

Informacije o šifriranju e-mailova

### **Šifrirana komunikacija s dm-om**

dm pridaje veliku važnost zaštiti Vaših podataka. Kako bismo Vaše podatke zaštitili ne samo unutar dm sistema, već i tijekom prijenosa putem Interneta, podržavamo tehnologije koje omogućuju sigurnu i šifriranu komunikaciju putem e-maila.

Zašto e-mailovi dm-a imaju elektronički potpis?

Kod e-mailova je kao i kod pisama moguće navesti pogrešnu adresu pošiljatelja. Ovu mogućnost koriste prevaranti kako bi pod lažnim identitetima slali takozvane spam i phishing e-maileve koji npr. stvaraju dojam da dolaze iz dm-a, a zapravo ih šalju neovlaštene treće strane.

Kako bi se ovo spriječilo, dm svojim e-mailovima dodaje elektronički potpis. On funkcionira slično kao pečat osiguravajući da tijekom prijenosa nije došlo do manipulacije s pošiljateljem i sadržajem.

Kako mogu utvrditi je li dm zaista poslao e-mail?

Molimo Vas, uzmite u obzir da se informacije u nastavku odnose isključivo na e-maileve koje šalju izravno zaposlenici dm-a i dm služba za korisnike. Tu se ne ubrajaju dm newsletteri, promocijski e-mailovi i ostale promocijske obavijesti koje bez elektroničkog potpisa šalju poslovni partneri dm-a.

Za slanje e-mailova dm koristi adrese koje završavaju na @dm-drogeriemarkt.ba. Ako niste sigurni je li neki e-mail poslan iz dm-a, najprije provjerite završava li adresa pošiljatelja na @dm-drogeriemarkt.ba. Molimo Vas da pažljivo pogledate jer bi prevaranti mogli pokušati koristiti neku sličnu adresu poput @dn.drogeriemarkt.ba ili @dm-ba.ba.

Svakom e-mailu s adresom pošiljatelja @dm-drogeriemarkt.ba se prije slanja također dodaje elektronički potpis. Većina programa za e-maileve automatski provjerava ovaj elektronički potpis i letimičnim pogledom možete utvrditi je li e-mail zaista poslao dm, a u nastavku Vam u tom pogledu dajemo kratke upute za najčešće korištene programe. Neki programi za e-maileve ne podržavaju elektronički potpis za e-maileve, pa umjesto elektroničkog potpisa u privitku imaju datoteku pod nazivom smime.p7s. koju možete zanemariti.

Ako u nekom e-malu koji stvara dojam da dolazi iz dm-a uopće nema elektroničkog potpisa, možda ga je poslao neko ko se neovlašteno predstavlja kao dm drogerie markt. U tom slučaju biste trebali biti posebno oprezni i [o tome nas obavijestiti](#) jer se možda radi o pokušaju prevare.

Mogućnosti

Outlook

Kod poruka dm-a pokraj adrese pošiljatelja mora biti vidljiv simbol pečata. Kada se na njega klikne mora se pojaviti prozor s tekstom: „Potpisano od strane: ...@dm-drogeriemarkt.ba. Elektronički potpis u ovoj poruci je valjan i pouzdan“. Ako pečat nedostaje ili je nakon teksta „Potpisano od strane: adresa koja ne završava na @dm.hr, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

Thunderbird

Kod poruka dm-a iznad e-maila mora biti vidljiva zatvorena omotnica. Kada se na nju klikne, mora se pojaviti prozor s tekstom *“Ova poruka sadrži valjani elektronički potpis. Ova poruka nije izmijenjena od trenutka slanja.”*

Ako omotnica nedostaje, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

#### Web-aplikacija Outlook / Outlook na webu / web-sučelje sustava Office365 Outlook

Kod poruka dm-a u popisu poruka mora pokraj pošiljatelja e-maila biti vidljiv simbol pečata. Dodatne pojedinosti o certifikatu i pouzdanosti se mogu provjeriti tek nakon instaliranja dodatka za preglednik (Browser-Plugin) koji Microsoft pruža za Internet Explorer, Edge i Chrome. Tehnička napomena: Pouzdanost certifikata je u ovom slučaju moguće provjeriti samo ako je administrator programa Exchange odnosno Office365 importirao korijenski certifikat "SwissSign Silver CA - G2". Ako pečata uopće nema, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

#### Windows Live Mail

Kod poruka dm-a mora iznad e-maila biti vidljiv simbol pečata pokraj kojeg je tekst *„Elektronički potpisano i provjereno“*. Ispod se nalazi općeniti informativni tekst o elektronički potpisanim porukama, a može ga se zatvoriti klikom na „Nastavi“. Ako pečat nedostaje, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

#### Outlook za Mac

Kod poruka dm-a mora iznad e-maila biti vidljiv simbol lokota pokraj kojeg je tekst *„Ova poruka je elektronički potpisana“*. Kada se klikne na „Više informacija“, mora se pojaviti prozor s napomenom *„Ovaj certifikat je valjan“*. Ako nedostaje lokot, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

#### Apple Mail

Kod poruka dm-a iznad teksta e-maila mora biti vidljiva crna kvačica smještena u tekst *„Sigurnost: Potpisano“*. Kada se klikne na kvačicu, mora se pojaviti prozor s informacijom *„Ovo certifikat je valjan“*. Ako kvačica nedostaje, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

#### Aplikacija za e-maileve na iPhoneu / iPadu

Kod poruka dm-a pokraj pošiljatelja mora biti vidljiva plava kvačica. Prilikom dodira imena pošiljatelja mora se pojaviti prozor s tekstom *„Potpisano. Pošiljatelj je potpisao e-mail s pouzdanim certifikatom“*. Ako kvačica nedostaje, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

## Aplikacija za GMail na Android-uređajima

Ako na svom Androidu koristite aplikaciju GMail i putem nje pristupate svom GMail-računu, također možete provjeriti elektronički potpis. Za provjeru dodirnite „Prikaži više informacija“. Kod poruka dm-a tada se moraju pojaviti zelena kvačica i tekst „*Potvrđena je e-mail adresa*“. Ako kvačica nedostaje., tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane! E-mail računima drugih davatelja usluga također je moguće pristupiti putem aplikacije Gmail, no aplikacija tada ne pruža funkcionalnost za prikaz elektroničkog potpisa.

## Aplikacija Android MailDroid

Kod poruka dm-a iznad e-maila mora biti vidljiva žuta traka s tekстом „*Potpisano. Kliknite za potvrdu*“. Nakon klika za potvrdu se pojavljuje informacija o statusu potpisivanja. Tekst mora glasniti „*Potpis: OK, Putanja: OK*“. Ako nedostaje žuta traka s tekстом „*Potpisano*“ ili status potpisivanja ne glasi „*OK*“, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

## Web-sučelje Gmaila / Google-Maila

Otvorite e-mail i kliknite na trokutić s vrhom okrenutim nadolje koji se nalazi ispod adrese pošiljalca. Tada se otvara prozor. Kod poruka dm-a moraju ispod adrese primatelja biti vidljivi zelena kvačica i tekst „*Potvrđena e-mail adresa*“. Ako kvačica nedostaje, tu poruku nije potpisao dm i ona možda dolazi od neovlaštene treće strane!

## Web-sučelje web.ba

Kod poruka dm-a mora iznad e-maila biti vidljiva olovka. Putem web-sučelja nije moguće provjeriti radi li se o valjanom potpisu. No ako olovke uopće nema, možete biti sigurni da tu poruku nije potpisao dm i da ona možda dolazi od neovlaštene treće strane!

## Na koji način mogu dm-u poslati šifrirane e-maileve?

Preduslov je da ste svoj program za e-maileve konfigurirali za šifriranje e-mailova i da imate vlastiti certifikat odnosno vlastiti ključ.

dm podržava metode šifriranja S/MIME i PGP. Na stranici <https://securemail.dm.de/web.app?op=search-keys> možete preuzeti javni certifikat za e-mail adresu primatelja u dm-u. Za preuzimanje odgovarajućeg certifikata jednostavno unesite u polje za pretraživanje adresu željenog primatelja na koju želite poslati šifrirani e-mail (npr. za [info@dm-drogeriemarkt.ba](mailto:info@dm-drogeriemarkt.ba)). PGP-ključeve možete pronaći na stranici DomainKeys. Primjenjuju se na sve e-mail adrese određene domene.

Kako mogu postići da mi se e-mailevi dm-a prenose u šifriranom obliku

I ovdje je predslav da ste svoj program za e-maileve konfigurirali za šifriranje e-mailova i da imate vlastiti certifikat odnosno vlastiti ključ.

Ako se radi o certifikatu S/MIME koji je izdalo neko općeprihvaćeno certifikacijsko tijelo (npr. SwissSign, Sectigo, D-Trust, GlobalSign, Actalis, QuoVadis...), dovoljno je da na adresu primatelja u dm-u pošaljete elektronički potpisan e-mail. Svoj certifikat ili svoj PGP-ključ također u svakom trenutku možete učitati na <https://securemail.dm.de> (potrebna je jednokratna registracija). U oba prethodno navedena slučaja dm će potom na Vašu adresu slati šifrirane e-maileve.

#### Dodatne informacije za poslovne partnere

Pružaju li dm certifikate za domeniju koju šifriraju sve e-mail adrese s određenom domenom?

Da, pored individualnih certifikata za šifriranje pojedinačnih e-mail adresa dm pruža i certifikate za domeniju pomoću kojih se mogu šifrirati e-mailevi koji se šalju na bilo koju e-mail adresu s određenom domenom. Certifikati za domene mogu se preuzeti na stranici <https://securemail.dm.de/web.app?op=search-domain-keys>, a prikladni su za poslovne partnere koji za šifriranje e-mailova koriste rješenje prevoditelj protokola (*enkripcijski gateway*).

Podržavaju li dm šifriranje prijenaša između poslužitelja e-pošte putem TLS-a?

Da. Svi poslužitelji dm-a za e-poštu imaju valjane poslužiteljske certifikate i podržavaju sve uobičajene protokole za šifriranje.

dm-domene također podržavaju MTA-STS (Mail Transfer Agent Strict Transport Security). Ako sustav za e-poštu poslovnog partnera također podržava MTA-STS, on će prema poslužiteljima dm-a za e-poštu automatski prisilno pokrenuti šifriranje prijenaša putem TLS-a (Forced TLS).

Može li šifriranje prijenaša putem TLS-a zamijeniti šifriranje pomoću S/MIME ili PGP-a?

Tijekom šifriranog prijenaša putem TLS-a ne šifrira se sam e-mail, već samo prijenaš do sljedećeg poslužitelja (hop). Na njemu je e-mail ponovno raspoloživ u čitljivom obliku, prije nego se - ako je potrebno - proslijedi sljedećem poslužitelju. Ovaj oblik šifriranog prijenaša sustavi dm-a koriste kada god je to moguće kao dodatnu sigurnosnu mjeru tijekom prijenaša e-maila, neovisno je sam e-mail već šifriran ili ne.

Nadalje, za klasificiranje šifriranja prijenaša putem TLS-a kod osjetljivih e-mailova kao potpune zamjene za šifriranje pomoću S/MiME ili PGP-a potrebno je ispuniti sljedeće uvjete:

- Opcija je na raspolaganju samo poslovnim partnerima dm-a.
- Budući da se prilikom šifriranja prijenaša šifrira samo veza do sljedećeg poslužitelja gdje je mail ponovno moguće pročitati, taj sljedeći poslužitelj mora biti na raspolaganju isključivo poslovnom partneru. To isključuje rad prevoditelja protokola za e-maileve putem pružatelja zajedničkog dijeljenja resursa poslužitelja tj. usluge sigurnosti hostiranih e-mailova.

- Svi poslužitelji za e-maileve koji su uključeni u prijenos u svakom trenutku moraju imati valjane certifikate nekog općeprihvaćenog certifikacijskog tijela.
- Šifriranje prijenosa između uključenih poslužitelja putem TLS-a mora biti prisilno pokrenuto (Forced TLS), što znači da se e-mail smije prenijeti samo nakon uspješnog uspostavljanja šifrirane veze.

Koje mogućnosti dm pruža za šifriranje e-mailova poslovnih partnera?

Za šifriranje e-mailova dm pruža mogućnosti prezentirane u dokumentu [Metode šifriranja-dm](#). Za više informacija i u slučaju upita povezanih s postavljanjem certifikata molimo Vas kontaktirajte [dm službu za korisnike](#).