement tools

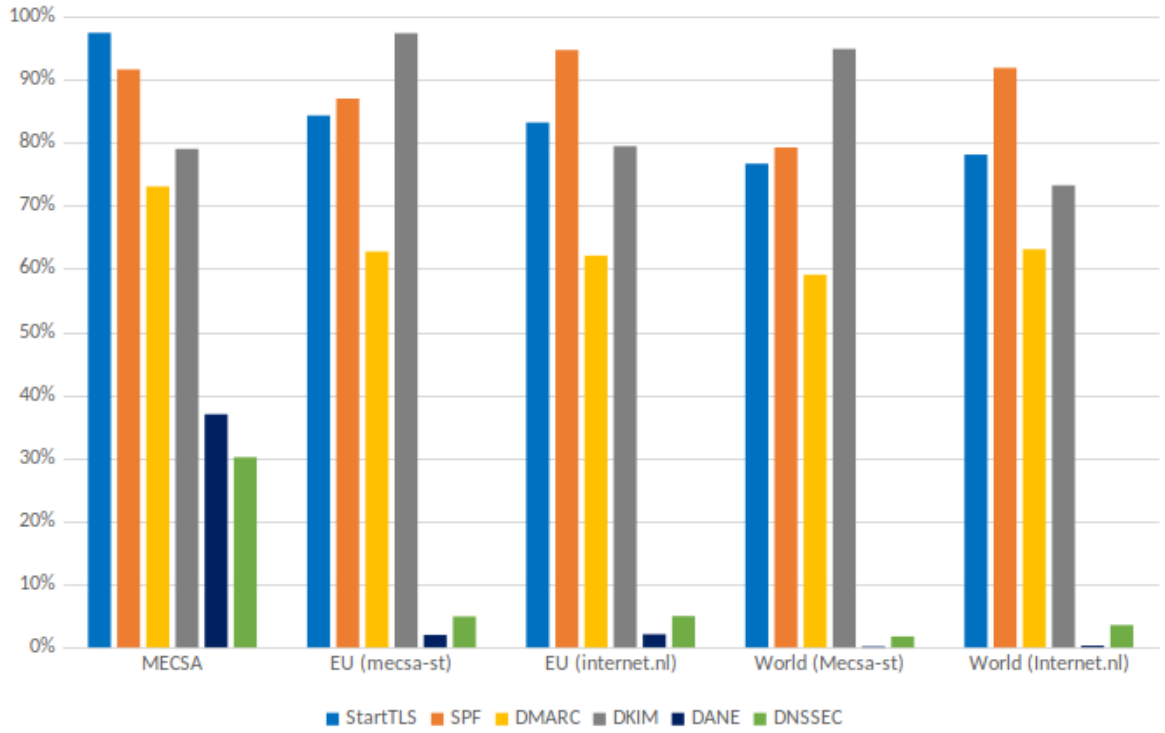


Figure 2: Email security standards adoption rates in Q3 2023 using a variety of measurement tools

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 email communication security standards used for protecting the exchange of email messages between email providers and measuring their level of adoption in European Union (EU) Member States (MSs). Email protocols were initially designed under the assumption that email servers and communication channels could be trusted and, thus, no security mechanisms were implemented. In order to mitigate the security issues caused by the lack of such mechanisms, a series of email security protocols have been proposed over the years: StartTLS, Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) and DNS-Based Authentication of Named Entities (DANE). The current level of adoption of email security standards by email providers is far from ideal. The results of a survey campaign that the Joint Research Centre (JRC) conducted in 2018 (Sanchez Martin and Draper Gil, 2019) and 2019 (Kambourakis et al., 2020), and more recently by other researchers (Lange et al., 2023) revealed serious gaps in the adoption of modern email security standards in the global email ecosystem.

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 email communication security standards used in the EU and globally. The previous report concerned Q1 2023 (Karopoulos et al., 2023), whereas this one presents results for Q3 2023. Similarly as the previous version, this report is based on open data and own measurements, performed at the JRC, and presents results and analysis of the adoption rates of StartTLS, SPF, DKIM, DMARC

and DANE. The key observations from Q1 2023 were that there is mixed support among these protocols in the EU: StartTLS, SPF and DKIM show high adoption rates (above 70%), DMARC has a medium adoption of around 50% in average, whereas the support of DANE is almost 0%. In most cases the global adoption rate tends to be lower than the EU average. Current measurements for Q3 2023 report similar figures in all cases, with increased adoption rates in the cases of StartTLS, DMARC, and DKIM.

The report is organised as follows. Section 2 describes the data sources and methodology used to collect the measurements. Section 3 presents the data analysis divided into subsections for the different standards, i.e., StartTLS, SPF, DKIM, DMARC and DANE. Finally, Section 4 concludes the report.

2 Data sources and methodology

2.1 Data sources

The set of external data sources used in the analysis of the uptake of email security standards in Q3 2023 is described in Table 1; these are the same sources used in the previous version of this report for Q1 2023.

Firstly, our analysis uses for reference purposes the detailed anonymised results of the analysis carried out in the email assessment requests received by the My Email Communications Security Assessment (MECSA) platform during a period covering roughly Q1 2023, and more specifically from 02/02/2023 and 16/06/2023. MECSA is an online tool designed and maintained by the JRC to assess the protection of email communications between email providers. It evaluates the capacity of email providers to secure email communications by analysing their usage of modern email security standards. MECSA analyses the support for StartTLS with X.509 certificates, SPF, DKIM, DMARC, DANE and DNSSEC, for the inbound and outbound services.

Secondly, we use a sub-list of domains contained in the "Email Encryption in Transit" part of the last edition of the Google Transparency Report to analyse the uptake of the target standards by country, dividing them into two groups: domains with country code Top-Level Domain (ccTLD) of a MS, EU domains, and a set of chosen non-EU ccTLD domains. The Google Transparency Report is a public site where Google publishes data statistics of different Google services, like email or HTTP. Google issued the first transparency report in 2010 and has been updating it regularly with *"[...] data that sheds light on how the policies and actions of governments and corporations affect privacy, security, and access to information online"* (Google, n.d.).

In addition, the Google Transparency Report provides statistics for StartTLS support in email in transit. According to Google([1]), these statistics consider only the cases where Google is only one of the providers involved in the email delivery; moreover, message recipients instead of Simple Mail Transfer Protocol (SMTP) connections are counted. Also, emails that are flagged as spam or inbound messages from hosts whose forward or reverse DNS is missing or inconsistent are not counted.

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

Source	Short description
MECSA data (European Commission, Joint Research Centre, n.d.b, Kambourakis et al., 2020)	Database containing the results of the analysis carried out by the MECSA platform in the last 6 months
Google Transparency Report (Google, n.d.)	Selected (EU and non-EU) ccTLD domains from the Google Transparency report analysed with the mecsa-st and internet.nl tools; StartTLS statistics

2.2 Methodology

We carry out three separate and complementary analyses in our assessment. For reference purposes, we utilise the detailed results obtained by the MECSA platform following the analysis of the total number of domains over the last 6 months. The average of the results for the assessment of each of the target standards (StartTLS, SPF, DMARC, DKIM, DAN, and DNSSEC) are used to compare against those obtained in our analysis of the Google Transparency Report domains. The methodology followed here is the same as in the previous versions of this report for Q1 2023 and is repeated here for the sake of completeness.

Our more in-depth analysis on the uptake of the standards is based on JRC's open source mecsa-st tool([2]) and the internet.nl([3]) service. Using each tool, we analyse the list of email domains obtained from the Google Transparency Report, classifying them based on their ccTLD into two groups EU domains (including .eu) and non-EU domains, for which we selected a groups of non-EU countries.

Internet.nl is an initiative of the Dutch Internet Standards Platform. It checks the implementation of modern Internet Standards for email, web and Internet connection and provides a score, according to how many standards are supported correctly. The internet.nl tests are based on the Internet Standards on the "comply-or-explain" list of the Dutch Standardisation Forum, on the security advice of the Dutch National Cyber Security Centre (NCSC) and on the relevant Request For Comments (RFC) of the Internet Engineering Task Force (IETF).

([1]) https://support.google.com/transparencyreport/answer/7381230?hl=en&ref_topic=7380433
([2]) https://github.com/mecsa/mecsa-st
([3]) https://internet.nl

Mecsa-st is the command line version of the MECSA online tool. It features a reduced version of the MECSA analysis engine limited to inbound tests([4]). Our analysis assesses the email domains under the ccTLDs of the EU MSs, including the '.eu' ccTLD, and a set of selected countries outside EU. In the following, a detailed description on how mecsa-st carries out the relevant tests is provided; the rest of the measurement tools, i.e., MECSA and internet.nl, perform similar tests:

StartTLS. For each Mail Exchanger (MX), an SMTP connection is established and a Transport Layer Security (TLS) communication channel is negotiated. If successful, the provided server certificate and the intermediate certificates are downloaded. During the establishment of the SMTP connection it is checked whether the REQUIRETLS SMTP service extension is announced (in the form of the EHLO keyword value "REQUIRETL"). This extension specifies that a message must be sent over a TLS communication channel. The X.509 certificate is validated checking signatures across the full certificate chain of trust, validating that the root Certification Authority (CA) is trusted and ensuring that the certificate is valid checking the CN and SAN attributes, expiration dates and Certificate Revocation Lists (CRLs).

SPF. Validation that a DNS SPF record exists, checking that the syntax is correct and assessing the default policy value (parameter "all"). A major difference between mecsa-st and internet.nl here is that mecsa-st validates a DNS SPF record only if it is compliant with RFC 7208 (Kitterman, 2014). For example, if an SPF record contains more than 10 include terms, mecsa-st flags it as invalid because it violates the limits set by RFC 7208; internet.nl, on the other hand, considers the SPF record as existing and is, thus, calculated in the final results. For this reason, the SPF adoption results reported by mecsa-st tend to be lower than those of internet.nl.

DKIM. Validation that a DKIM DNS record exists by sending a DNS request to the authoritative DNS servers for the domain tested (NS records), requesting the entry domainkey. If the answer NXDOMAIN is received (instead of NOERROR), the validation fails.

DMARC. Validation that a DNS DMARC record exists, checking that the syntax is correct and assessing the policy value (parameter p=).

DANE. Validation of DANE records for each MX. This test is independent from the DNSSEC test.

DNSSEC. The assessment of DNSSEC is composed of the following checks: (a) Verification that the domain is protected by DNSSEC; (b) Check that both SPF and DMARC records - if present - are protected by DNSSEC; (c) Check that MX records - if present - are protected by DNSSEC and validate their respective domain names and TLS Authentication (TLSA) records.

([4]) Outbound tests are not supported by mecsa-st. These types of tests require the reception of emails from the email domain to be evaluated in order to generate an inbound connection. As a result of this, mecsa-st analysis can only provide a limited analysis of DKIM (without checking the presence of a valid signature) and only assesses StartTLS for inbound communications. More information is available at (European Commission, Joint Research Centre, n.d.a).

3 Current state of adoption of email security protocols

Figure 3 present the penetration rates for each email security protocol grouped by origin. Compared to the previous measurement period, i.e., Q1 2023 (Karopoulos et al., 2023), there is a notable increase of about 14 percentage points in StartTLS adoption in the EU and a similar increase in non-EU countries. Similarly, there is an increase of 14 percentage points in DMARC adoption in the EU and a 5 percentage point increase in non-EU countries. Finally, the same increase, i.e., 14 percentage points, was also observed for DKIM. The rest of the results follow the trends observed in the previous measurement periods. Overall, the remarks and recommendations of the previous reports (Draper-Gill et al., 2022a, Draper-Gill et al., 2022b, Karopoulos et al., 2023) still apply here given the similarities in the deployment results.

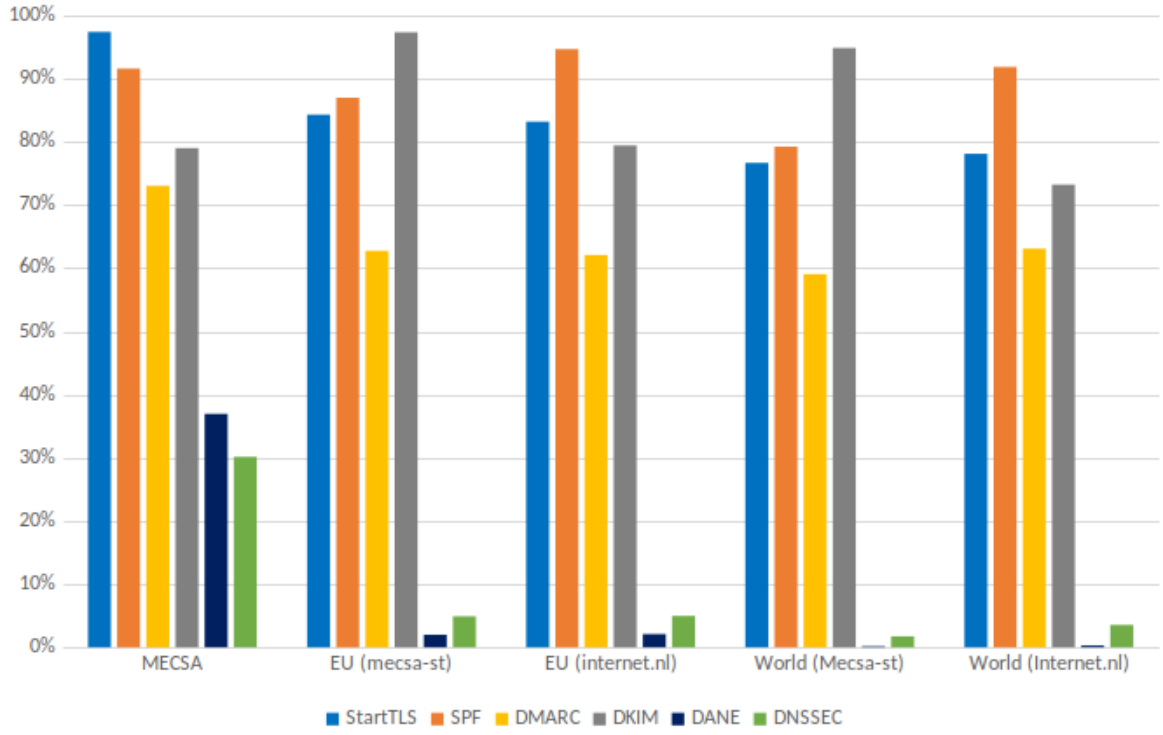


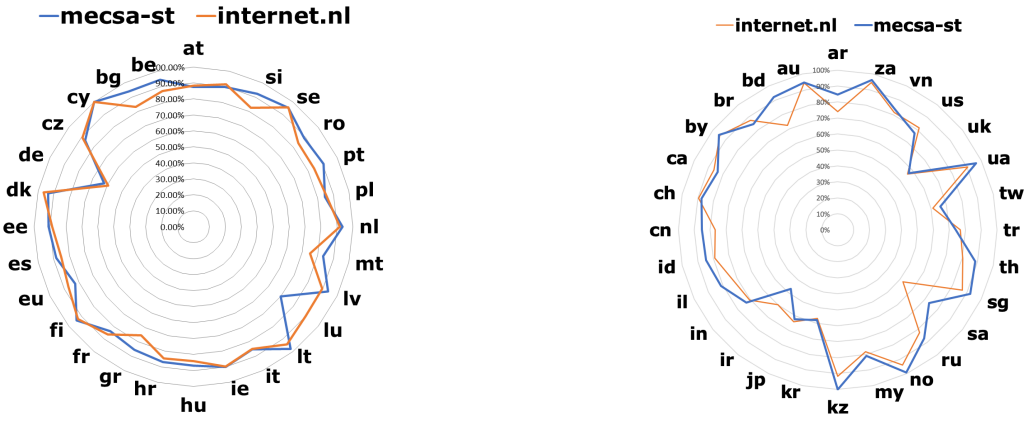
Figure 3: Modern Email Security Standards adoption rates

3.1 StartTLS

Figures 4a and 4b illustrate the StartTLS results by ccTLD, grouped by (a) EU and (b) non-EU ccTLDs, for both mecsa-st and internet.nl tests.

These results are in most cases inline with the previous measurement period, i.e., Q1 2023 (Karopoulos et al., 2023), with some exceptions as follows. There is a significant increase in the EU average of 14 percentage points in the mecsa-st data and 15 percentage points in the internet.nl data. Comparing EU countries, Germany (de) which had an average of 30% in both datasets and a major drop of 14 percentage points in Q1 2023, now shows a 32% increase. Another significant difference in this round of measurements is observed in the case of Malta, which had a decrease of around 17%. These differences are due to that Malta has a very low number of domains of 12 domains. In the vast majority of all other EU MSs the differences were in the order of less than 10 percentage points.

Regarding non-EU countries, the average StartTLS adoption rate has an increase of about 5 and 10 percentage points, in mecsa-st and internet.nl data, respectively. In contrast to the previous measurement periods, the results for the non-EU ccTLD domains show a high support for StartTLS (above 80%) for most of the countries, while the others present a lower support (between 47% and 80%) with United Kingdom (uk), Korea (ca) and Iran (ir) having a low support for StartTLS ($<$60%). One major difference between the two measurement tools is observed in the case of Saudi Arabia (sa), which scores 73% with mecsa-st and 52% with internet.nl. With respect to the last measurement period, a significant increase ($>$ 20 percentage points) was noted in the fol-



(a) EU ccTLD domains

(b) Non-EU ccTLD domains

Figure 4: StartTLS adoption

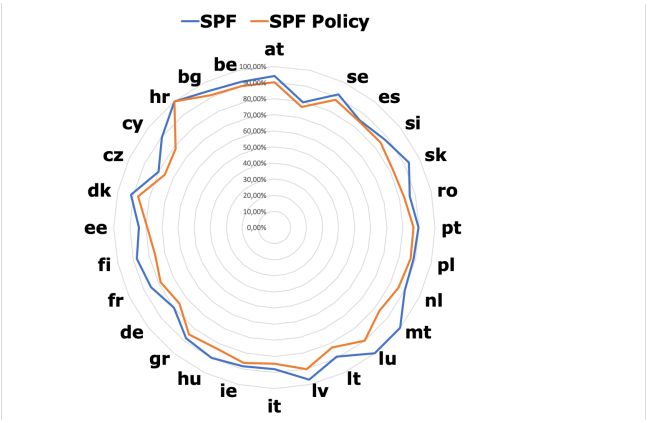
lowing countries: Canada (40.72 percentage points), whereas a drop of 37 percentage points was noted in the previous report, i.e., Q1 2023, United Kingdom (27.47 percentage points), China (25 percentage points), and the United States (23.53 percentage points). The rest of the results are comparable with the previous measurement periods with small differences.

In general, the EU ccTLDs domains have a support rate greater than the one related to non-EU ccTLDs of about 7 percentage points; this gap, however, is bridged given the fact that in Q3 2022 this difference was around 20 percentage points. The MECSA web platform shows a bit higher adoption rates of about 13 percentage points but these results are not directly comparable, as MECSA uses a much limited set of domains.

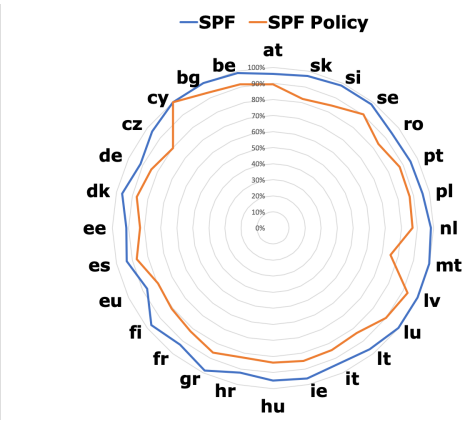
3.2 SPF

Figures 5a and 5b depict the adoption rate of the SPF protocol and strict SPF policy for EU domains obtained with mecsa-st and internet.nl, respectively. As in the last measurement period, most EU ccTLD domains continue to have values of SPF adoption around 90% with almost all of them implementing a strict SPF policy. With reference to the mecsa-st dataset, there is a slight decrease in the EU average for SPF adoption and for the implementation of strict SPF policy (-3 percentage points in both cases), reaching 87% and 82%, respectively. The internet.nl dataset also shows a slight decrease of 1 percentage point in the EU average for SPF adoption and 1 percentage point for the implementation of strict SPF policy, reaching 96 and 86% respectively. Overall, the results for SPF support obtained in mecsa-st are in general slightly lower that the ones obtained with the internet.nl tool. This situation is depicted in Figure 5c, whereas the results for SPF policy support are quite similar (Figure 5d). Regarding the single countries, it is worth mentioning that again in this measurement period Malta experienced a significant difference in its SPF policy support rate: in mecsa-st the rate increased to 83% (+16 percentage points), while an increase was also observed in the result of internet.nl (+8 percentage points compared to the previous measurement period). A similar situation is observed in Luxembourg (lu) in SPF policy, where in both tools support rates decreased to 90% (+23 percentage points). Such differences can be explained considering that the number of domains tested for Malta and Luxembourg is quite low, i.e., 6 and 3, respectively; moreover, the 3 Luxembourgian domains of Q1 2023 are different from the 3 domains checked in Q3 2023. It could therefore be the case that a change in a single or a small number of domains could result in major differences in support rate percentages.

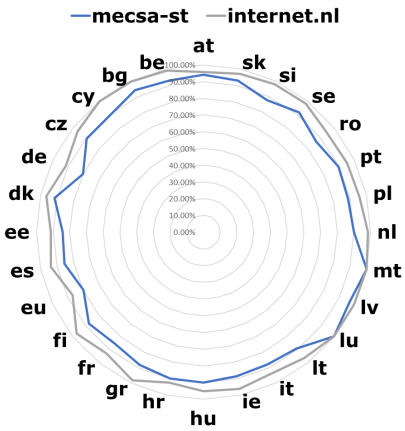
The average adoption rate of SPF and strict SPF policy for non-EU domains is around 70 and 76% respectively, with a small increase in the order of 10 and 7 percentage points, respectively compared to Q1 2023. Figures 6a and 6b present the adoption rate of the SPF protocol and strict SPF policy for non-EU domains obtained with mecsa-st and internet.nl, respectively. The results are similar to the ones obtained in the last measurement period, with the exception of China (cn) and Canada (ca), with an increase of 25 and 40 percentage points in SPF according to mecsa-st, respectively. Also, as shown in Figure 6c, SPF support is in general higher in the internet.nl results, whereas with reference to Figure 6d, the results for SPF policy support are identical.



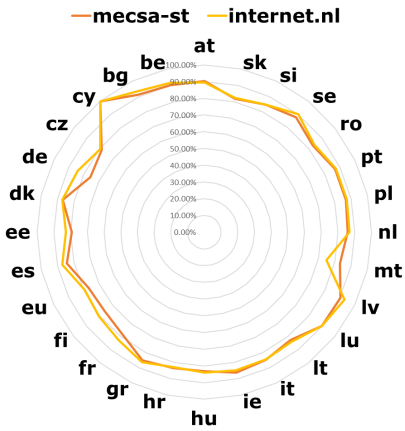
(a) mecsa-st EU ccTLD domains



(b) internet-nl EU ccTLD domains

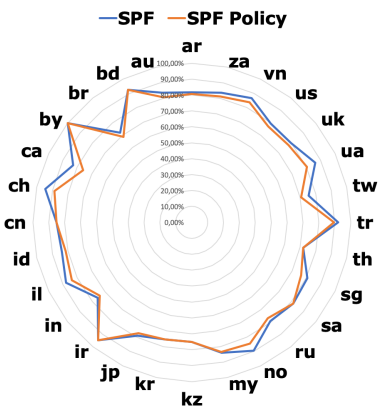


(c) SPF EU ccTLD domains

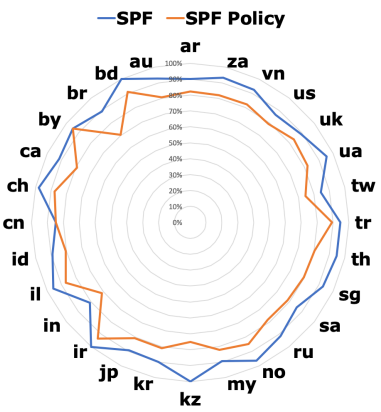


(d) SPF Policy EU ccTLD domains

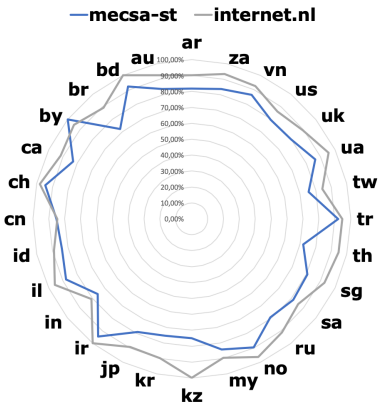
Figure 5: SPF and SPF strict policy adoption in EU



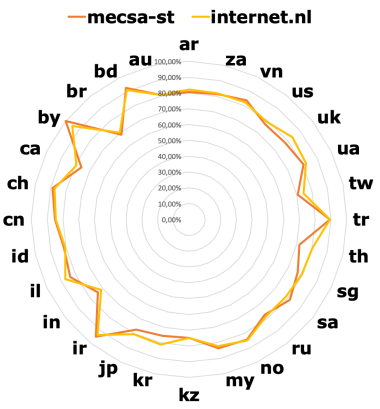
(a) mecsa-st non-EU ccTLD domains



(b) internet-nl non-EU ccTLD domains

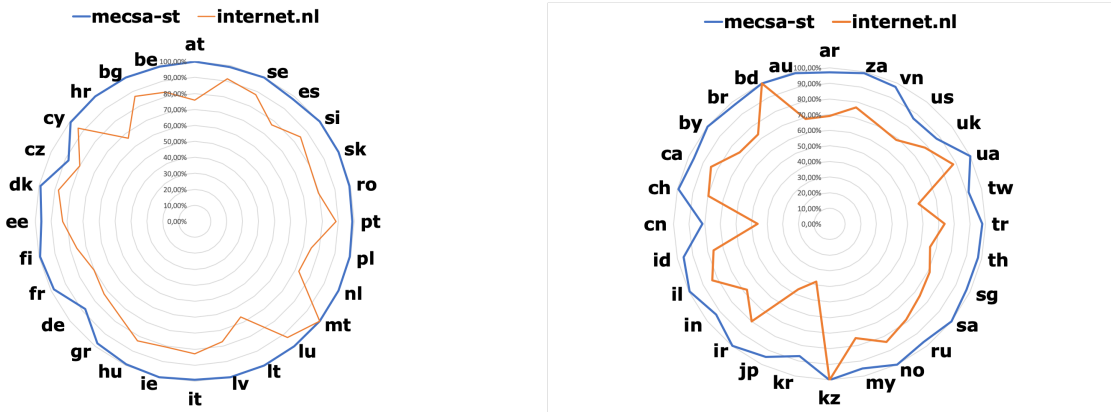


(c) SPF non-EU ccTLD domains



(d) SPF Policy non-EU ccTLD domains

Figure 6: SPF and SPF strict policy adoption in non-EU ccTLD domains



(a) EU ccTLD domains

(b) non-EU ccTLD domains

Figure 7: DKIM adoption

3.3 DKIM

Figures 7a and 7b present the adoption rate results for DKIM, grouped by ccTLD (both for EU and non-EU domains). The results from mecsa-st and internet.nl are almost identical for both EU and non-EU ccTLD domains.

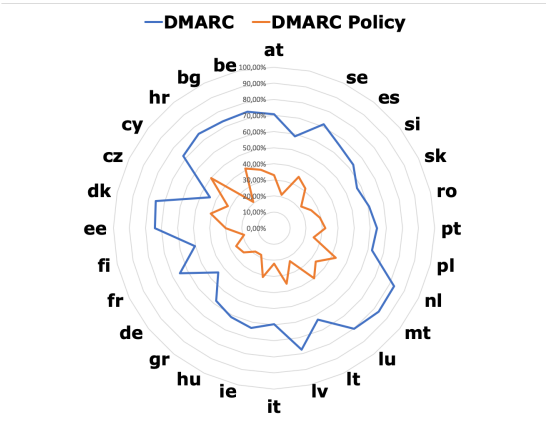
The average calculated for EU from both tools differs (97% in mecsa-st and 79% in internet.nl), with an increase of 14 percentage points for mecsa-st and a decrease of 4 percentage points for internet.nl, respectively compared to the previous measurement period. Regarding individual EU countries, most of them experienced a small increase in support rate and show a DKIM support rate between 87% and 100%.

Similarly, for non-EU countries, the results of each tool differs (95% in mecsa-st and 73% in internet.nl), with an increase of about 18 percentage point for mecsa-st and a decrease of 2% for internet.nl, compared to Q1 2023. When looking at the results of mecsa-st, there are no major outliers. In contrast, in the results obdained by internet.nl, major outliers are South Korea (kr) with 38%, China (cn) with 46%, and Japan (jp) with 47% support rate. It is important to note that, regarding the differences between the MECSA web platform data and the data obtained with mecsa-st, mecsa-st tests cannot fully evaluate the support of DKIM. Precisely, the results of the MECSA web platform are similar to those of internet.nl.

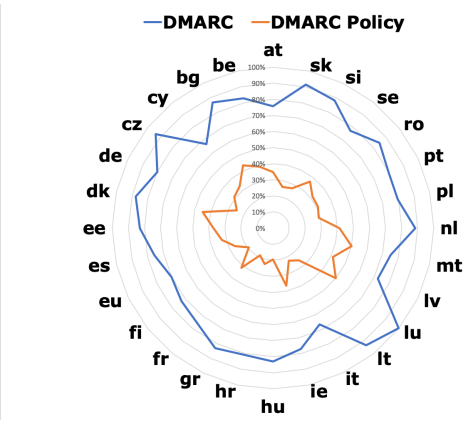
3.4 DMARC

Figures 8a and 8b, illustrate the adoption rate results for DMARC and DMARC strict policy adoption for EU ccTLDs as obtained with the mecsa-st and internet.nl tools, respectively. Similarly, Figures 9a and 9b show the relevant adoption rate results for non-EU ccTLDs. The results from mecsa-st and internet.nl are almost identical for both EU and non-EU ccTLD domains.

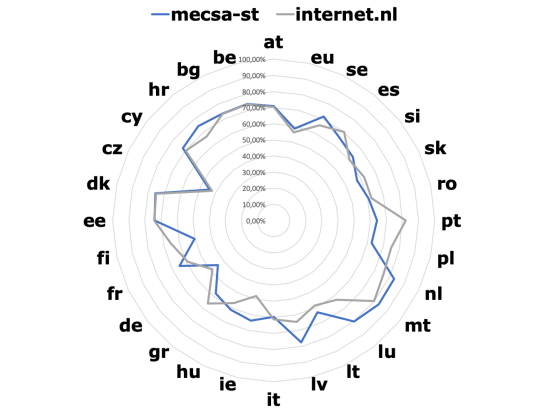
It is observed that the DMARC support among EU MSs remains low, but with a notable increase of around 14 percentage points in the adoption rate since Q1 2023. More specifically, the EU average from the mecsa-st dataset increased to 63% (+14 percentage points) and the DMARC policy rate increased to 28% (+7 percentage points). The EU average for DMARC from the internet.nl dataset increased to 62% (+12 percentage points) and the DMARC policy rate increased to 30% (+6 percentage point). Luxemburg (lu), Malta (mt), and the Netherlands (nl) lead with adoption rates over 80%, although there is quite a difference between their DMARC support rates and their DMARC policy rates (around 40 to 50%). On the opposite side of the ranking, Germany (de) continues to lag behind with an adoption rate of 44%, increased from 19% in Q1 2023. Compared to the previous measurement period, and without considering MSs with a very low number (< 50) of domains such as Cyprus, Malta, and Luxembourg, Germany (de) had an increase of 25 percentage points and Estonia (ee) an increase of 13 percentage points in DMARC support, whereas Slovenia (fi) had the biggest drop of around -6 percentage points in DMARC support; Similar results are observed in both tools. As seen from the EU MSs, the support for strict policies (between 19 and 50%) are still quite far from that of the DMARC support. Figures 8c and 8d present the DMARC and DMARC policy support rates for EU MSs, where a few deviations are observed between the results collected with the two tools.



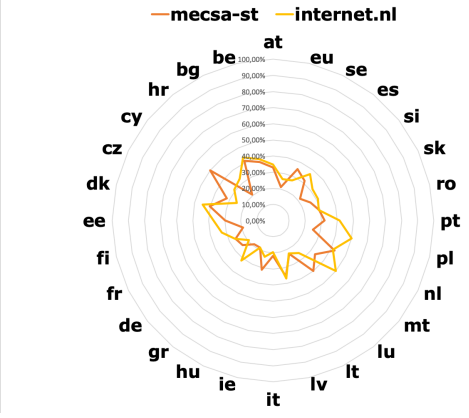
(a) mecsa-st EU ccTLD domains



(b) internet-nl EU ccTLD domains

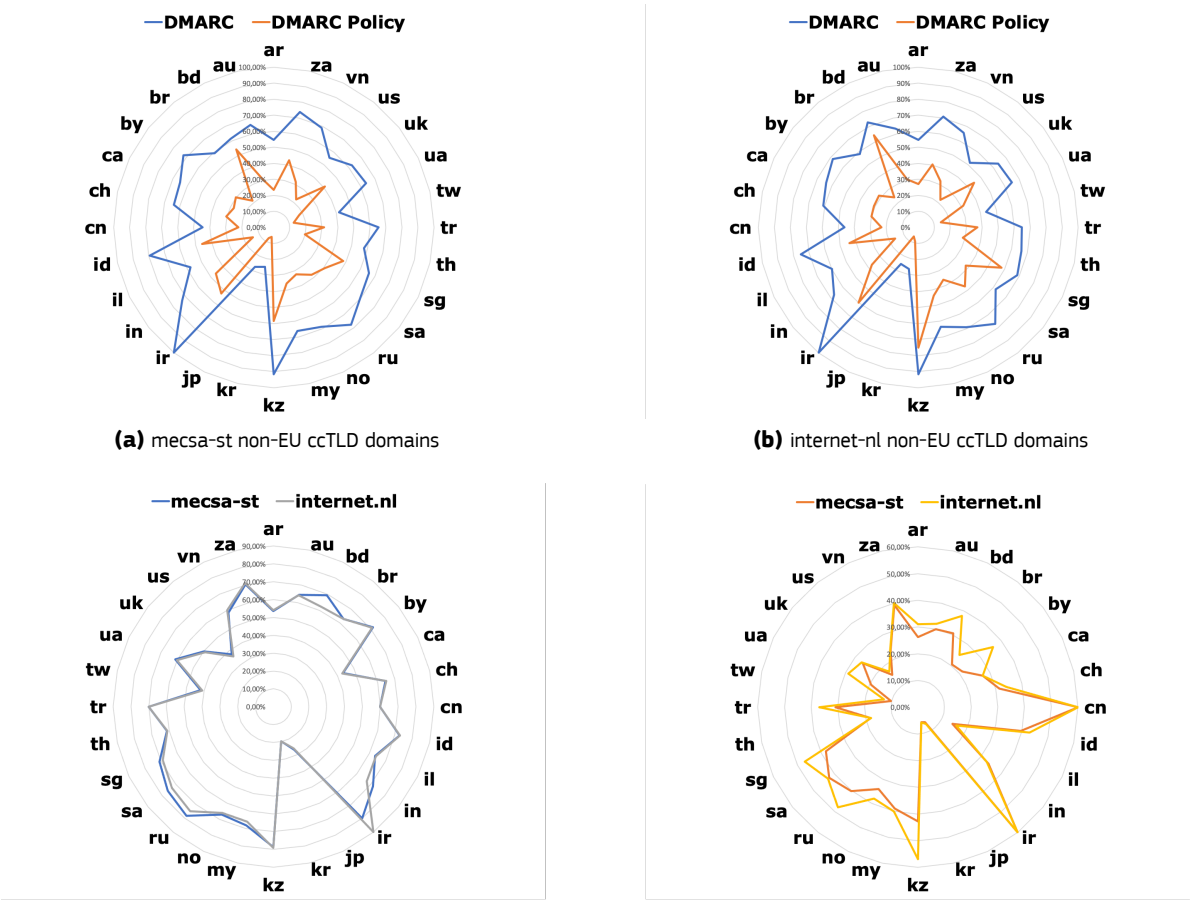


(c) DMARC EU ccTLD domains



(d) DMARC Policy EU ccTLD domains

Figure 8: DMARC and DMARC strict policy adoption in EU



(a) mecsa-st non-EU ccTLD domains

(b) internet-nl non-EU ccTLD domains

(c) DMARC non-EU ccTLD domains

(d) DMARC Policy non-EU ccTLD domains

Figure 9: DMARC and DMARC strict policy adoption in non-EU ccTLD domains

The average adoption rate for DMARC for non-EU ccTLDs is around 59% and for DMARC strict policy 28%; both figures increased from Q3 2022 by 5 and 3 percentage points respectively. DMARC and DMARC policy support for non-EU domains is quite similar in the two datasets. The non-EU countries with the lowest DMARC support are Japan (27%), South Korea (25%), and Taiwan (42%). The lowest strict DMARC policy adoption is observed in Japan (7%), South Korea (6%), Taiwan (13%) and Israel (15%). Moreover, with reference to Figures 9c and 9d, the support for DMARC strict policies remains far behind from that of DMARC.

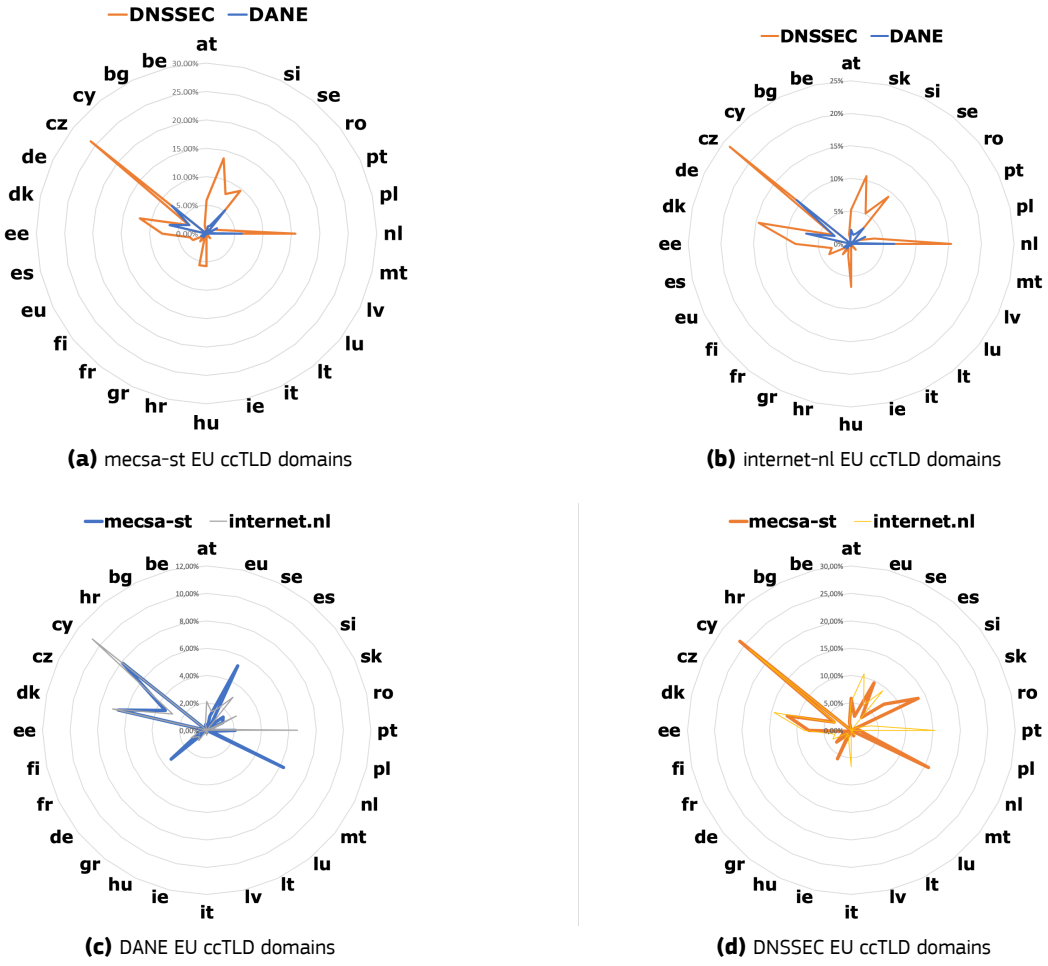
Overall, the averages for both EU and non-EU ccTLDs are lower than the results obtained from the MECSA web platform.

3.5 DANE

Figures 10a and 10b depict the adoption rate results for DANE and DNSSEC for EU ccTLDs as obtained with mecsa-st and internet.nl, respectively. The DNSSEC values are included for information purposes, since DANE requires DNSSEC.

As in the previous measurement period, the average support for DANE is around 2% in the MSs. In the vast majority of countries the support rates range between 0 and 3% with a few of outliers, i.e., Denmark (dk), Netherlands (nl), Czech Republic (cz), and Sweden (se) having from 3% to 10% depending on the tool used. Recall that this outcome is rooted in the lack of DNSSEC support, since DANE cannot exist without DNSSEC. In line with the previous measurement periods, in those countries that have an increased support for DNSSEC, like the Netherlands (nl) and Czech Republic (cz), the support for DANE lags behind. The results obtained with mecsa-st and internet.nl are highly correlated, as shown in Figures 10c and 10d.

With reference to Figures 11a and 11b, regarding the non-EU countries, DANE and DNSSEC support demonstrates the same behaviour as with EU ccTLD domains, having a very low average adoption rate of around



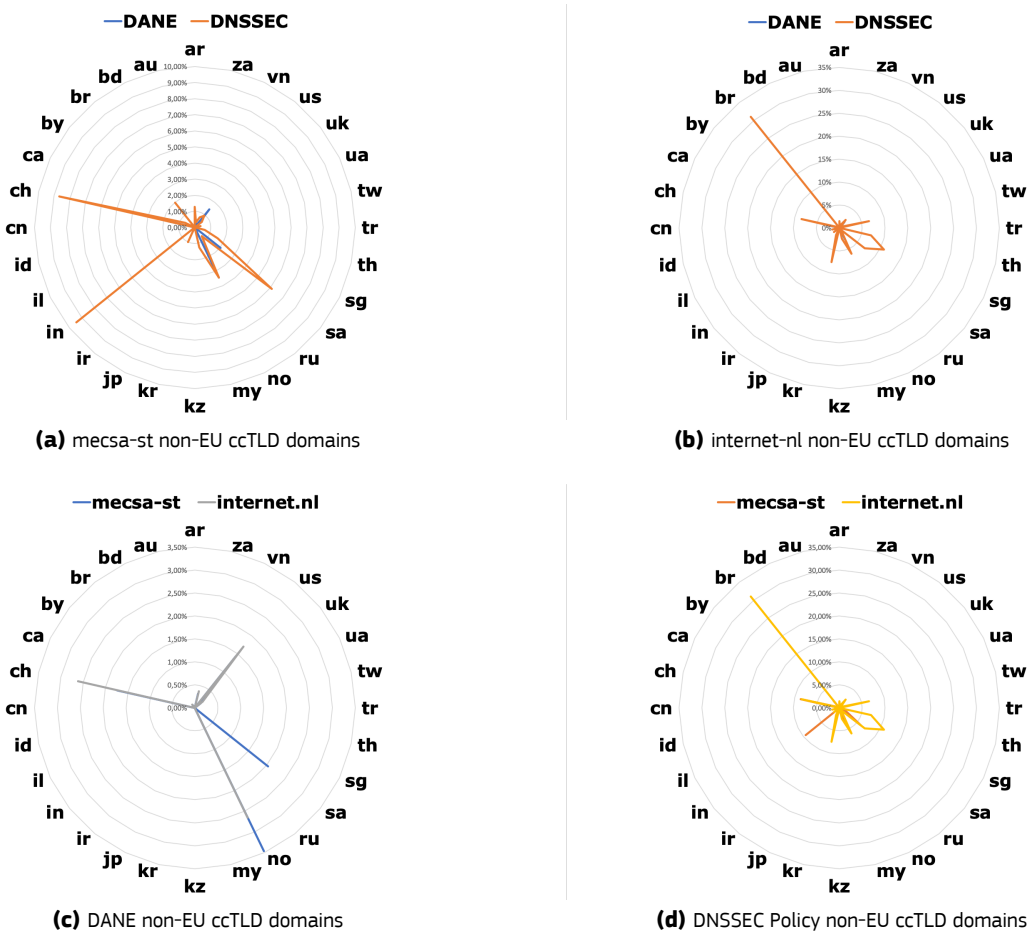
(a) mecsa-st EU ccTLD domains

(b) internet-nl EU ccTLD domains

(c) DANE EU ccTLD domains

(d) DNSSEC EU ccTLD domains

Figure 10: DANE and DNSSEC adoption in EU



(a) mecsa-st non-EU ccTLD domains

(b) internet-nl non-EU ccTLD domains

(c) DANE non-EU ccTLD domains

(d) DNSSEC Policy non-EU ccTLD domains

Figure 11: DANE and DNSSEC adoption in non-EU ccTLD domains

315 0 and 2%, respectively. The results from the two measurement tools are almost identical, with insignificant differences in the order of 0.5%, as shown in Figures 11c and 11d, the two datasets show similar data.

No less important, the MECSA web platform results show around 37% and 30% support for DANE and DNSSEC, respectively, which is much higher than the results stemming from mecsa-st and internet.nl.

4 Conclusions

The level of adoption of the set of Internet standards related to email communications in the EU (EU ccTLDs) follows a slightly higher trend to the one observed for the selected non-EU countries (non-EU ccTLDs), i.e., the average StartTLS support rate in the EU is about 10 percentage points higher than the non-EU average in both tools, while the SPF support rate in the EU is around 3-8% higher than the selection of non-EU countries, depending on the tool. The MECSA platform presents higher adoption rates than the other two tools, between 10 and 30 percentage points, with the exception of SPF and DKIM where the MECSA platform results are about the same. It should be noted that, mainly due to the minor differences in the results of the present and the previous measurement periods, the conclusions described in the previous reports (Draper-Gill et al., 2022a, Draper-Gill et al., 2022b, Karopoulos et al., 2023) still apply here and are repeated for convenience.

- StartTLS results are similar with both measurement tools. MECSA results reached 97% of adoption, considering 2044 unique email domains tested. EU ccTLDs show a uniform distribution across MSs with few outliers, close to 13 percentage points below the value recorded by the MECSA tool. The results for non-EU ccTLDs have a higher variance with several outliers, dragging the overall adoption rate close to 77%. Compared to the results of the previous measurement period, i.e., Q1 2023, the MECSA web platform reports a small increase of 4 percentage points, whereas mecsa-st and internet.nl report an increase of about 14 percentage points in EU and an increase of 15 and 20 percentage points in non-EU domains, respectively.

- SPF is also a widely used standard reaching similar levels to StartTLS, in the range of 87-95% in the EU, according to all tools used. A slightly lower adoption of around 79-92% is observed in non-EU domains. Broad usage of strict SPF policies is also observed across both the EU and non-EU domains.

- DKIM support for both EU and non-EU ccTLDs is high, ranging from 73 to 97%, just below SPF, although the results reported by the mecsa-st and internet.nl tools cannot be considered fully representative, considering their limitations, as described in Section 2.2. The results from MECSA, which are considered more accurate, show an adoption value of 79%. The results reported here are similar to the ones of Q1 2023 with the exception of the MECSA web platform which has an increase of 3 percentage points.

- DMARC shows a much lower rate of adoption than SPF and DKIM, the main protocols related to it, in the range of 62-63%, according to mecsa-st and internet.nl; the respective rate from MECSA web platform is higher at 73%. Moreover, the support for strict policies is also very low, much lower than in the SPF case, ranging from 26 to 28%.

- DANE (DNSSEC) is the less supported protocol, with almost no support at all, even in the cases where the domain tested has DNSSEC support. The results obtained analysing the ccTLD domains extracted from the Google Transparency Report differ from the ones obtained with the MECSA online tool, where we observe a rate of adoption of around 30%.

- mecsa-st results are generally aligned with those obtained with internet.nl results. There are some differences in individual country adoption rates in StartTLS and in the average adoption of SPF for both EU and non-EU domains but they are not significant and can be attributed to implementation differences of these two tools. Despite this discrepancy, mecsa-st and internet.nl are two reliable tools that can be used to make a systematic analysis of the level of adoption of email security standards, with periodical tests. Both tools allow the automatization of the tests and the generation of results.

The results presented in this report are consistent among the different sources analysed, providing us with an overview of the state of email security protocols in EU MSs. The results also present opportunities for improving the security and adoption of email security standards, in particular in the cases of DMARC and DANE. DMARC results present a gap between the adoption of DMARC and the implementation of strict policies. Without a strict policy, DMARC has no effect in the security of email services. Reducing this gap would have a positive impact in the overall security of these domains. Regarding DANE, its adoption rate is much lower than DNSSEC, a mandatory protocol to deploy DANE. Those domains with DNSSEC support should be able to easily adopt DANE to protect the confidentiality of their email communications.

To increase the level of adoption of the different standards there is the need to develop additional strategies specific to each protocol. For instance, to improve the adoption of SPF and DKIM it might be needed to first improve the adoption of DMARC and the implementation of strict policy and reporting features. DMARC reporting

370 is needed to measure the performance of SPF and DKIM implementations. The promotion of DANE requires, first, the increase in adoption of DNSSEC, as it is a requirement in the standard.

References

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

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

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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.

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)'. URL https://pokeinthe.io. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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.

CDNetworks, 'State of the Web Security, H1 2020'. URL https://www.cdnetworks.com. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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

Draper-Gill, G., Kampourakis, G. and G Karopoulos, J. S. M., 'Email communication security standards: an analysis of uptake in the EU - March 2022', , No KJ-NA-31-280-EN-N (online), 2022a. ISSN 1831-9424 (online). .

Draper-Gill, G., Kampourakis, G., Karopoulos, G., Spigolon, R. and Martin, J. S., 'Email communication security standards: an analysis of uptake in the EU - September 2022', *Publications Office of the European Union*, 2022b.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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 23/10/2023.

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. Last visited 23/10/2023.

European Commission, 'EU Internet Standards Deployment Monitoring Website'. n.d. URL https://ec.europa.eu/internet-standards/index.html. Last visited 23/10/2023.

European Commission, Directorate-General for Communications Networks, Content and Technology, 'Regulation of the european parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/ec (regulation on privacy and electronic communications)'. 2017. URL https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010.

European Commission, Joint Research Centre, 'MECSA Standalone Tool, mecsa-st'. n.d.a. URL https://github.com/mecsa/mecsa-st. Last visited 23/10/2023.

European Commission, Joint Research Centre, 'My Email Communications Security Assessment'. n.d.b. URL https://mecsa.jrc.ec.europa.eu. Last visited 23/10/2023.

European Parliament, C. o. t. E. U., 'Directive (eu) 2018/1972 of the european parliament and of the council of 11 december 2018 establishing the european electronic communications code'. URL https://eur-lex.europa.eu/eli/dir/2018/1972/oj.

European Parliament, C. o. t. E. U., 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)'. 2016. URL https://eur-lex.europa.eu/eli/reg/2016/679/oj.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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'. 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 16/06/2023.

Google, 'Google Transparency Report: Email Encryption in Transit'. n.d. URL https://transparencyreport.google.com/safer-email/. Last visited 10/02/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

Hoffman, P., 'Cryptographic Algorithm Identifier Allocation for DNSSEC'. RFC 6014 (Proposed Standard), Nov. 2010. URL http://www.ietf.org/rfc/rfc6014.txt. Last visited 23/10/2023.

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. Last visited 23/10/2023.

Hong, J., 'The state of phishing attacks', *Communications of the ACM*, Vol. 55, No 1, 2012, pp. 74–81. ISSN 0001-0782. .

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. Last visited 23/10/2023.

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.

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. .

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, pp. 83–95.

Karopoulos, G., Kouliaridis, V. and Martin, J. S., 'Email communication security standards: an analysis of uptake in the eu - march 2023', , No KJ-NA-31-397-EN-N (online), 2023. ISSN 1831-9424 (online). .

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. Last visited 23/10/2023.

Klensin, J., 'Simple Mail Transfer Protocol'. RFC 5321 (Draft Standard), Oct. 2008. URL http://www.ietf.org/rfc/rfc5321.txt. Updated by RFC 7504. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

Lange, C., Chang, T., Fiedler, M. and Petrlic, R., 'An email a day could give your health data away', *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 2023.

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. .

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.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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. Last visited 23/10/2023.

Nordström, O. and Dovrolis, C., 'Beware of bgp attacks', *SIGCOMM Computer Communication Review*, Vol. 34, No 2, 2004, pp. 1–8. ISSN 0146-4833. .

OWASP, 'OWASP Top Ten'. a. URL https://owasp.org/www-project-top-ten/. Last visited 23/10/2023.

OWASP, 'Secure Headers Project'. b. URL https://owasp.org/www-project-secure-headers/.

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', , p. 7.

Q-Success, 'Usage statistics of Default protocol https for websites'. a. URL https://w3techs.com/technologies/details/ce-httpsdefault.

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

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

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

QUIC WG, 'Charter for Working Group'. URL https://datatracker.ietf.org/wg/quic/about/. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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.

Sanchez Martin, J. and Draper Gil, G., 'My email communications security assessment (mecsa): 2018 results', , No KJ-NA-29674-EN-N (online), 2019. ISSN 1831-9424 (online). .

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. Last visited 23/10/2023.

Scott Helme, 'Top 1 Million Analysis - March 2020'. a. URL https://scotthelme.co.uk/top-1-million-analysis-march-2020/. Last visited 23/10/2023.

Scott Helme, 'Top 1 Million Sites Security Analysis'. b. URL https://crawler.ninja/. Last visited 23/10/2023.

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. Last visited 23/10/2023.

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.

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. Last visited 23/10/2023.

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.

List of abbreviations and definitions

CA Certification Authority

CRL Certificate Revocation List

ccTLD country code Top-Level Domain

DANE DNS-Based Authentication of Named Entities

DKIM Domain Keys Identified Mail

DMARC Domain-based Message Authentication, Reporting and Conformance

DNS Domain Name System

EC European Commission

EU European Union

IETF Internet Engineering Task Force

JRC Joint Research Centre

MECSA My Email Communications Security Assessment

MS Member State

MX Mail Exchanger

NCSC National Cyber Security Centre

RFC Request For Comments

SMTP Simple Mail Transfer Protocol

SPF Sender Policy Framework

TLS Transport Layer Security

TLSA TLS Authentication

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