Human Systems Engineering and Design (IHSED2025), Vol. 198, 2025, 458–465
https://doi.org/10.54941/ahfe1006799

Monitoring the Adoption of E-Mail Security Standards in Selected Healthcare Entities in Poland

Patryk Morawiec

Faculty of Informatics and Communication, University of Economics in Katowice,
1 Maja 50, 40–287 Katowice, Poland

ABSTRACT

Since 25 September 2023 configuration of DMARC protocol is mandatory for public entities in Poland. This article presents the status of implementation of the DMARC, SPF and DKIM security protocols in domains used by healthcare entities in Poland. Selected domains were analysed using EasyDMARC online software. Out of 302 domains, the DMARC protocol was somehow configured in 232, including 181 in secure way, and was missing in 70. Other protocols are used with varying degrees of success. The SPF protocol is properly implemented in most examined domains, while vast majority of domains is missing the implementation of DKIM protocol.

Keywords: Spoofing, Healthcare, Cybersecurity standards, Domain, E-mail, Security protocols

INTRODUCTION

Spoofing and other methods of unauthorized access to e-mail domain pose a serious challenge in cybersecurity policies in healthcare entities. According to darknet analysis reports, healthcare data are the most sought-after goods on the illegal market (Cherian, 2022), and therefore the number of cyberattacks on hospital infrastructure is rising, mostly including ransomware attacks (Dupont *et al.*, 2020; Olsen, 2023). E-mail messages still remains the main source of these threats (Ewoh and Vartiainen, 2024). On a positive note, according to 2024 HIMSS report, awareness of e-mail and ransomware security threats is relatively high, and cybersecurity training for healthcare employees is mostly considered as effective (*2024 HIMSS Healthcare Cybersecurity Survey*, 2025). In Poland the number of security incidents is also rising significantly, while over the last years the number of unauthorized access to data has decreased significantly (Dorobisz, 2024).

There are several methods currently used in practice to protect against these threats. The DMARC standard (Domain-based Message Authentication, Reporting and Conformance) is an authorization and reporting protocol based on SPF (Sender Policy Framework) and/or DKIM (DomainKeys Identified Mail). Article is a pilot study on the security of healthcare sector websites in Poland. The goal is to investigate the adoption of DMARC standard as well as the SPF and DKIM protocols, like also to examine the domain administration policy for unvalidated e-mails.

The mandatory tags of the DMARC record are v (protocol version) and p (policy for main domain), other non-mandatory but often used tags are:

- sp – policy for subdomains,
- rua – e-mail address for bulk reports,
- ruf – e-mail address for detailed reports,
- pct – percentage of non-validated messages (range from 1 to 100) to which the DMARC policy is applied. It is recommended to set low percentage at the beginning of DMARC implementation and gradually increase to 100% value.

DMARC policies can be set in p and sp tags as (Google Help Center, no date):

- none – where no action is taken, all unauthenticated messages is delivered to recipient inbox. This option is recommended only at the beginning of implementation process to verify how the authentication works. Later, it should be changed to quarantine or reject for better protection against spoofing.
- quarantine – where unauthenticated messages are delivered directly to SPAM folder and marked as a SPAM.
- reject – where unauthenticated messages are not delivered, the sending server usually receives a message about delivery problem.

Properly implemented DMARC in addition to the benefits of increased security level can also increase e-mail deliverability by 10% (Rudra, 2022). However, applying too restrictive DMARC policy can lead to misclassification of legitimate messages which is evaluated to be 36.9–62.7% for DMARC authentication and 2.8–11.1% for SPF or DKIM authentication itself (Konno, Kitagawa and Yamai, 2020). For all public entities in Poland, use of DMARC is mandatory since 25 September 2023 (*Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej*, 2023), similar regulations are also implemented in many European countries (Rudra, 2022).

The literature on this topic is not very extensive. DMARC adoption was a subject of studies in US for non-federal government institutions, where the SPF protocol implementation was shown to grow faster than the growth of newly registered domains, while DMARC implementation was shown to grow slightly slower (Gebhard and Perouli, 2023). In Croatia, enterprises in both public as well as private sector were analysed by Pranić in case of DMARC implementation. The low level of implementation and negligence in implementing the protocol outside the pharmaceutical and banking sectors were pointed out (Pranić, 2023).

SPF protocol is one of the DMARC protocol component among DKIM and is the longest-used method to secure e-mail domain. Technically is an additional line in DNS record (Anh, Anh and Thang, 2010) may looks like code below.

```
example.com IN TXT "v=spf1 mx -all"
```

Originally SPF was designed to authenticate e-mail sender to protect against potential phishing. However implemented alone, SPF has some severe limitations such as (Görling, 2007):

- impossibility to verify whole e-mail addresses, only sender's domain,
- inability to prove the actual domain ownership by the institution associated with it,
- lack of content verification,
- no encryption.

DKIM protocol is a cryptography-based authentication framework for identity validation of e-mail sender during the time message is transferred via the Internet (Yusuf, Adebayo and Zirra, 2015).

Presented for a first time in 2004 as DomainKeys ('Brief history of email authentication', 2015), didn't gain much recognition. As the official RFC standard DKIM was published in 2007 (Delany, 2007) and updated in 2018 (Kitterman, 2018). DKIM verifies validity of digital signature of e-mail header and body to provide authenticity of e-mail sender (Konno, Kitagawa and Yamai, 2020).

Relatively new method of domain security is BIMI protocol (Brand Indicators for Message Identification) and related with BIMI VMC (Verified Mark Certificate) or CMC (Common Mark Certificate) certificates ('Brand Indicators for Message Identification', no date; *Certyfikaty CMC*, no date; *Certyfikaty VMC*, no date). This standard verifies the authenticity of the sender by compliance of an implemented logo file, which in the case of a VMC certificate must match the file filed with the patent office. This method requires earlier implementation of DMARC standard. BIMI protocol is currently the most effective tool for protection against spoofing and also provides additional benefits in the form of improved brand identification and associated increased trust (Steinbrinck, 2024). The main obstacle to popularize this solution among broad scope of companies and public institutions seems the necessity to verify logo file with patent office with VMC certificate. In the case of a CMC certificate, such a match is not necessary, but the level of confidence is slightly reduced. The additional disadvantage of this protocol is also its high annual cost for obtaining required VMC/CMC certificate.

MATERIAL AND METHODS

The research was conducted on publicly available web pages of healthcare entities in Poland. Analysed research sample consisted of internet domains of healthcare entities from all voivodeships in Poland. It was examined 302 domains; the median was 20 entities per voivodeship.

Selected domains were examined with use of EasyDMARC Domain Scanner, an online cybersecurity software ('EasyDMARC Domain Scanner and Health Check', no date). The domain verification took place on 14 April – 16 April 2025.

Domains Evaluation

Domains Scanner examines 3 domain authentication protocols (SPF, DMARC and DKIM), gives a score mark from 0 to 10 (higher is better) and classifies potential risk level, where ('EasyDMARC Domain Scanner and Health Check', no date):

- 0–3 points – high risk level,
- 4–7 points – medium risk level,
- 8–10 points – low risk level.

The majority of examined domains (71.52%) was classified as medium risk level. Only 8 domains (2.65%) were classified as low risk, while in 25.83%, the risk were classified high level.

In case of DMARC protocol, the applied policy for handling non-validated messages based on the default tag settings (p tag) were also examined.

Table 1 shows the implemented policies among healthcare entities domains.

Table 1: DMARC protocol policies among the domains in polish healthcare entities.

Voivodeship	All Entities	DMARC Policy			
		Missing	None	Quarantine	Reject
Lower Silesian	20; (6.62%)	5; (25.00%)	4; (20.00%)	7; (35.00%)	4; (20.00%)
Kuyavian-Pomeranian	20; (6.62%)	4; (20.00%)	6; (30.00%)	5; (25.00%)	5; (25.00%)
Lublin	22; (7.29 %)	7; (31.82 %)	4; (18.18 %)	7; (31.82 %)	4; (18.18 %)
Lubusz	10; (3.31%)	2; (20.00%)	2; (20.00%)	4; (40.00%)	2; (20.00%)
Łódź	21; (6.95%)	6; (28.57%)	0; (0.00%)	12; (57.14%)	3; (14.29%)
Lesser Poland	23; (7.62%)	7; (30.43%)	5; (21.74%)	7; (30.43%)	4; (17.40%)
Masovian	22; (7.29%)	3; (13.63%)	5; (22.73%)	7; (31.82%)	7; (31.82%)
Opole	13; (4.30%)	1; (7.69%)	3; (23.08%)	4; (30.77%)	5; (38.46%)
Subcarpathian	20; (6.62%)	4; (20.00%)	5; (25.00%)	5; (25.00%)	6; (30.00%)
Podlaskie	16; (5.30%)	4; (25.00%)	2; (12.50%)	7; (43.75%)	3; (18.75%)
Pomeranian	18; (5.96%)	8; (44.44%)	0; (0.00%)	9; (50.00%)	1; (5.56%)
Silesian	23; (7.62%)	4; (17.40%)	2; (8.69%)	11; (47.82%)	6; (26.09%)
Holy Cross	15; (4.97%)	3; (20.00%)	1; (6.67%)	7; (46.67%)	4; (26.66%)
Warmian-Masurian	18; (5.96%)	4; (22.22%)	3; (16.67%)	4; (22.22%)	7; (38.89%)
Greater Poland	21; (6.95%)	4; (19.05%)	5; (23.81%)	10; (47.62%)	2; (9.52%)
West Pomeranian	20; (6.62%)	4; (20.00%)	4; (20.00%)	8; (40.00%)	4; (20.00%)
TOTAL	**302; (100%)**	**70; (23.18%)**	**51; (16.89%)**	**114; (37.75%)**	**67; (22.18%)**

In 23.18% of all examined domains there was no DMARC record implemented at all (missing value) and another 16.89% has the policy (p tag) set as none. The majority of domains (37.75%) have the policy set as quarantine and for 22.18% of domains the policy is set to reject non-validated e-mails (see Figure 1).

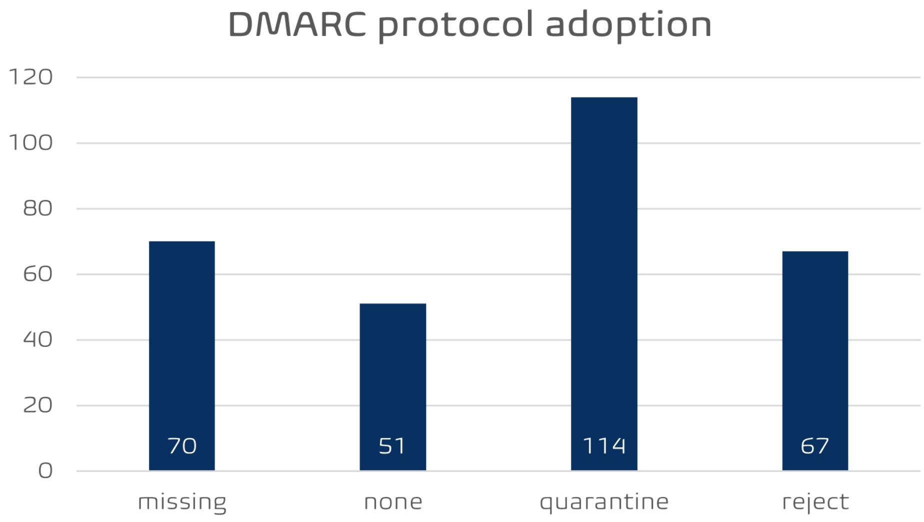

Figure 1: DMARC protocol adoption and policy implementation (absolute numbers).

In Table 2 there are shown the configuration of the remaining protocols.

Table 2: SPF and DKIM setting for healthcare entities domains in Poland.

Voivodeship	All Entities	SPF Record			DKIM Record	
		Valid	Warning	Invalid	Valid	Invalid
Lower Silesian	20; (6.62%)	18; (90.00%)	2; (10.00%)	0; (0.00%)	3; (15.00%)	17; (85.00%)
Kuyavian-Pomeranian	20; (6.62%)	20; (100.00%)	0; (0.00%)	0; (0.00%)	3; (15.00%)	17; (85.00%)
Lublin	22; (7.29%)	18; (81.82%)	3; (13.63%)	1; (4.55 %)	5; (22.73%)	17; (77.27%)
Lubusz	10; (3.31%)	8; (80.00%)	2; (20.00%)	0; (0.00%)	1; (10.00%)	9; (90.00%)
Łódź	21; (6.95%)	16; (76.19%)	3; (14.29%)	2; (9.52%)	2; (9.52%)	19; (90.48%)
Lesser Poland	23; (7.62%)	17; (73.91%)	5; (21.74%)	1; (4.35%)	1; (4.35%)	22; (95.65%)
Masovian	22; (7.29%)	19; (86.36%)	3; (13.64%)	0; (0.00%)	2; (9.09%)	20; (90.91%)
Opole	13; (4.30%)	13; (100.00%)	0; (0.00%)	0; (0.00%)	4; (30.77%)	9; (69.23%)
Subcarpathian	20; (6.62%)	15; (75.00%)	4; (20.00%)	1; (5.00%)	2; (10.00%)	18; (90.00%)
Podlaskie	16; (5.30%)	14; (87.50%)	2; (12.50%)	0; (0.00%)	2; (12.50%)	14; (87.50%)
Pomeranian	18; (5.96%)	18; (100.00%)	0; (0.00%)	0; (0.00%)	4; (22.22%)	14; (77.78%)
Silesian	23; (7.62%)	18; (78.26%)	2; (8.70%)	3; (13.04%)	2; (8.70%)	21; (91.30%)
Holy Cross	15; (4.97%)	12; (80.00%)	2; (13.33%)	1; (6.67%)	2; (13.33%)	13; (86.67%)
Warmian-Masurian	18; (5.96%)	18; (100.00%)	0; (0.00%)	0; (0.00%)	3; (16.67%)	15; (83.33%)
Greater Poland	21; (6.95%)	19; (90.48%)	2; (9.52%)	0; (0.00%)	2; (9.52%)	19; (90.48%)
West Pomeranian	20; (6.62%)	16; (80.00%)	2; (10.00%)	2; (10.00%)	3; (15.00%)	17; (85.00%)
TOTAL	302; (100%)	259; (85.76%)	32; (10.60%)	11; (3.64%)	41; (13.58%)	261; (86.42%)

While SPF record is implemented properly in vast majority of cases (85.76% has valid record), the DKIM record is invalid in 86.42% of examined domains, including missing record in 77.48% or incorrectly configured in 8.94% of domains.

It were also observed some differences between p tag and sp tag setting in analysed domains. This situation occurred in 4.97% of examined domains. However, this does not constitute a configuration error in itself, but it can potentially lead to differences in the classification of messages originating from the main domain compared to messages originating from subdomains.

In 3.64% of domains, incorrect configuration of reporting mechanism was demonstrated. Lack of rua tag was also found in 10.26% of examined domains. In 2 cases a pct was defined below 100%.

CONCLUSION AND FURTHER WORK

To maximize effective protection against phishing and spoofing threats, it is recommended to implement DMARC protocol. Both SPF and DKIM protocols are also recommended to be implemented, although DMARC requires only one of them as mandatory. In healthcare entities, especially in public institutions where implementation of these protocols is obligatory, this should be a particularly important issue. Unfortunately, many of public institutions are still missing or its configuration is not fully secure. The most secure policies were implemented in Holy Cross and Silesian voivodships, while the most missing values in DMARC implementation were observed in Pomeranian voivodeship.

A secure implemented DMARC policy should have the p tag (and optionally sp tag) set as “reject” option. It is also important to remember that there is no full protection against the earlier mentioned threats. An example is one of the examined institutions, which, despite the correct implementation of the DMARC protocol, fell victim to a data leak, which it was reported on its website in March 2025.

As a recommendation, it is recommended to include up-to-date knowledge of the protocols currently used by global vendors in training for domain administrators in public healthcare facilities e.g. BIMI like also performing periodic reviews of the existing status of used domains and the correctness of SPF, DKIM and DMARC records. It is also recommended to verify the validity of e-mail addresses intended for receiving DMARC reports.

Presented article is an introduction to further studies on cybersecurity in Polish healthcare entities and is therefore not without some limitations and does not exhaust the research topic. The further studies will focus on in-depth analyses of detected problems. Further analyses might be also performed using a variety of diagnostic tools that analyses each single aspect separately.

REFERENCES

2024 HIMSS Healthcare Cybersecurity Survey (2025). Chicago, IL: Healthcare Information and Management Systems Society. Available at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey/ (Accessed: 17 April 2025).

Anh, N. T., Anh, T. Q. and Thang, N. X. (2010) ‘Spam Filter Based on Dynamic Sender Policy Framework’, in *2010 Second International Conference on Knowledge and Systems Engineering. 2010 Second International Conference on Knowledge and Systems Engineering (KSE)*, Hanoi, Vietnam: IEEE, pp. 224–228. Available at: https://doi.org/10.1109/KSE.2010.11.

'Brand Indicators for Message Identification' (no date) *EmailLabs*. Available at: https://emaillabs.io/bimi/ (Accessed: 29 June 2025).

'Brief history of email authentication' (2015) *dmarcian*, 5 October. Available at: https://dmarcian.com/brief-history-of-email-authentication/ (Accessed: 30 June 2025).

Certyfikaty CMC (no date) *MSERWIS*. Available at: https://www.mserwis.pl/certyfikaty-cmc (Accessed: 29 June 2025).

Certyfikaty VMC (no date) *MSERWIS*. Available at: https://www.mserwis.pl/certyfikaty-vmc (Accessed: 29 June 2025).

Cherian, S. (2022) *Healthcare Data: The Perfect Storm*, *Forbes*. Available at: https://www.forbes.com/councils/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/ (Accessed: 18 April 2025).

Delany, M. (2007) *Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)*. RFC4870. RFC Editor, p. RFC4870. Available at: https://doi.org/10.17487/rfc4870.

Dorobisz, J. (2024) 'Analysis of trends and risks in the field of network security based on statistical data', *GIS Odyssey Journal*, 4(2), pp. 147–163. Available at: https://doi.org/10.57599/gisoj.2024.4.2.147.

Dupont, G. *et al.* (2020) 'A Matter of Life and Death: Analyzing the Security of Healthcare Networks', in M. Hölbl, K. Rannenberg, and T. Welzer (eds) *ICT Systems Security and Privacy Protection*. Cham: Springer International Publishing (IFIP Advances in Information and Communication Technology), pp. 355–369. Available at: https://doi.org/10.1007/978-3-030-58201-2_24.

'EasyDMARC Domain Scanner and Health Check' (no date). Zoetermeer: EasyDMARC Inc. Available at: https://easydmarc.com/domain-scanner (Accessed: 10 April 2025).

Ewoh, P. and Vartiainen, T. (2024) 'Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review', *Journal of Medical Internet Research*, 26, p. e46904. Available at: https://doi.org/10.2196/46904.

Gebhard, A. and Perouli, D. (2023) 'Poster: Measuring Adoption of SPF, DMARC, and CAA DNS Records with Nonfederal Governments in the United States', in *2023 IEEE 31st International Conference on Network Protocols (ICNP)*. *2023 IEEE 31st International Conference on Network Protocols (ICNP)*, Reykjavik, Iceland: IEEE, pp. 1–2. Available at: https://doi.org/10.1109/ICNP59255.2023.10355622.

Google Help Center (no date) *Set up DMARC*, *Google Workspace Admin Help*. Available at: https://support.google.com/a/answer/2466580?hl=en (Accessed: 18 April 2025).

Görling, S. (2007) 'An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism', *Internet Research*, 17(2), pp. 169–179. Available at: https://doi.org/10.1108/10662240710737022.

Kitterman, S. (2018) *Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)*. RFC8301. RFC Editor, p. RFC8301. Available at: https://doi.org/10.17487/RFC8301.

Konno, K., Kitagawa, N. and Yamai, N. (2020) 'False Positive Detection in Sender Domain Authentication by DMARC Report Analysis', in *Proceedings of the 2020 The 3rd International Conference on Information Science and System*. *ICISS 2020: 2020 The 3rd International Conference on Information Science and System*, Cambridge United Kingdom: ACM, pp. 38–42. Available at: https://doi.org/10.1145/3388176.3388217.

Olsen, E. (2023) *Ransomware attacks on healthcare facilities cost $77.5B in downtime, report finds*, *Healthcare Dive*. Available at: https://www.healthcaredive.com/news/healthcare-ransomware-costs-comparitech-77-billion/698044/ (Accessed: 28 October 2024).

Pranić, D. (2023) 'Analysis of DMARC Implementation in Republic of Croatia', in *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*. *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia: IEEE, pp. 1219–1224. Available at: https://doi.org/10.23919/MIPRO57284.2023.10159639.

Rudra, A. (2022) 'DMARC Requirements in 2025', *PowerDMARC*, 30 June. Available at: https://powerdmarc.com/dmarc-requirements/ (Accessed: 17 April 2025).

Steinbrinck, K. (2024) 'Email Authentication Protocols in 2024: Your Guide to SPF, DKIM, DMARC, and BIMI', *Email on Acid*, 21 February. Available at: https://www.emailonacid.com/blog/article/email-deliverability/email-authentication-protocols/ (Accessed: 30 June 2025).

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (2023). Available at: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20230001703 (Accessed: 18 April 2025).

Yusuf, S. E., Adebayo, K. J. and Zirra, P. B. (2015) 'Addressing Advanced Persistent Threats using Domainkeys Identified Mail (DKIM) and Sender Policy Framework (SPF)', *Journal of Emerging Trends in Computing and Information Sciences*, 6(1), pp. 60–67.