# **Dodatna pojasnila posameznih mehanizmov poštnega sistema:**

## **1. Preverjanje pristnosti pošiljatelja**

V skladu z dobro prakso se preverja pristnost pošiljatelja e-pošte po standardih SPF, DKIM in DMARC.

Preverjanje je namenjeno preprečevanju lažnega predstavljanja in zmanjšanja količine neželene e-pošte. Preverja se vsa vhodna e-poštna sporočila iz interneta v omrežje HKOM.

1. **SPF (Sender Policy Framework)** je način preverjanja pristnosti domene pošiljatelja ovojnice sporočila (MAIL FROM).

Več o SPF na povezavi <https://en.wikipedia.org/wiki/Sender_Policy_Framework>

Lastnik domene v SPF DNS zapisu pooblasti strežnike, iz katerih je dovoljeno pošiljati sporočila. SPF zapis se nahaja v TXT DNS polju. Začeti se mora z v=spf1.

SPF preverja pristnost pošiljatelja ovojnice e-pošte. Strežnik prejemnika preveri ali domena pošiljatelja lahko izvira iz IP številke strežnika, ki pošilja e-sporočilo.

Trenutno stanje nastavljenega mehanizma na centralnem poštnem sistemu: SPF se preverja, če je SPF na domeni pošiljatelja nastavljen. V primeru negativnega rezultata se sporočilo zavrne, če je vrednost SPF pri pošiljatelju privzeto nastavljena na "fail" ali "softfail".

Napoved: Načrtuje se vklop zavračanja sporočil za domene, ki nimajo nastavljenega SPF preverjanja. Načrtuje se vklop zavračanja e-pošte tudi v primeru, če je SPF privzeto nastavljen na "neutral" ali "pass".

1. **DKIM** preverja pristnost pošiljatelja vsebine e-pošte. Strežnik prejemnika preveri ali je sporočilo DKIM podpisano.

Več o DKIM na povezavi <https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail>

DKIM kriptografsko podpisuje sporočila, zaglavje in vsebino. Zaglavje ni podpisano v celoti. Podpisane so samo tiste glave, ki so pomembne za verodostojnost pošiljatelja in vsebine npr. From, To, Subject, Message-ID, Date, ...

DKIM podpis poveže sporočilo in identiteto podpisnika. Identiteta podpisnika je vključena v podpis in je povezana z domeno podpisnika.

Standard ne zahteva, da je domena podpisnika enaka domeni pošiljatelja ali kateri drugi domeni v e-naslovih zaglavja sporočila. Povezavo med domeno podpisnika in domeno pošiljatelja se lahko določi v DMARC DNS zapisu.

DKIM ne potrebuje overitelja digitalnih potrdil (CA). Javni ključ je dostopen v DNS v poddomeni "\_domainkey" domene podpisnika.

Trenutno stanje nastavljenega mehanizma na centralnem poštnem sistemu: DKIM se preverja, vendar pa negativen rezultat ne povzroči zavrnitve sporočila, se pa rezultat uporabi v DMARC mehanizmu.

Napoved: Ni predvidenih sprememb.

1. **DMARC** je določen v standardu RFC 7489 ([RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC) (rfc-editor.org)](https://www.rfc-editor.org/rfc/rfc7489.html))

Dodatna razlaga je na povezavi <https://en.wikipedia.org/wiki/DMARC>

DMARC je dodaten mehanizem, ki uporablja rezultat SPF in/ali DKIM mehanizma. Lastnik domene z DMARC DNS zapisom pove, kako se preveri pristnost sporočila.

Podprti sta dve metodi pristnosti, SPF in DKIM.

DMARC se, tako kot SPF in DKIM, preverja na vhodni strani prejemnikove infrastrukture.

Potek preverjanja:

Najprej se preverita SPF in DKIM. DKIM podpisov je lahko več, preveriti je potrebno vsakega posebej.

Če je preverjanje pristnosti po SPF/DKIM metodi uspešno, se preveri poravnavo domene SPF/DKIM metode z domeno iz e-naslova RFC5322.From. Preveriti je potrebno poravnavo za vsak DKIM podpis posebej.

Če je katerakoli metoda in poravnava te metode uspešna, je uspešno tudi DMARC preverjanje.

DMARC rezultat je uspešen, če je uspešen SPF rezultat ali DKIM rezultat, pri čemer mora biti domena DKIM ključa usklajena z domeno pošiljatelja vsebine sporočila.

Trenutno stanje nastavljenega mehanizma na centralnem poštnem sistemu: DMARC se preverja, vendar pa negativen rezultat ne pomeni zavrnitve sporočila.

Napoved: Načrtuje se vklop zavračanja e-sporočila na osnovi negativnega DMARC rezultata.

**Lastnik domene je odgovoren za pravilne SPF, DKIM in DMARC DNS zapise.** Nepravilni DNS zapisi lahko povzročijo zavračanje legalne e-pošte.

E-poštne domene, ki nimajo svojih strežnikov, ampak gostujejo pri ponudnikih oblačne storitve e-pošte, morajo SPF, DKIM in DMARC zapise nastaviti po navodilih ponudnikov oblačnih storitev.

Opozorilo: Na osnovi SPF, DKIM in DMARC rezultata se e-sporočilo lahko zavrne. E-sporočilo zavrne HKOM e-poštni strežnik, za pripravo in pošiljanje povratnice pošiljatelju pa je odgovoren strežnik, ki e-sporočilo pošilja.

## **2. Preverjanje skladnosti s standardom RFC 5322**

Standard RFC 5322 predpisuje nekatera polja v glavi sporočila. Standard [RFC 5322](https://www.rfc-editor.org/rfc/rfc5322) je nastal leta 2008 kot pregled oziroma združitev starejših standardov [RFC 822](https://www.rfc-editor.org/rfc/rfc822) in [RFC 2822](https://www.rfc-editor.org/rfc/rfc2822). Vsebuje tudi priporočila na osnovi uporabe in izkušenj s tega področja in manjše spremembe, ki so bile predpisane v mnogih drugih [RFC](https://www.rfc-editor.org/rfc/) standardih.

RFC 5322 predpisuje zgradbo sporočila. Namenski odjemalci npr. Outlook ali Lotus Notes pošljejo pravilno zgrajeno sporočilo. Večja težava je pri aplikacijah, ki pošiljajo sporočila. Pošiljanje sporočil je samo en delček aplikacije. Razvijalci običajno ne poznajo standardov s področja oblikovanja sporočil. Večina aplikacij določi samo dva elementa poštnega sporočila, to je pošiljatelja (From) in prejemnika (To), kar pa po standardu 5322 ne bo več dovolj.

Google je napovedal, da bo od [1.februar 2024](https://support.google.com/mail/answer/81126?hl=en) dalje pregledoval skladnost prejetih sporočil s tem standardom. Kratek povzetek napovedi Googla:

* Message-ID polje je obvezno
* Polja, ki lahko nastopijo samo enkrat (single-instance): From, To, Subject, Date, ...
* Date polje je po standardu obvezno, v Google napovedi ni omenjeno, priporočam, da ga aplikacije vseeno nastavijo.
* From polje lahko po standardu vsebuje več e-naslovov, Google je napovedal, da bo dovoljeval le en e-naslov.

Priporočilo MDP je , da sporočilo vsebuje naslednja polja, ki se pojavijo točno enkrat:

- From

- To

- Message-ID

- Date

- Subject

Na osnovi rezultata preverjanja skladnosti z RFC 5322 se e-sporočilo lahko zavrne. Sporočilo zavrne HKOM e-poštni strežnik, za pripravo in pošiljanje povratnice pošiljatelju pa je odgovoren strežnik, ki e-sporočilo pošilja.

## **3. Preverjanje neželene e-pošte (SPAM)**

Za preverjanje neželene e-pošte se uporablja različne mehanizme, od ključnih besed, črnih seznamov (black-lists), "greylistinga", spremljanja "lažnih" povratnic, do statističnih metod in drugih mehanizmov. Vsak mehanizem prispeva delček ocene. Nabor mehanizmov se prilagaja trenutni oceni tveganja.

Vsako vhodno e-sporočilo se oceni z verjetnostjo, da je sporočilo neželeno. Sporočila z majhno verjetnostjo se dostavijo prejemniku. Sporočila s srednjo oceno se označijo in dostavijo prejemniku.

Sporočila z visoko oceno se zavržejo, povratnice pa se iz varnostnih razlogov ne pošlje.

Pri preverjanju neželene e-pošte lahko pride do napačne pozitivne ocene (false positive) in s tem do zavrženega e-sporočila, pri čemer se povratnice ne pošlje.

## **4. Varnostno pregledovanje vsebine e-pošte**

Uporablja se avtomatizirana orodja za proti virusno pregledovanje e-pošte. Vsa vhodna e-pošta se varnostno pregleda proti škodljivi kodi. Pregleda se s klasičnimi proti virusnimi mehanizmi na osnovi vzorcev. Dodatno se vsebina preveri z naprednimi orodji (npr. sendbox, analiza makrojev), ki ocenijo prisotnost potencialno škodljivih elementov.

V primeru zaznane škodljive kode oz. velikega varnostnega tveganja, se e-sporočilo zavrže, povratnice se iz varnostnih razlogov ne pošlje.

Priporočilo MDP: Za zmanjšanje možnosti napačno pozitivno ocenjenih e-sporočil priporočamo, da se, če je možno, ne uporablja formatov priponk z vključenimi makroji, to so datoteke s končnicami xlsm, xltm, xlam, xlm, docm, dotm, …)

Več informacij na povezavah:

<https://support.microsoft.com/sl-si/office/oblike-zapisa-datoteke-ki-jih-podpira-excel-0943ff2c-6014-4e8d-aaea-b83d51d46247>

<https://support.microsoft.com/sl-si/office/file-formats-for-saving-documents-88de3863-c9e5-4f89-be60-906f9065e43c>

## **5. Prepovedane priponke**

Prepovedane so priponke, ki lahko sprožijo izvršljivo kodo kot so izvršljive datoteke, povezave (linki), slike datotečnih sistemov in podobno.

Seznam prepovedanih priponk se prilagaja trenutni oceni tveganja.

## **6. Dodatne povezave in razlage**

* Spletno mesto Domenca.com /Baza znanja / DMARC, DKIM in SPF

<https://www.domenca.com/podpora/kb/dmarc-dkim-in-spf/>

* Spletno mesto Evropske komisije / EU Internet Standards Deployment MonitoringWebsite / Modern Email Security Standards <https://ec.europa.eu/internet-standards/email.html>

Nekaj večjih svetovnih ponudnikov in njihove politike:

* Spletno mesto Zoho.com / Google and Yahoo's new email sender guidelines <https://www.zoho.com/blog/zeptomail/google-yahoo-new-sender-guidelines.html>
* Spletno mesto Google podpore /Email sender guidelines

<https://support.google.com/a/answer/81126?hl=en&visit_id=638439582481182036-3491573858&rd=1>

* Spletno mesto Pravilniki, prakse in navodila / razlaga pravila pri pošiljanju poštnih sporočil uporabnikom storitve Outlook.com <https://sendersupport.olc.protection.outlook.com/pm/policies.aspx>
* Spletno mesto 'More Secure, Less Spam: Enforcing Email Standards for a Better Experience' <https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam>
* Spletno mesto Telekom.de (na poljuden način razlaga osnovna pravila varne uporabe e-pošte) <https://postmaster.t-online.de/index.en.html>