Tehničke preporuke za povećanje sigurnosti komunikacije elektroničkom poštom

Sadržaj

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

1. Uvod

Sigurnosni mehanizmi koji osiguravaju povjerljivost, integritet i raspoloživost informacija nisu od začetaka ugrađeni u osnovne komunikacijske protokole namijenjene razmjeni elektroničke pošte, već su se tijekom dužeg razdoblja dodavali u obliku novih dodatnih protokola ili nadogradnji postojećih protokola. Zbog postojanja većeg broja standarda koji nisu svi jednako prihvaćeni, teškoća u njihovoj implementaciji te nesigurnih standardnih postavki poslužitelja koji sudjeluju u razmjeni elektroničke pošte, presretanje elektroničke pošte i lažiranje pošiljatelja poruke elektroničke pošte i dalje predstavljaju stvarnu prijetnju.

Prilikom slanja poruke elektroničke pošte od pošiljatelja do primatelja, poruka putuje kroz niz poslužitelja kroz različite računalne mreže. Standardi razmjene elektroničke pošte i dalje izričito propisuju prijenos poruke nezaštićenim komunikacijskim kanalom, što predstavlja mogućnost presretanja poruke te narušavanje njene povjerljivosti i/ili integriteta. S ciljem zaštite poruke elektroničke pošte u prijenosu, potrebno je poslužitelje elektroničke pošte konfigurirati na način da se prijenos poruke obavlja kroz zaštićeni komunikacijski kanal.

Osim mogućnosti presretanja poruka, temeljni standardi na kojima se zasniva komunikacija elektroničkom poštom omogućavaju relativno jednostavno lažiranje pošiljatelja poruke elektroničke pošte. Poruke elektroničke pošte s lažnim pošiljateljem predstavljaju podskup neželjenih poruka elektroničke pošte (engl. s*pam*), no njihov cilj uglavnom se razlikuje od "tradicionalnih" *spam* poruka − najčešći cilj *spam* poruka je ostvarivanje financijske dobiti reklamiranjem i prodajom proizvoda i usluga ili poticanjem na brzu zaradu. Lažiranjem pošiljatelja poruke, napadač primatelja nastoji uvjeriti u autentičnost poruke i iskoristiti njegovo povjerenje u navodnog pošiljatelja. Poruke s lažiranim pošiljateljem zbog toga se najčešće koriste za provedbu *phishing* napada ili narušavanje reputacije osobe ili organizacije u čije se ime šalje poruka elektroničke pošte.

Tijekom godina razvili su se zaštitni mehanizmi koji ograničavaju lažiranje pošiljatelja poruke elektroničke pošte, a tri najistaknutija mehanizma su:

- **SPF** (engl. *Sender Policy Framework*)
- **DKIM** (engl. *DomainKeys Identified Mail*) i
- **DMARC** (engl. *Domain-based Message Authentication, Reporting & Conformance*)

Sva tri mehanizma temelje se na postavkama DNS poslužitelja te je za njihovo postavljanje potrebno dodati odgovarajuće DNS zapise.

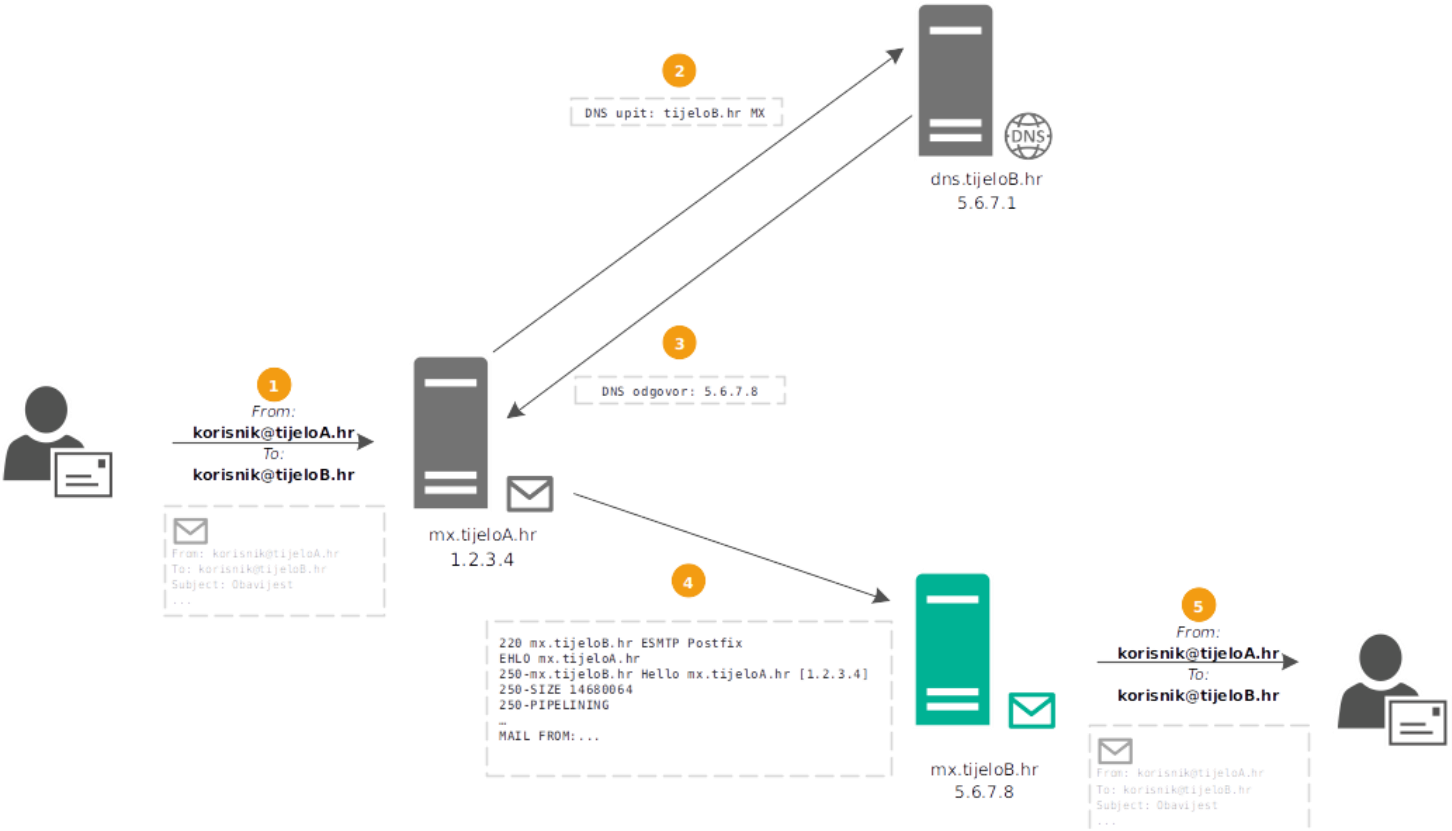
U nastavku dokumenta navedene su tehničke smjernice za konfiguraciju poslužitelja elektroničke pošte koji se nalazi na perimetru organizacije (MTA – engl. *Message Transfer Agent* ili MX – engl. *Message Exchanger* poslužitelj) i DNS poslužitelja u organizaciji temeljene na prethodno navedenim mehanizmima kojima se presretanje poruka i slanje lažiranih poruka elektroničke pošte svodi na najmanju moguću mjeru.

Zavod za sigurnost informacijskih sustava (ZSIS) ovim smjernicama želi osigurati razmjenu poruka elektroničke pošte s drugim poslužiteljima putem sigurnog komunikacijskog kanala te spriječiti slanje lažiranih poruka elektroničke pošte u ime državnih tijela, jedinica lokalne i područne (regionalne) samouprave te pravnih osobama s javnim ovlastima kao i narušavanje reputacije tih tijela, mogućnost njihove pojave na "crnim listama" (engl. *mail blacklist*) te posljedičnu nemogućnost slanja elektroničke pošte.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

2. STARTTLS

Razmjena poruka elektroničke pošte između poslužitelja elektroničke pošte obavlja se putem SMTP protokola (engl. *Simple Mail Transfer Protocol*). SMTP protokol je tekstualni protokol u kojem se pojedini detalji razmjene kao i same poruke elektroničke pošte prenose u **izvornom obliku**, tj. putem nezaštićenog komunikacijskog kanala. Primjer razmjene poruke elektroničke pošte između dva tijela državne uprave (*Tijelo A* i *Tijelo B*) prikazan je na sljedećoj slici:



Slika 1: Slanje poruke elektroničke pošte iz *Tijela A* u *Tijelo B*

Pojedini koraci opisani su u nastavku:

1. Korisnik informacijskog sustava u *Tijelu A* (adresa: *korisnik@tijeloA.hr*) šalje poruku elektroničke pošte prema korisniku u *Tijelu B* (adresa: *korisnik@tijeloB.hr*) na uobičajen način, koristeći se klijentom/preglednikom elektroničke pošte (npr. *Outlook*).
2. Poslužitelj elektroničke pošte u *Tijelu A* (*mx.tijeloA.hr*/1.2.3.4) zaprima poruku elektroničke pošte te šalje DNS upit s ciljem dohvata MX zapisa za domenu *tijeloB.hr*.

   Napomena: Iako je na slici prikazan direktan DNS upit prema poslužitelju autoritativnom za *Tijelo B*, u stvarnoj situaciji bit će poslan niz rekurzivnih DNS upita, no rezultat je isti – odgovor koji sadrži IP adresu poslužitelja elektroničke pošte za domenu *tijeloB.hr*.
3. DNS poslužitelj odgovara s IP adresom MX poslužitelja domene *tijeloB.hr.*
4. Poslužitelj elektroničke pošte *Tijela A* uspostavlja mrežnu vezu s poslužiteljem elektroničke pošte u *Tijelu B* čiju je IP adresu upravo doznao. Mrežna veza uspostavlja se na standardnom mrežnom portu 25/TCP korištenjem SMTP protokola.
5. Poslužitelj elektroničke pošte dostavlja poruku primatelju.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

U koraku 4., poruka elektroničke pošte putuje po nezaštićenoj računalnoj mreži (internetskoj infrastrukturi) u nezaštićenom obliku – napadač koji ima mogućnost nadzora mrežnog prometa može presresti proizvoljnu poruku elektroničke pošte te pročitati i/ili izmijeniti njen sadržaj (ukoliko isti nije zaštićen nekim drugim mehanizmom). SMTP komunikacija prikazana je u nastavku (oznaka *S* označava poslužitelj elektroničke pošte koji zaprima poruku, dok oznaka *C* predstavlja klijenta, tj. poslužitelj elektroničke pošte koji šalje poruku):

```
S: 220 mx.tijeloB.hr ESMTP
C: EHLO mx.tijeloA.hr
S: 250-mx.tijeloB.hr
S: 250-PIPELINING
S: 250-SIZE 102400000
S: 250-VRFY
S: 250-ETRN
S: 250 8BITMIME
C: MAIL FROM:<korisnik@tijeloA.hr>
S: 250 Ok
C: RCPT TO:<korisnik@tijeloB.hr>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: <slanje poruke, zajedno sa zaglavljima, naslovom i tijelom>
C: .
S: 250 Ok: queued as 31DAA4E00DD
C: QUIT
```

S ciljem sprječavanja narušavanja povjerljivosti i integriteta razvijen je dodatak na SMTP protokol u obliku dodatne naredbe pod nazivom **STARTTLS**.

STARTTLS mehanizam omogućava „nadogradnju“ mrežne veze koja je uspostavljena u izvornom obliku u kriptirani komunikacijski kanal zaštićen TLS protokolom, tj. pripadnim algoritmima enkripcije podataka. Primjer SMTP komunikacije u kojoj poslužitelj elektroničke pošte u *Tijelu B* podržava STARTTLS naredbu prikazan je u nastavku:

```
S: 220 mx.tijeloB.hr ESMTP
C: EHLO mx.tijeloA.hr
S: 250-mx.tijeloB.hr
S: 250-PIPELINING
S: 250-STARTTLS
S: 250-SIZE 102400000
S: 250-VRFY
S: 250-ETRN
S: 250 8BITMIME
C: STARTTLS
S: 220 Ready to start TLS
C: EHLO mx.tijeloA.hr
S: 250-mx.tijeloB.hr
S: 250-PIPELINING
S: 250-SIZE 102400000
S: 250-VRFY
S: 250-ETRN
S: 250 8BITMIME
C: MAIL FROM:<korisnik@tijeloA.hr>
S: 250 Ok
C: RCPT TO:<korisnik@tijeloB.hr>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: <slanje poruke, zajedno sa zaglavljima, naslovom i tijelom>
C: .
S: 250 Ok: queued as 31DAA4E00DD
C: QUIT
```


Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Za razliku od komunikacije s poslužiteljem koji ne podržava STARTTLS mehanizam, u ovom slučaju poslužitelj u *Tijelu B* podržava STARTTLS mehanizam (označeno žutom bojom). Ukoliko klijent također podržava (ili eksplicitno zahtijeva) STARTTLS mehanizam, izdat će naredbu STARTTLS (označeno tamnozelenom bojom), nakon čega će se uspostaviti kriptirana TLS sjednica i sve daljnje naredbe izmjenjivat će se kroz siguran komunikacijski kanal. U prethodnom isječku, crvenom bojom označene su naredbe koje se prenose u izvornom obliku, dok se naredbe i odgovori poslužitelja označeni zelenom bojom prenose zaštićenim komunikacijskim kanalom.

Svi moderni transportni poslužitelji elektroničke pošte podržavaju STARTTLS mehanizam. Zbog razlika u načinu parametriziranja i konfiguracije navedenog mehanizma za različite inačice poslužitelja elektroničke pošte, u nastavku su navedene općenite smjernice. Za detaljnije informacije, potrebno je slijediti službene upute za konkretnu inačicu.

2.1. Konfiguracija na strani pošiljatelja (izlaz poruka)

Parametrizacija u kontekstu pošiljatelja poruka elektroničke pošte (tj. MTA poslužitelja koji se u svojstvu klijenta povezuje s drugim MTA poslužiteljem radi prijenosa poruke) znatno je jednostavnija od konfiguracije na strani primatelja poruka. Većina poslužitelja elektroničke pošte će za izlazne poruke (tj. pri uspostavi veze s drugim MTA poslužiteljima) automatski koristiti STARTTLS mehanizam, ako ga drugi poslužitelj podržava (tzv. oportunistička enkripcija), a dodatne postavke poslužitelja dozvoljavaju definiranje razine sigurnosti i parametre kriptiranja sjednice. Standardne razine sigurnosti navedene su u nastavku:

- **Bez TLS sjednice** – najniža razina sigurnosti, TLS sjednica neće biti uspostavljena korištenjem STARTTLS naredbe.
- **Oportunistička enkripcija** – TLS sjednica je preferirana u odnosu na komunikaciju u izvornom obliku. Ako drugi poslužitelj elektroničke pošte podržava uspostavu sigurne sjednice, ona će biti uspostavljena. U protivnom, komunikacija će se odvijati u izvornom obliku.
- **Obavezna enkripcija** – komunikacija se obavlja isključivo putem TLS sjednice. Ako poslužitelj ne podržava STARTTLS mehanizam, ova postavka uzrokuje prekid komunikacije i poruka neće biti isporučena primatelju.

Osim opisanih razina sigurnosti, neke inačice poslužitelja elektroničke pošte pružaju dodatne razine sigurnosti, poput oportunističke enkripcije uz dodatnu provjeru ispravnosti digitalnog certifikata kojeg pruža druga strana (ako certifikat nije ispravan, ako nije potpisan od odgovarajućeg certifikacijskog tijela ili je istekao, komunikacijska veza će biti prekinuta ili će se sjednica odvijati putem nezaštićenog komunikacijskog kanala).

Preporučena razina sigurnosti

Usprkos činjenici da postoje veće razine sigurnosti, preporuka je na poslužitelju podesiti **oportunističku enkripciju** (drugi naziv je preferirana enkripcija). Vrlo veliki broj poslužitelja elektroničke pošte na Internetu ima nesigurne postavke te nema mogućnost uspostave zaštićenog komunikacijskog kanala korištenjem STARTTLS naredbe. Korištenjem oportunističke enkripcije, poruke će ipak biti dostavljene i primateljima u organizacijama koje koriste tako postavljene poslužitelje – strožije i sigurnije postavke uzrokovale bi probleme u dostavi poruka željenim primateljima ili bi u potpunosti onemogućile njihovu isporuku.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Ipak, preporuča se nadzor i pregled komunikacije s MTA poslužiteljima partnerskih organizacija s kojima se provodi učestala komunikacija elektroničkom poštom. Ako se sa sigurnošću može ustanoviti da partnerska organizacija koristi poslužitelj koji podržava uspostavu sigurnog komunikacijskog kanala, za sve takve organizacije preporuča se koristiti **obaveznu enkripciju**. Većina poslužitelja elektroničke pošte dozvoljava postavljanje eksplicitne liste poslužitelja za koje se zahtijeva uspostava sigurnog komunikacijskog kanala.

Također, potrebno je napomenuti da ako organizacija koristi pružatelje usluge elektroničke pošte u oblaku, postoji vrlo velika vjerojatnost da je oportunistička enkripcija s odgovarajućim parametrima već postavljena. Postavke STARTTLS mehanizma u tom slučaju je potrebno provjeriti i koordinirati s pružateljem usluge.

Uz razinu sigurnosti, većina poslužitelja elektroničke pošte pruža mogućnost definiranja parametra kriptiranja (kao jedan ili više konfiguracijskih parametara) – inačicu TLS protokola, korištene algoritme kriptiranja i sl. Odabir ispravnih postavki nije jednostavan, zbog potrebnog kompromisa između najveće moguće razine sigurnosti i činjenice da poslužitelj s kojim se uspostavlja sjednica možda ne podržava modernije i sigurnije postavke. Također, ako poslužitelj elektroničke pošte na kojem se obavlja konfiguracija nije ažuran, postoji velika vjerojatnost da sigurne postavke nisu podržane zbog zastarjelosti. U tom slučaju, svakako se preporuča nadogradnja poslužitelja na zadnju dostupnu inačicu. Zbog činjenice da je oportunistička enkripcija odabrana kao preporučena razina zaštite, poruka će uvijek biti isporučena, čak i kada poslužitelji zbog nekompatibilnih postavki ne uspiju uspostaviti sigurnu sjednicu. Preporuke su navedene u nastavku:

Preporučene postavke TLS sjednice

1. Koristiti TLS protokol inačice **1.2** ili **1.3**.
   TLS protokol inačice **1.3** je protokol objavljen krajem 2018. godine te još nije u širokoj upotrebi, iako predstavlja najsigurniju inačicu.
   Dodatno, potrebno je **eksplicitno zabraniti** zastarjele inačice TLS protokola – SSLv2, SSLv3 i TLSv1 (uglavnom korištenjem konfiguracijske postavke `!SSLv2,!SSLv3,!TLSv1`).
   TLS protokol inačice **1.1** trenutačno je dozvoljeno koristiti, ali ga je preporučljivo zamijeniti novijim inačicama te u budućnosti napustiti podršku za taj protokol.
2. Za razmjenu kriptografskih ključeva koristiti *Diffie-Hellman* algoritam razmjene ključeva temeljen na eliptičnim krivuljama (**ECDHE**) ili konačnim poljima (**DHE**).
3. Kao simetrični algoritam za kriptiranje preporuča se koristiti algoritme koji kombiniraju enkripciju i autentifikaciju (tzv. AEAD algoritme – engl. *Authenticated Encryption With Associated Data*), npr. **AES-GCM** (s veličinom ključeva od 128 ili 256 okteta) ili **ChaCha20-Poly1305**.
4. Za potrebe sažimanja podataka preporuča se koristiti **SHA-256** ili **SHA-384** algoritme.
5. Skup algoritama i postavki po preferencijama (tj. prioritetima od najsigurnijeg prema manje sigurnima) preporuča se postaviti kao u sljedećoj listi (nazivi algoritama koriste standardizirana imena koja se koriste u SSL/TLS bibliotekama) [1]:
   - `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
   - `TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256`
   - `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
   - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
   - `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Više informacija o preporučenim skupovima algoritama moguće je pronaći u smjernicama za uspostavu sigurnih TLS sjednica nizozemskog Nacionalnog centra za kibernetičku sigurnost [1], a za konkretne konfiguracijske postavke preporuča se korištenje službenih uputa ili javno dostupnih izvora informacija [2].

2.2. Konfiguracija na strani primatelja (ulaz poruka)

Konfiguracijske postavke na strani primatelja djelomice su slične onima na strani pošiljatelja, u kontekstu postavki sigurnosne razine i željenih kriptografskih parametara:

Preporučena razina sigurnosti

Slično strani pošiljatelja, preporučena razina sigurnosti je **preferirana/oportunistička enkripcija**. Na taj način će poslužitelj uvijek ponuditi klijentu mogućnost uspostave kriptirane sjednice, a većina MTA poslužitelja u svojstvu klijenta će podržati uspostavu kriptirane sjednice. Ako klijent ne podržava uspostavu kriptirane sjednice, komunikacija će se nastaviti odvijati u izvornom obliku i neće doći do gubitka poruke.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Preporučene postavke TLS sjednice

1. Odabrati parametre TLS sjednice koji su istovjetni preporukama prethodno navedenima za stranu pošiljatelja (tj. MTA klijent).
2. Osigurati da se skupovi algoritama postavljeni na poslužitelju primjenjuju kao referentna lista algoritama, pri čemu klijent zatim odabire jedan od ponuđenih algoritama po vlastitim mogućnostima (prema standardnim postavkama, klijentska lista algoritama je referentna lista, što može rezultirati uspostavom sjednice korištenjem manje sigurnih algoritama). U nekim inačicama poslužitelja elektroničke pošte ovo svojstvo je automatski omogućeno nakon definiranja liste željenih skupova algoritama, dok se kod nekih inačica opcija mora eksplicitno omogućiti (npr. opcije `ssl_prefer_server_ciphers` u Dovecot poslužitelju, `tls_preempt_cipherlist` u Postfix poslužitelju i sl.).

Za razliku od strane pošiljatelja, na primateljskoj strani potrebno je posjedovati odgovarajući digitalni certifikat (x.509 certifikat).

Preporučene postavke digitalnog certifikata na poslužitelju elektroničke pošte

1. Prilikom stvaranja digitalnog certifikata, odabrati sigurne postavke privatnog ključa.
   - Ako se stvara certifikat temeljen na eliptičnim krivuljama (ECDSA algoritam za provjeru digitalnog potpisa certifikata) tada se preporuča korištenje algoritma **ECDSA-256** s krivuljom **P-256** i korištenje **SHA-256** algoritma sažimanja. U nastavku je navedena naredba alata `openssl` pomoću kojeg je moguće stvoriti ključ i zahtjev za potpisivanje certifikata (CSR – engl. *Certificate Signing Request*) s navedenim svojstvima:

     ```
     openssl ecparam -out server.key -name prime256v1 –genkey
     openssl req -new -key server.key -out server.csr -sha256
     ```

   - Ako se stvara certifikat temeljen na RSA algoritmu, tada se preporuča korištenje veličine ključa od **barem 2048** okteta i **SHA-256** algoritma sažimanja. Openssl naredba za stvaranje takvog ključa navedena je u nastavku:

     ```
     openssl req -new -newkey rsa:2048 -nodes -keyout server.key -
     out server.csr
     ```

   Iako privatni ključevi/certifikati temeljeni na eliptičnim krivuljama imaju znatno bolje performanse i sigurnosna svojstva od ključeva/certifikata temeljenih na RSA algoritmu, postoji mogućnost da klijentska strana ne podržava takve certifikate. Zbog korištene oportunističke enkripcije, u takvim slučajevima komunikacija neće biti zaštićena.
2. U zahtjevu za potpisivanje certifikata preporuča se kao *Common Name* parametar koristiti FQDN naziv MX poslužitelja, ako je moguće.
3. Zahtjev za potpisivanje certifikata preporuča se poslati općeprihvaćenom certifikacijskom autoritetu (CA – engl. *Certificate authority*) s ciljem uspostave cjelokupnog *lanca povjerenja* (engl. *chain of trust*). Umjesto plaćenih certifikata, moguće je korištenje i besplatnih servisa (*Let's Encrypt*) za potpisivanje/izdavanje certifikata, uz napomenu da je takve certifikate potrebno češće mijenjati i administrirati.
4. Podesiti poslužitelj elektroničke pošte s ciljem korištenja potpisanog certifikata.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Mora li x.509 certifikat na poslužitelju elektroničke pošte biti potpisan od strane prihvaćenog certifikacijskog autoriteta?

Velika većina poslužitelja elektroničke pošte trenutno ne provjerava ispravnost digitalnog certifikata MTA poslužitelja s kojim se uspostavlja TLS sjednica, zbog činjenice da većina poslužitelja koristi vlastito-potpisane (engl. *self-signed*) certifikate, tj. certifikate koji nisu potpisani od strane prihvaćenog certifikacijskog autoriteta. Neprihvaćanje takvih certifikata rezultiralo bi neisporučenim porukama elektroničke pošte, što je neprihvatljivo.

Iako je za potrebe uspostave TLS sjednice moguće i dozvoljeno koristiti vlastito-potpisane certifikate, njihova upotreba se ipak **ne preporučuje** − postoje besplatni servisi koji izdaju važeće certifikate, a pojedini poslužitelji ipak provjeravaju ispravnost certifikata te na temelju rezultata provjere mogu odbiti isporuku ili postaviti dodatne oznake na poruku (npr. moguća neželjena pošta i sl.).

2.3. Sigurnost STARTTLS mehanizma

STARTTLS mehanizam predstavlja nadogradnju SMTP protokola koji je nastao kao najprikladniji odgovor na problem nezaštićene komunikacije između MTA poslužitelja u trenutku kada nisu postojali alternativni mehanizmi zaštite. Najveći problem mehanizma je činjenica da se uspostava kriptirane sjednice obavlja *nakon* što je nezaštićeni komunikacijski kanal između MTA poslužitelja već uspostavljen. Napadač koji ima mogućnost presretanja i izmjene mrežnog prometa (tzv. MitM – *Man in the Middle*) može vrlo jednostavno modificirati odgovor poslužitelja i ukloniti mogućnost uspostave kriptirane sjednice (tj. odgovoriti klijentu da MTA poslužitelj *ne podržava* STARTTLS mehanizam). MTA poslužitelj klijent će u tom slučaju pretpostaviti da odredišni poslužitelj ne podržava uspostavu sigurne sjednice te će nastaviti sjednicu u nezaštićenom obliku.
Također, zbog činjenice da većina MTA poslužitelja ne provjerava ispravnost x.509 certifikata, napadač može jednostavno poslati klijentu svoj vlastito-potpisani certifikat koji će biti prihvaćen te na taj način kroz vlastiti poslužitelj prenositi podatke u čitljivom obliku, dok će izvorišni i odredišni MTA poslužitelj imati iluziju da je između njih uspostavljen zaštićeni komunikacijski kanal.

Iako STARTTLS mehanizam posjeduje vrlo jasne i izražene ranjivosti, on ipak pruža zaštitu od *pasivnog nadzora* − napadač koji nema mogućnost aktivnog djelovanja prema strani pošiljatelja ili strani primatelja ne može vidjeti sadržaj kriptirane sjednice.

2.4. Alternativni sigurnosni mehanizmi

Razvojem tehnologije, ali i zbog sve izraženijih prijetnji suvremenoj komunikaciji putem elektroničke pošte, razvila su se i alternativna i sigurnija rješenja za zaštitu komunikacijskog kanala između MTA poslužitelja. Trenutačna alternativna rješenja navedena su u nastavku:

- **DANE** (engl. *DNS-based Authentication of Named Entities*) - sigurnosni mehanizam koji se temelji na dodavanju novog zapisa u DNS poslužitelj. Navedeni zapis (zapis tipa *TLSA*) sadržava kriptografski sažetak certifikata koji se koristi za uspostavu sigurne sjednice na MTA poslužitelju. U slučaju korištenja DANE mehanizma, klijentski MTA poslužitelj najprije provjerava postojanje TLSA zapisa te uspoređuje sažetak u zapisu sa sažetkom certifikata kojeg je ponudio poslužitelj na strani primatelja. Ako su sažetci istovjetni, uspostavljena je sigurna sjednica.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Velika prednost DANE mehanizma jest nemogućnost napadača da lažira nedostatak mogućnosti uspostave sigurne sjednice, kao i korištenje vlastitog certifikata, jer su informacija o dostupnosti sigurne sjednice i sažetak (*digitalni otisak*) ispravnog certifikata sadržani u DNS zapisu. Također, DANE mehanizam ne zahtijeva postojanje treće strane (certifikacijskog autoriteta) koja jamči za autentičnost certifikata, već je potpuna kontrola identiteta nad vlasnikom domene, odnosno DNS zone.
Izraziti nedostatak DANE mehanizma jest nužnost prethodne uspostave DNSSEC zaštite na razini DNS poslužitelja (bez DNSSEC zaštite i provjere ispravnosti zapisa na strani klijentskog MTA poslužitelja, napadač može poslati proizvoljne nepotpisane DNS zapise i na taj način u potpunosti narušiti sigurnost mehanizma). Dodatno, pojedini poslužitelji elektroničke pošte još ne podržavaju DANE mehanizam, iako razina kompatibilnosti kontinuirano raste.

- **MTA-STS** (engl. *MTA Strict Transport Security*) − sigurnosni mehanizam koji se temelji na *sigurnosnoj politici* koja se nalazi na web poslužitelju točno određenog imena na točno određenoj lokaciji (naziv poslužitelja mora biti *mta-sts.domena.hr*, a putanja do politike *https://mta-sts.domena.hr/.well-known/mta-sts.txt*). Politikom se specificiraju nazivi MX poslužitelja te vremenski rok čuvanja informacija iz politike na klijentskoj strani. Dodatno, korištenjem posebnog DNS zapisa organizacija objavljuje činjenicu da MTA poslužitelj podržava MTA-STS mehanizam.
  Klijentski MTA poslužitelj provjerom DNS zapisa može ustanoviti da poslužitelj na strani primatelja podržava uspostavu sigurne sjednice te na taj način uspostaviti sigurnu sjednicu, praćenjem objavljene politike.
  Prednost MTA-STS mehanizma jest eliminiranje potrebe za DNSSEC zaštitom, kao i nešto jednostavnija konfiguracija u odnosu na DANE.
  Nedostaci su potreba za dodatnim (web) poslužiteljem te činjenica da ovaj mehanizam pruža nižu razinu zaštite nego DANE mehanizam − tzv. *TOFU* (engl. *trust on first use*) princip. Također, opisani sigurnosni mehanizam je izrazito nov i nedovoljno raširen te je razina kompatibilnosti poslužitelja elektroničke pošte s MTA-STS mehanizmom vrlo malena (tvrtka Google je nedavno započela s korištenjem MTA-STS mehanizma u vlastitoj infrastrukturi te se zbog toga očekuju velike promjene u razini prihvaćenosti).

Oba mehanizma u ovom su trenutku izvan opsega ovog dokumenta te je za njihov detaljniji opis i način konfiguracije potrebno proučiti same standarde i javno dostupne smjernice za njihovu implementaciju.

Zaštita sadržaja poruka elektroničke pošte

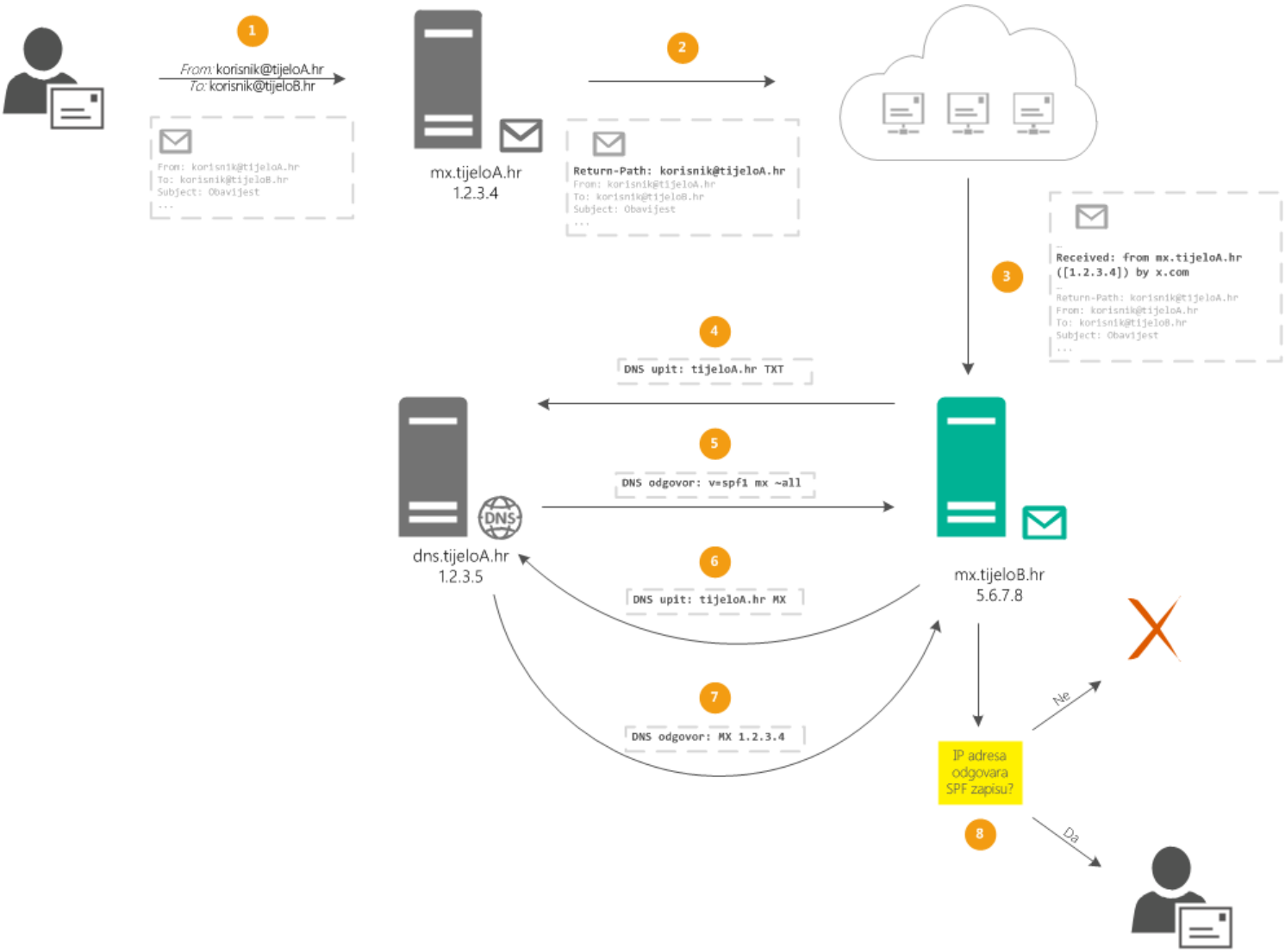
Svi prethodno mehanizmi predstavljaju isključivo zaštitu **transporta** poruka između dva poslužitelja elektroničke pošte na perimetru organizacija ili unutar organizacija (ako je potrebno).
Smjernice u ovom dokumentu **ne obuhvaćaju** mehanizme zaštite sadržaja poruke elektroničke pošte *od korisnika do korisnika* (engl. *end-to-end*). Takvi mehanizmi ne provode se automatski, već gotovo isključivo zahtijevaju korisničku interakciju, uspostavu određene razine podupiruće PKI infrastrukture te razmjenu ključeva sa svim korisnicima s kojima se zaštićene poruke žele razmjenjivati.
ZSIS je razvio vlastito rješenje za zaštitu elektroničke pošte od korisnika do korisnika kojom se razmjenjuju klasificirani podaci do stupnja tajnosti *Ograničeno* (*ZSIS e-Kript*), a postoje i druga prihvaćena rješenja (*PGP* i *S/MIME*).
Korištenje i ispravne postavke takvih sigurnosnih mehanizama nisu u opsegu ovog dokumenta.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

3. SPF

SPF (engl. *Sender Policy Framework*) predstavlja tehnički standard koji omogućava vlasniku domene s koje se šalju poruke elektroničke pošte definiranje IP adresa dozvoljenih pošiljatelja poruka za navedenu domenu te politike postupanja s porukama koje ne zadovoljavaju definirane uvjete. Na taj način odredišni poslužitelj elektroničke pošte može prilikom primitka poruke provjeriti da li je pošiljatelj poruke (tj. izvorišna IP adresa) "autoriziran" za slanje elektroničke pošte za tu domenu te s porukom postupiti u skladu s definiranom politikom.

Pojednostavljeni prikaz rada SPF mehanizma prikazan je na sljedećoj slici koja opisuje postupak slanja poruke elektroničke pošte iz *Tijela A* u *Tijelo B*, pri čemu *Tijelo A* ima postavljen SPF zapis:



Slika 2: Postupak slanja poruke elektroničke pošte i provjera SPF zapisa

Pojedini koraci detaljno su opisani u nastavku:

1. Korisnik informacijskog sustava u *Tijelu A* (adresa: *korisnik@tijeloA.hr*) šalje poruku elektroničke pošte prema korisniku u *Tijelu B* (adresa: *korisnik@tijeloB.hr*) na uobičajen način, koristeći se klijentom/preglednikom elektroničke pošte (npr. *Outlook*).

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

2. Poslužitelj elektroničke pošte u *Tijelu A* imena *mx.tijeloA.hr* i IP adrese 1.2.3.4 zaprima poruku elektroničke pošte, postavlja `Return-Path` parametar zaglavlja poruke na vrijednost `korisnik@tijeloA.hr` te ju prosljeđuje MX poslužitelju elektroničke pošte u *Tijelu B* ili drugom poslužitelju elektroničke pošte kao posredniku u dostavi poruke do odredišta. `Return-Path` parametar zaglavlja naziva se još i *adresa pošiljatelja u omotnici poruke* (engl. *envelope sender address*) i razlikuje se od *adrese pošiljatelja u zaglavlju poruke* (engl. *header sender address*) koja je navedena u `From` parametru zaglavlja. `Return-Path` parametar koristi se prije svega kao odredište povratnih poruka u slučaju nemogućnosti isporuke poruke pošiljatelju (engl. *bounce address*) i ne prikazuje se u klijentu elektroničke pošte, već se u klijentu prikazuje `From` parametar. `Return-Path` parametar ključan je za djelovanje SPF mehanizma, kao što je opisano u sljedećim koracima.
3. Prilikom primitka poruke elektroničke pošte, poslužitelj elektroničke pošte u *Tijelu B* (*mx.tijeloB.hr* s adresom 5.6.7.8) pregledava zaglavlje poruke te na temelju `Return-Path` parametra identificira izvorišnu domenu poruke – *tijeloA.hr*.
4. Poslužitelj *mx.tijeloB.hr* postavlja DNS upit prema DNS poslužitelju autoritativnom za *Tijelo A* (*dns.tijeloA.hr*), tražeći sve DNS zapise tipa TXT.
5. DNS poslužitelj *dns.tijeloA.hr* odgovara sa postojećim TXT zapisima. U opisanom slučaju, kao odgovor na upit šalje se jedan zapis sadržaja `v=spf1 mx ~all`. Navedenim zapisom domena *tijeloA.hr* označava da su „legitimne“ samo one poruke elektroničke pošte koje dolaze s izvorišne adrese poslužitelja elektroničke pošte (MX DNS zapis). Sve ostale poruke nisu legitimne, a odredišnom poslužitelju prepušta se odluka o postupanju s takvim porukama. Format TXT zapisa koji se odnose na SPF mehanizam bit će detaljno objašnjen u nastavku dokumenta.
6. Budući da je u SPF zapisu kao legitimna adresa navedeno ime MX poslužitelja (parametar `mx`), poslužitelj *mx.tijeloB.hr* provodi još jedan DNS upit prema *dns.tijeloA.hr* kako bi doznao adresu poslužitelja elektroničke pošte (tj. poslužitelj traži MX zapis za domenu *tijeloA.hr*.
7. DNS poslužitelj *dns.tijeloA.hr* odgovara s adresom koja odgovara MX zapisu – 1.2.3.4
8. Poslužitelj elektroničke pošte *mx.tijeloB.hr* uspoređuje primljenu adresu (1.2.3.4) s izvorišnom adresom (u ovom slučaju 1.2.3.4) te, zbog pozitivnog rezultata usporedbe, prosljeđuje poruku primatelju (*korisnik@tijeloB.hr*). U slučaju da poruka nema izvorišnu adresu 1.2.3.4, zbog parametra `~all` u SPF zapisu, s porukom će se postupiti prema postavkama na poslužitelju *mx.tijeloB.hr* (poruka može biti označena kao neželjena pošta, može biti odbačena, vraćena pošiljatelju i sl.).

Temelj SPF mehanizma predstavlja odgovarajući TXT zapis na autoritativnom DNS poslužitelju.

TXT ili SPF zapis?

Stari SPF standard koji je bio u upotrebi do 2014. definirao je poseban tip DNS zapisa – SPF zapis. Promjene koje su 2014. godine nastupile u standardu eksplicitno navode da je jedini dozvoljeni tip DNS zapisa za SPF upravo tip TXT (numerički tip 16) te se SPF zapis (numerički tip 99) prestaje koristiti.

TXT zapis ima oblik jedne linije u posebnom formatu.

Može li se koristiti veći broj SPF zapisa istovremeno?

Veći broj TXT zapisa koji se odnose na SPF mehanizam **nije dozvoljeno koristiti**. U takvom slučaju odredišni poslužitelj elektroničke pošte ne zna koji TXT zapis označava korišteni SPF mehanizam te provjera SPF zapisa sa strane primatelja rezultira porukom o greški. Za potrebe SPF mehanizma koristi se **isključivo jedan DNS zapis tipa TXT**.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Primjer jednog DNS zapisa naveden je u nastavku:

```
tijelo.hr.  TXT  "v=spf1 a mx ip4:1.2.3.4 -all"
```

Elementi zapisa opisani su u sljedećoj tablici:

`v=spf1`	Oznaka korištene inačice SPF mehanizma. Trenutno uvijek `v=spf1`.
`a`	Za slanje poruka elektroničke pošte za domenu *tijelo.hr* dozvoljeno je koristiti poslužitelj čija IP adresa odgovara DNS zapisu tipa A ili AAAA (adresni zapis) za tu domenu.
`mx`	Poruka je legitimna ukoliko je izvorišna adresa jednaka IP adresi definiranoj za MX poslužitelj za domenu *tijelo.hr* (tj. poruka je legitimna ukoliko dolazi s mail exchange poslužitelja domene *tijelo.hr*). Ovaj element zapisa ima najviši prioritet i prvi se provjerava.
`ip4:1.2.3.4`	Poruka je legitimna ukoliko je izvorišna adresa jednaka IP adresi 1.2.3.4.
`-all`	Ukoliko poruka ne zadovoljava niti jedan od prethodno navedenih uvjeta, potrebno ju je eksplicitno odbiti!

„Elementi“ koji predstavljaju dozvoljene pošiljatelje poruka za određenu domenu nazivaju se *mehanizmi* u SPF terminologiji. Popis mehanizma prikazan je u sljedećoj tablici:

`all`	Sve IP adrese legitimni su pošiljatelji poruka elektroničke pošte. Ovaj mehanizam koristi se uglavnom na kraju SPF zapisa.
`a`	Ako je izvorišna IP adresa poruke elektroničke pošte jednaka *bilo kojem* DNS zapisu tipa A, uvjet je zadovoljen.
`mx`	Ako je izvorišna IP adresa poruke elektroničke pošte jednaka *adresi* MX zapisa, uvjet je zadovoljen.
`ip4`	Ako je izvorišna IP adresa jednaka navedenoj adresi ili se nalazi u zadanom rasponu adresa, uvjet je zadovoljen.
`ip6`	Isto kao `ip4`, samo za IP verziju 6.
`ptr`	DNS ime koje odgovara izvorišnoj IP adresi mora odgovarati postavljenom nazivu za zadovoljavanje uvjeta. **Ovaj tip zapisa se ne preporučuje koristiti!**
`exists`	Ako je DNS upit za A zapisom domene koja je navedena uz mehanizam `exists` uspješan, uvjet je zadovoljen. Rezultat DNS upita je nebitan za zadovoljavanje upita.
`include`	Svi mehanizmi koji su zadovoljeni za domenu navedenu uz `include` mehanizam, zadovoljavaju i ovaj uvjet.

Uz svaki mehanizam može biti naveden *kvalifikator*:

`+`	`Pass` – ukoliko izvorišna IP adresa zadovoljava mehanizam, tada je poruka prihvaćena. Ako uz mehanizam nije naveden niti jedan drugi kvalifikator, podrazumijeva se ovaj kvalifikator.
`-`	`Fail` – ukoliko izvorišna IP adresa zadovoljava mehanizam, tada takva poruka ne smije biti prihvaćena.
`~`	`SoftFail` – ukoliko izvorišna IP adresa zadovoljava mehanizam, tada se takva poruka privremeno prihvaća, ali o konačnom prihvaćanju odlučuje odredišni poslužitelj elektroničke pošte.
`?`	`Neutral` – domena eksplicitno ne oglašava da li je izvorišna IP adresa legitimni pošiljatelj poruka za domenu ili ne – ništa se ne može zaključiti o IP adresi koja je poslala poruku.

S ciljem jednostavnijeg postavljanja ispravnih SPF zapisa, navedeno je nekoliko primjera s preporučenim postavkama:

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Primjeri preporučenih zapisa

1. `tijelo.hr TXT „v=spf1 mx -all"`

   poruka elektroničke pošte prihvaća se ako je izvorišna IP adresa jednaka IP adresi koja odgovara MX zapisu domene *tijelo.hr*. U suprotnom, poruka se odbacuje (*hard fail*)

2. `tijelo.hr TXT „v=spf1 a:mail.tijelo.hr -all"`

   isto kao 1., uz razliku da se ne koristi MX zapis domene *tijelo.hr*, već se specificira da izvorišna IP adresa mora odgovarati DNS zapisu tipa A za ime `mail.tijelo.hr` (najčešće isto kao i MX zapis)

3. `tijelo.hr TXT „v=spf1 mx ~all"`

   isto kao i 1., samo se poruka potencijalno prihvaća (`SoftFail`) - o konačnom prihvaćanju/odbacivanju odlučuje odredišni poslužitelj elektroničke pošte

4. `tijelo.hr TXT „v=spf1 a mx -all"`

   slično kao 1 i 2. – izvorišna IP adresa mora odgovarati IP adresi bilo kojeg A/AAAA zapisa ili IP adresi koja odgovara MX zapisu za domenu *tijelo.hr*

5. `tijelo.hr TXT „v=spf1 a mx ip4:1.2.3.4 -all"`

   slično kao 4. – ako izvorišna adresa ne zadovoljava niti jedan A/AAAA zapis, niti odgovara IP adresi koja odgovara MX zapisu, ali je jednaka IP adresi 1.2.3.4, tada se poruka prihvaća

6. `tijelo.hr TXT „v=spf1 a mx ip4:1.2.3.4 ip4:5.6.7.8 -all"`

   isto kao 5., uz dodatak da izvorišna adresa može biti jednaka i IP adresi 5.6.7.8 da bi poruka bila smatrana legitimnom

7. `tijelo.hr TXT „v=spf1 a mx ip4:1.2.3.4/30 -all"`

   isto kao 5. uz razliku da izvorišna adresa može biti iz raspona IP adresa 1.2.3.4/30

8. `tijelo.hr TXT „v=spf1 a mx ip4:1.2.3.4 include:drugotijelo.hr -all"`

   isto kao 5. ali se dodatno provjerava SPF zapis za domenu *drugotijelo.hr*. Ako izvorišna adresa zadovoljava mehanizme SPF zapisa za domenu *drugotijelo.hr*, poruka se prihvaća

Prethodno navedene primjere preporučuje se detaljnije analizirati i prilagoditi vlastitoj infrastrukturi, uz pomoć službene dokumentacije SPF mehanizma [3] za potpuni pregled standarda.

Razlika između `-all` i `~all`?

Mehanizam `all` koristi se uz odgovarajući kvalifikator na kraju SPF zapisa najčešće kao oznaka postupanja sa svim porukama koje ne zadovoljavaju prethodno navedene uvjete. Dva najčešće korištena kvalifikatora su `-` (`Fail`) i `~` (`SoftFail`). **Preporučuje se korištenje kvalifikatora `-` (`Fail`),** ali potrebno je uzeti u obzir da korištenje navedene kombinacije (`-all`) može uzrokovati neisporučivanje (legitimne) elektroničke pošte u slučaju pogrešne konfiguracije SPF zapisa ili drugih promjena u DNS zapisima.

Vjerojatnost opisanih problema smanjena je korištenjem kombinacije `~all`, ali odgovornost za odbacivanje poruka prebacuje se na odredišni poslužitelj, što u konačnici ipak može rezultirati prihvaćanjem lažiranih poruka.

U nastavku su navedene česte pogreške koje su uočene prilikom oblikovanja SPF zapisa:

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Primjeri pogrešnih zapisa

1. `tijelo.hr TXT „v=spf1 a mx all"`

   zapis je pogrešan zbog nepostojećeg kvalifikatora uz mehanizam `all` – ovako oblikovan SPF zapis **prihvaća svaku izvorišnu IP adresu!**

2. `tijelo.hr TXT „v=spf1 a -all" ; TXT „v=spf1 mx -all"`

   prema standardu, dopušteno je korištenje **isključivo jednog** TXT zapisa u DNS poslužitelju. Prilikom postojanja više zapisa, mehanizam provjere na strani poslužitelja elektroničke pošte nije definiran!

3. `tijelo.hr TXT „v=spf1 -all"`

   zapis definira da se domena tijelo.hr ne koristi za slanje elektroničke pošte. **Ovaj zapis može biti legitiman** ako je doista riječ o domeni za koju ne postoji poslužitelj elektroničke pošte i koja se ne koristi za razmjenu elektroničke pošte, no često je riječ o pogrešno definiranom SPF zapisu.

3.1. Konfiguracija na strani pošiljatelja (izlaz poruka)

Postavke SPF mehanizma na strani pošiljatelja svode se na dodavanje odgovarajućeg (ispravnog) TXT zapisa na DNS poslužitelj koji je autoritativan za zonu/domenu organizacije i u kojoj se nalaze MX zapisi za poslužitelje elektroničke pošte.

3.2. Konfiguracija na strani primatelja (ulaz poruka)

Implementacija SPF mehanizma na strani MTA poslužitelja koji prima poruku elektroničke pošte, odnosno uspostava provjere SPF zapisa, najčešće se ne provodi samostalno, već u kombinaciji s DMARC sigurnosnim mehanizmom koji će biti opisan u nastavku dokumenta.

Provjera SPF zapisa i politika postupanja s porukama elektroničke pošte u ovisnosti o rezultatu SPF provjere može se implementirati i samostalno, a takav je postupak relativno složen. Osnovni preduvjet za provjeru SPF zapisa jest podrška za SPF mehanizam od strane poslužitelja elektroničke pošte, odnosno postojanje odgovarajuće programske podrške. Većina popularnih inačica poslužitelja elektroničke pošte ima ugrađenu podršku za provjeru SPF mehanizma/zapisa [4], dok je kod nekih poslužitelja elektroničke pošte (npr. Postfix i Exim) potrebno instalirati dodatne programske pakete.

Provjera SPF mehanizma na strani primatelja

Provjeru SPF zapisa na strani primatelja preporuča se provesti u kombinaciji s DMARC mehanizmom.

Alternativno, provjeru SPF zapisa moguće je provesti samostalno korištenjem odgovarajućih postavki i programske podrške na poslužitelju elektroničke pošte. U tom slučaju potrebno je definirati politiku upravljanja porukama elektroničke pošte u ovisnosti o rezultatima provjere − npr. odbacivanje poruka u slučaju nezadovoljavanja uvjeta iz SPF zapisa, ili prosljeđivanje tih poruka krajnjem primatelju ako se koristi kvalifikator `~all`, uz dodavanje specifične oznake takvoj poruci elektroničke pošte (npr. oznaku da je riječ o potencijalno lažiranoj poruci kroz naslov poruke ili kroz druge mehanizme).

Za konkretne postavke potrebno je proučiti službenu dokumentaciju autora poslužitelja elektroničke pošte ili SPF programske podrške za konkretnu inačicu poslužitelja elektroničke pošte.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Ima li smisla imati SPF zapis u DNS poslužitelju bez validacije na strani primatelja poruka?

U određenim slučajevima konfiguracija SPF mehanizma na strani primatelja poruka nije moguća – npr. ako podrška za provjeru nije ugrađena u poslužitelj elektroničke pošte ili ako ne postoji odgovarajuća programska nadogradnja. Također, u slučajevima kad organizacija provodi prosljeđivanje poruka elektroničke pošte u ime druge organizacije ili kad organizacija pruža uslugu javne *mailing liste*, provjera SPF zapisa na strani primatelja vrlo vjerojatno neće biti uspješna (zbog činjenice da je poruka proslijeđena u ime izvorne organizacije, koristeći se novim MX poslužiteljima, domenom i IP adresama).

Bez obzira na opisane probleme, konfiguracija mehanizma na strani pošiljatelja (tj. dodavanje SPF zapisa u DNS poslužitelj) **svakako se preporuča**, čak i u slučaju ako organizacija ne može provoditi provjere na strani primatelja.

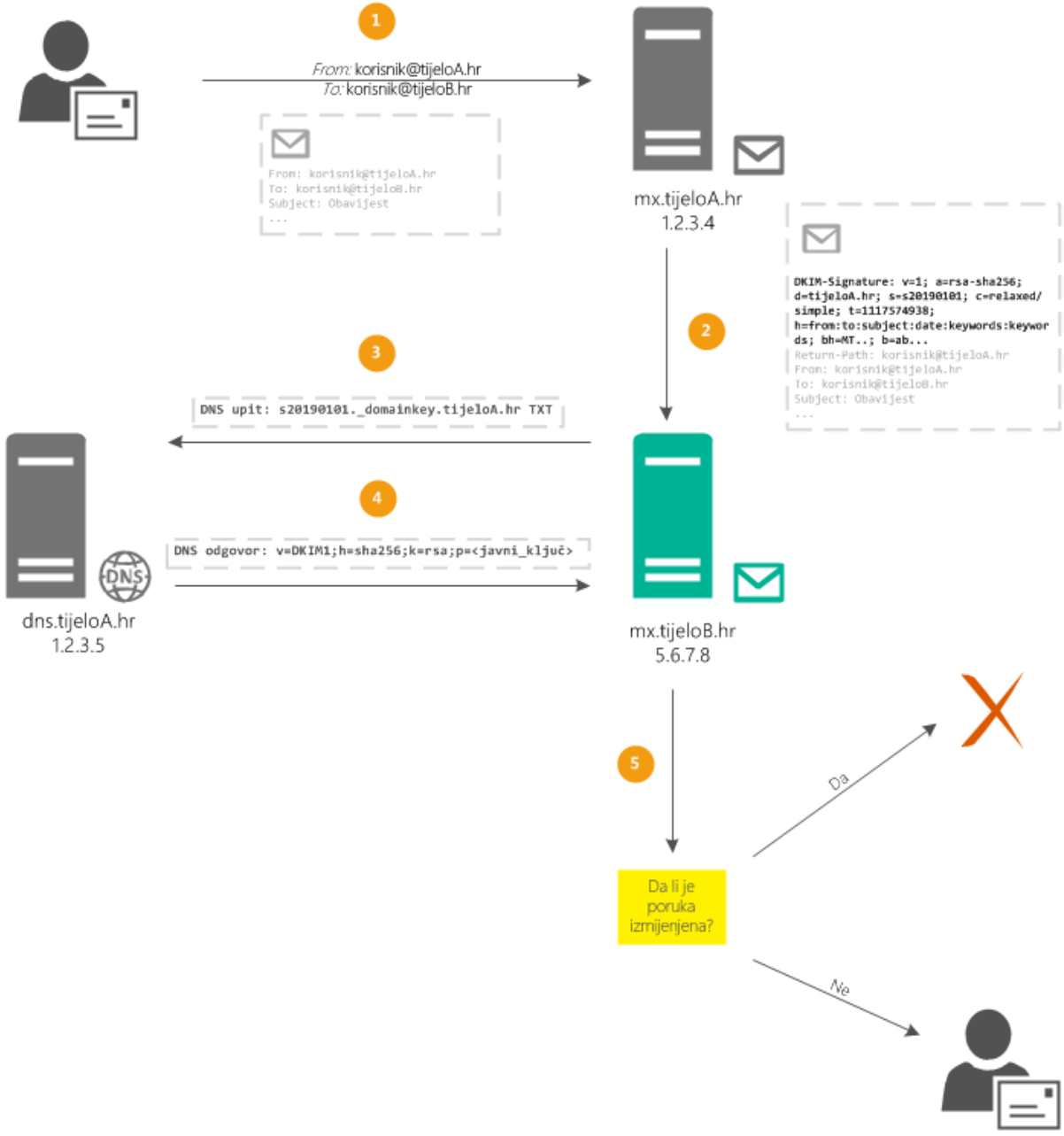
Postojanje SPF zapisa smatra se sastavnim dijelom *sigurnosne higijene* i predstavlja dio dobrih praksi koje drugim organizacijama pružaju djelomičan uvid u sveukupnu svijest o informacijskoj sigurnosti u organizaciji koja je zapise postavila.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

4. DKIM

DKIM (engl. *DomainKeys Identified Mail*) predstavlja tehnički standard koji je svojom namjenom vrlo sličan SPF mehanizmu – spriječiti slanje lažiranih poruka elektroničke pošte, odnosno omogućiti MTA poslužitelju na strani primatelja provjeru da li je poruka doista došla iz organizacije iz koje je navodni pošiljatelj (na temelju domene) te da li je poruka elektroničke pošte (njena zaglavlja i tijelo) izmijenjena u prijenosu. Za razliku od SPF mehanizma, koji se temelji isključivo na DNS zapisima, temelj DKIM mehanizma čini asimetrična kriptografija. S ciljem zaštite poruke DKIM mehanizmom, organizacija stvara par asimetričnih ključeva – poslužitelj elektroničke pošte potpisuje poruku privatnim ključem, a MTA poslužitelj na strani primatelja provjerava taj potpis na temelju javnog ključa koji je pohranjen u odgovarajućem DNS zapisu.

Pojednostavljeni prikaz djelovanja DKIM prikazan je na sljedećoj slici koja opisuje postupak slanja poruke elektroničke pošte iz *Tijela A* u *Tijelo B*, pri čemu *Tijelo A* ima uspostavljen DKIM mehanizam:



Slika 3: Postupak slanja poruke elektroničke pošte i način rada DKIM mehanizma

Koraci prikazani na prethodnoj slici detaljno su opisani u nastavku:

1. Korisnik informacijskog sustava u *Tijelu A* (adresa: *korisnik@tijeloA.hr*) šalje poruku elektroničke pošte prema korisniku u *Tijelu B* (adresa: *korisnik@tijeloB.hr*) na uobičajen način, koristeći se klijentom/preglednikom elektroničke pošte (npr. *Outlook*).
2. Poslužitelj elektroničke pošte u *Tijelu A* imena *mx.tijeloA.hr* i IP adrese 1.2.3.4 zaprima poruku elektroničke pošte. Provodi se sažimanje elemenata u poruci elektroničke pošte (zaglavlja i tijela) korištenjem odabranog algoritma sažimanja te se sažetak potpisuje korištenjem privatnog RSA ključa koji je pohranjen na poslužitelju, stvarajući na taj način *digitalni potpis*. Digitalni potpis, odabrani elementi (od kojih su neki propisani standardom, dok neke poslužitelj može sam odabrati), korišteni algoritam, parametri kriptiranja te oznaka izvorišne domene dodaju se u poseban element zaglavlja poruke elektroničke pošte pod nazivom `DKIM-Signature`, označavajući na taj način pošiljatelju na strani primatelja da izvorišni poslužitelj elektroničke pošte koristi DKIM mehanizam. Parametri `DKIM-Signature` elementa zaglavlja bit će detaljno opisani u nastavku dokumenta.
3. Prilikom primitka poruke elektroničke pošte, poslužitelj elektroničke pošte u *Tijelu B* (*mx.tijeloB.hr* s adresom 5.6.7.8) pregledava zaglavlje poruke te uočava `DKIM-Signature` element zaglavlja. Iz navedenog elementa zaglavlja na temelju specificirane *domene* (parametar `d`, na gornjoj slici *tijeloA.hr*) i tzv. *selektora* (parametar `s`, na gornjoj slici *s20190101*) postavlja DNS upit prema DNS poslužitelju autoritativnom za *Tijelo A* u kojem traži zapis tipa TXT, s nazivom u obliku `selektor._domainkey.domena` (u gornjem primjeru `s20190101._domainkey.tijeloA.hr`)
4. DNS poslužitelj *dns.tijeloA.hr* odgovara s odgovarajućim zapisom. U opisanom slučaju, kao odgovor na upit šalje se zapis sadržaja `v=DKIM1;h=sha256;k=rsa;p=<javni_ključ>`. Navedeni zapis zapravo sadržava javni RSA ključ kojim poslužitelj na strani primatelja može provjeriti ispravnost digitalnog potpisa.
5. Poslužitelj elektroničke pošte *mx.tijeloB.hr* provodi sažimanje istih elemenata nad kojima je sažimanje proveo i izvorišni poslužitelj (specificirano parametrima `DKIM-Signature` elementa zaglavlja). Korištenjem dohvaćenog javnog ključa provodi dekripciju digitalnih potpisa te uspoređuje sažetke. Ako su sažetci istovjetni, poruka nije mijenjana tijekom prijenosa i doista je poslana od strane navedenog pošiljatelja (odnosno pripadnog MX poslužitelja). Ako sažetci nisu istovjetni, postoji mogućnost da je poruka lažirana ili namjerno modificirana. Postupanje s takvim porukama ovisi o postavkama poslužitelja ili o drugim sigurnosnim mehanizmima (npr. DMARC).

4.1. Konfiguracija na strani pošiljatelja (izlaz poruka)

S ciljem implementacije DKIM mehanizma, prvi korak na strani pošiljatelja jest stvaranje para RSA kriptografskih ključeva.

Preporuke za stvaranje RSA ključeva

Ako organizacija koristi pružatelje usluge elektroničke pošte u oblaku, tada većina takvih pružatelja usluge ima vlastito sučelje za automatsko stvaranje para ključeva i automatsko postavljanje svih potrebnih parametara DKIM mehanizma (uključujući i DNS zapise).

Ako organizacija ima vlastite poslužitelje elektroničke pošte koji nemaju mogućnost jednostavnog konfiguriranja DKIM mehanizma, tada je potrebno ručno stvoriti par RSA ključeva.

Preporuča se stvaranje ključeva veličine **barem 2048 okteta**.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Na operacijskom sustavu Linux korištenjem `openssl` naredbe provodi se na sljedeći način:

```
openssl genrsa -out private.key 2048
openssl rsa -in private.key -pubout -out public.key
```

Na operacijskom sustavu Windows moguće je koristiti `PuTTYgen` alat.

DKIM mehanizam ne propisuje i ne provjerava starost ključa. U skladu s pravilima dobre prakse, preporuča se mijenjanje ključa svakih **12 mjeseci**. Zbog potrebe za ručnom rotacijom ključeva i zamjenom DNS zapisa, **dozvoljena je** i rotacija ključeva s većim vremenskim odmakom (npr. 2 ili više godina).

Nakon što je stvoren odgovarajući par RSA ključeva, u DNS poslužitelj potrebno je dodati odgovarajući TXT zapis kojim se označava podrška za DKIM mehanizam.

Preporuke za „DKIM TXT“ zapis koji sadržava RSA javni ključ

Prije dodavanja TXT zapisa, potrebno je odabrati njegov naziv, tj. *selektor* parametar. Cilj navedenog parametra jest podrška za veći broj DKIM ključeva za istu organizaciju, ako za to postoji potreba. Standard ne propisuje odabir selektora – kao selektor može biti odabrana geografska lokacija pojedine podružnice, datumi promjene ključeva ili bilo koji drugi znakovni niz koji je dozvoljen kao ime DNS zapisa. Kao vrijednost parametra preporuča se korištenje formata **sGGGGMMDDxx**, pri čemu pojedina polja imaju sljedeće značenje:

- **s** – fiksna vrijednost koja označava selektor
- **GGGG** – godina u četveroznamenkastom formatu (označava godinu kada je zapis dodan)
- **MM** – mjesec u dvoznamenkastom formatu (označava mjesec kada je zapis dodan)
- **DD** – dan u dvoznamenkastom formatu (označava dan kada je zapis dodan)
- **xx** – proizvoljna vrijednost koju organizacija sama odabire (može biti jedan ili više znakova, uz potreban oprez kako se ne bi prekoračila ograničenja duljine zapisa u DNS sustavu)

Korištenjem ovako odabranog selektora, organizacija će u svakom trenutku imati informaciju o zadnjoj promjeni ključa.

Prema opisanome, željeni TXT zapis u *Tijelu A* stvoren 1. siječnja 2019. godine imat će sljedeći naziv:

```
s20190101._domainkey.tijeloA.hr
```

`_domainkey` dio je nužni i fiksni dio DKIM mehanizma koji označava da je riječ o zapisu koji se koristi prilikom validacije DKIM potpisa.

Vrijednost opisanog TXT zapisa potrebno je postaviti na sljedeću vrijednost:

```
v=DKIM1;h=sha256;k=rsa;p=<javni_ključ>
```

Pojedini parametri zapisa imaju sljedeće značenje:

`v=DKIM1`	Oznaka korištene inačice DKIM mehanizma. Trenutno uvijek `v=DKIM1`
`h=sha256`	Oznaka korištenog algoritma sažimanja zaglavlja i tijela poruke. Preporuča se korištenje **SHA-256** algoritma

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

`k=rsa`	Oznaka korištenog tipa kriptografskog ključa. Jedina podržana vrijednost je `rsa`
`p=…`	Parametar `p` sadržava konkretnu vrijednost javnog ključa u *Base64* enkodiranom obliku.

Primjer javnog RSA ključa naveden je u nastavku:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1winVJaAh65xi8Wl0Srm
uj+GOb6KXOopMxEAQaO+Id4vCCUckC51NqCHHHFOkKdnW9dERXU19fprgMZllqiS
2I8FodKeKQKUU5ViwsbA0Sp+kLiKaqRPlmUgDo47kSYCgn7XG2JXlHe7EAx9tUNL
VaHOrQP276ggGITacIpGAzoLCS6XgNY43UIluPmnTKkHSdtj9BXaybBZuu+Sgxwi
MpgGdZIUG6PmKSZp24jlupZO3MF/bF0R/A8mc0LNYt9H5JgBwxWglR795sG4ssMe
3itNoZviPK0aBrcE6lm7/L+dL6g7FToc4+fwpyri6DV9u5ZoDGCQVHE1nMgFwmcq
OwIDAQAB
-----END PUBLIC KEY-----
```

Navedeni ključ potrebno je dodati kao vrijednost parametra p u gornjem TXT zapisu, pritom pazeći na ograničenje veličine vrijednosti u DNS zapisu! S ciljem minimiziranja problema s navedenim ograničenjem, preporuča se koristiti zagrade i navodne znakove za „razdvajanje“ vrijednosti u zapisu, kao što to propisuju određeni DNS poslužitelji i pružatelji usluga.

Konačni TXT zapis iz opisanih primjera koji je potrebno dodati u DNS poslužitelj ima sljedeći oblik (obratiti pažnju na zagrade i navodne znakove):

```
s20190101._domainkey.tijeloA.hr IN TXT ("v=DKIM1; h=sha256;
k=rsa; p="
"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1winVJaAh65xi8Wl0Srm"
"uj+GOb6KXOopMxEAQaO+Id4vCCUckC51NqCHHHFOkKdnW9dERXU19fprgMZllqiS"
"2I8FodKeKQKUU5ViwsbA0Sp+kLiKaqRPlmUgDo47kSYCgn7XG2JXlHe7EAx9tUNL"
"VaHOrQP276ggGITacIpGAzoLCS6XgNY43UIluPmnTKkHSdtj9BXaybBZuu+Sgxwi"
"MpgGdZIUG6PmKSZp24jlupZO3MF/bF0R/A8mc0LNYt9H5JgBwxWglR795sG4ssMe"
"3itNoZviPK0aBrcE6lm7/L+dL6g7FToc4+fwpyri6DV9u5ZoDGCQVHE1nMgFwmcq"
"OwIDAQAB")
```

Nakon stvaranja para RSA ključeva i dodavanja javnog ključa u TXT zapis na DNS poslužitelj (tj. stvaranja TXT zapisa kojeg zahtijeva DKIM mehanizam), potrebno je omogućiti DKIM mehanizam na poslužitelju elektroničke pošte i odabrati odgovarajuće parametre digitalnog potpisivanja poruka.

Preporučene postavke DKIM mehanizma na poslužitelju elektroničke pošte

Prije omogućavanja DKIM mehanizma na poslužitelju elektroničke pošte, potrebno je provjeriti da li inačica poslužitelja elektroničke pošte podržava DKIM mehanizam. Iako je DKIM mehanizam relativno nedavno prihvaćen kao tehnički standard (prva inačica je prihvaćena 2011. godine), većina poslužitelja elektroničke pošte i zaštitnih uređaja na perimetru (engl. *mail gateway* ili *mail security appliance*) podržava DKIM mehanizam kroz ugrađenu programsku podršku ili kao nadogradnje/dodatke koje je potrebno dodatno ugraditi u poslužitelj. Većina pružatelja usluge elektroničke pošte u oblaku (npr. Microsoft Office 365, Google i drugi) ima ugrađeni DKIM mehanizam i omogućava njegovu konfiguraciju.

Najpoznatiju iznimku predstavlja Microsoft Exchange poslužitelj za kojeg ne postoji službena podrška za DKIM standard, iako postoje neslužbeni dodaci koje je razvila zajednica s ciljem dodavanja podrške za DKIM standard. Njihova upotreba na produkcijskim Exchange poslužiteljima se ne preporučuje, budući da je riječ o neslužbenim i nedovoljno provjerenim dodacima. Ipak, zbog činjenice da se Exchange poslužitelj rijetko koristi kao MX poslužitelj (u tzv. transportnoj ulozi), nedostatak podrške ne bi trebao utjecati na konačnu mogućnost implementaciju mehanizma.

Ako poslužitelj elektroničke pošte podržava implementaciju DKIM mehanizma, tada je na poslužitelj najprije potrebno postaviti stvoreni par ključeva (točnije, potrebno je postaviti samo privatni ključ) te podesiti odgovarajuće parametre mehanizma. Podešavanje uključuje najmanje sljedeće parametre:

- **domena** – mora odgovarati domeni za koju je prethodno dodan odgovarajući TXT zapis s RSA javnim ključem
- **selektor** – mora odgovarati selektoru koji je prethodno odabran kao dio naziva TXT zapisa
- **algoritam sažimanja** – preporuča se odabir **SHA-256** algoritma. Ovaj parametar mora odgovarati parametru `h` u TXT zapisu. Standard dozvoljava i korištenje SHA-512 algoritma, no podrška za isti nije toliko raširena kao za SHA-256 algoritam.
- **algoritam kanonizacije** – prilikom prijenosa poruke elektroničke pošte, poslužitelji elektroničke pošte mogu provesti manje ili značajnije izmjene izvorne poruke – npr. pojedini elementi zaglavlja mogu biti prepisani velikim slovima, veći broj praznina može biti zamijenjen jednom prazninom i sl. Sve takve izmjene mijenjaju izvornu poruku, a time i vrijednost digitalnog potpisa koji je rezultat djelovanja DKIM mehanizma. U DKIM mehanizam je zbog toga ugrađena mogućnost specifikacije *kanonizacijskog algoritma* kojim je moguće specificirati do koje se mjere toleriraju izmjene u zaglavljima i tijelu poruke, a da pritom digitalni potpis i dalje ostane važeći (tj. da poslužitelj na strani primatelja može provesti isti postupak pridržavajući se pravila određenih kanonizacijskim algoritmom i dobiti isti sažetak).
  Moguće su dvije vrijednosti algoritma:
  - `simple` – mali broj dozvoljenih izmjena ili bez izmjena
  - `relaxed` – dozvoljene izmjene poput uklanjanja nepotrebnih praznina i sl.

  Konkretne izmjene koje se dozvoljavaju pojedinim algoritmom opisane su u samom standardu [5]. Željeni format kanonizacije zadaje se u formatu zaglavlje/tijelo, tj. najprije se navodi algoritam koji se primjenjuje na elemente zaglavlja, a potom algoritam koji se primjenjuje na tijelo poruke.
  Preporučena vrijednost algoritma kanonizacije je **`relaxed/relaxed`**, kako bi se omogućile minimalne promjene zaglavlja i tijela poruke tijekom prijenosa.
- **elementi zaglavlja** – potrebno je odrediti elemente zaglavlja koji će biti obuhvaćeni digitalnim potpisom. DKIM standard kao jedini obavezni element zaglavlja koji mora biti obuhvaćen digitalnim potpisom propisuje `From:` element.

  U nastavku su navedeni elementi zaglavlja koje se preporuča obuhvatiti digitalnim potpisom:
  - `From`

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

- To
- Reply-To
- Cc
- Subject
- Date
- In-Reply-To
- References
- Content-Type
- Content-Transfer-Encoding
- Content-Disposition

Popis elemenata zaglavlja najčešće se navodi u obliku niza željenih elemenata odvojenih znakom „:“. Prema prethodno navedenoj listi, preporučena vrijednost navedena je u nastavku:

```
From:To:Reply-To:Cc:Subject:Date:In-Reply-To:References:Content-
Type:Content-Transfer-Encoding:Content-Disposition
```

Organizacija može dodati proizvoljne elemente zaglavlja u popis elemenata koji se potpisuju, pazeći pritom da se ne potpisuju elementi koji su podložni izmjenama tijekom prijenosa (npr. `Return-Path`, `Received`, `Comments` i sl.).

Ako element zaglavlja nije prisutan u konkretnoj poruci koja se potpisuje, on će biti izostavljen pri izradi digitalnog potpisa.

- **prepisivanje (engl. *oversigning*)** – izraženi problem DKIM mehanizma jest mogućnost dodavanja dodatnih elemenata zaglavlja od strane napadača, čija interpretacija od strane klijenta elektroničke pošte primatelja može biti različita od inicijalne. Npr. ako napadač presretne poruku i postavi dodatan `From` element zaglavlja tako da poruka sadržava dva `From` elementa, potpis će i dalje ostati ispravan, zbog činjenice da je njime obuhvaćeno prvo `From` polje. Klijent elektroničke pošte primatelja (ovisno o inačici) prikazuje samo drugo `From` polje, čime je narušen osnovni koncept sigurnosti DKIM mehanizma te je primatelju uspješno poslana lažirana poruka elektroničke pošte.

  Kako bi se spriječila provedba ovakvih napada, DKIM standard propisuje da svi takvi „problematični“ elementi zaglavlja moraju biti navedeni (i potpisani) barem jednom više nego što je stvaran broj njihovog pojavljivanja u poruci elektroničke pošte – zbog toga je u postavke prepisivanja (najčešći naziv za postavku je *oversign headers*) potrebno **minimalno dodati** element zaglavlja `From`.

- **vremenski interval ispravnosti** – ako postavke DKIM mehanizma za konkretnu inačicu poslužitelja elektroničke pošte to dozvoljavaju, preporuča se postavljanje vremenskog intervala unutar kojeg se digitalni potpis zaglavlja i tijela poruka važećim. Definicija vremenskog intervala ispravnosti najčešće se svodi na definiranje odmaka u odnosu na vrijeme izrade digitalnog potpisa, što znači da vrijeme na poslužitelju elektroničke pošte koji provodi potpisivanje **mora biti ispravno podešeno** (tj. sinkronizirano s izvorom točnog vremena).

  Vremenski interval se preporuča postaviti na vrijednost koja je približno sukladna intervalu rotacije RSA ključeva koji se koriste za potpisivanje, tj. na razdoblje od **12 mjeseci**.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Za detaljnije informacije o konkretnim konfiguracijskim parametrima za korištenu inačicu poslužitelja elektroničke pošte potrebno je proučiti službenu dokumentaciju poslužitelja ili pripadnih DKIM dodataka.

Izbjegavati korištenje parametra `l`!

Standard propisuje postojanje parametra `l` koji se može koristiti za ograničavanje duljine tijela poruke elektroničke pošte koje će biti obuhvaćeno digitalnim potpisom. Osnovna namjena tog parametra je obuhvatiti samo onaj dio tijela poruke koji je stvorio korisnik i izbjeći moguće dodatke na tijelo poruke, poput potpisa koji dodaje antivirusni *gateway* poslužitelj na perimetru, različite grupne liste i sl.

Iako navedeni parametar svakako ima svoju primjenu, postoji izražena mogućnost njegove zloupotrebe − napadač može na postojeće tijelo poruke u prijenosu dodati novi tekst (potencijalno skrivajući prethodni, koristeći se posebnim tehnikama), pri čemu će tijelo poruke i dalje imati ispravan digitalni potpis, zbog činjenice da se pri izradi sažetka/potpisa uzima samo fiksna duljina tijela poruke. [5, poglavlje 8.2.]

Zbog navedenih problema, **potrebno je izbjegavati korištenje parametra `l`**!

Što ako uz MX poslužitelj postoji uređaj/usluga koja provodi dodatno filtriranje/izmjene poruke prilikom slanja?

Budući da se DKIM mehanizmom nastoji osigurati integritet poruke u prijenosu, bilo koji uređaj ili usluga koja provodi dodatne izmjene poruke elektroničke pošte (npr. izmjena postojećih zaglavlja, dodavanje potpisa u tijelo poruke i sl.) nakon što je poruka već potpisana (tj. ima odgovarajući `DKIM-Signature` element zaglavlja) uzrokovat će neispravnu vrijednost digitalnog potpisa na strani primatelja.

Zbog navedenog problema uvijek se preporuča implementacija DKIM potpisivanja na **posljednjem poslužitelju/uređaju** na izlazu poruke elektroničke pošte iz organizacije.

4.2. Konfiguracija na strani primatelja (ulaz poruka)

Uspostava DKIM mehanizma na strani primatelja jednostavnija je od konfiguracije na strani pošiljatelja (nema potrebe za stvaranjem i upravljanjem ključeva, dodavanja zapisa na DNS poslužitelj i sl.). Konfiguracija na strani primatelja svodi se na uspostavu DKIM mehanizma na ulaznom MX poslužitelju (točnije, na prvom poslužitelju/uređaju koji se nalazi na ulazu poruke elektroničke pošte u organizaciju i koji ima mogućnost uspostave DKIM mehanizma) s ciljem provjere digitalnog potpisa elemenata zaglavlja i tijela poruke dohvaćanjem javnog RSA ključa s DNS poslužitelja autoritativnog za izvorišnu organizaciju.

Druga (i preporučena) mogućnost jest provjera DKIM ispravnosti u kombinaciji s DMARC sigurnosnim mehanizmom koji je opisan u poglavlju 5.

Implementacija DKIM mehanizma na strani primatelja

U većini inačica poslužitelja elektroničke pošte, podrška za verifikaciju DKIM digitalnih potpisa inicijalno je omogućena i potrebno ju je postaviti na željenu politiku upravljanja porukama elektroničke pošte u ovisnosti o rezultatima provjere digitalnog potpisa. Politika se može svoditi na konfiguracijske datoteke (npr. za Postfix i Exim poslužitelj elektroničke pošte) ili na uspostavu transportnih pravila (za Office 365 poslužitelj).

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

U slučaju da ulazna poruka nema ispravan digitalni potpis, njeno odbacivanje se **ne preporučuje**, zbog činjenice da neispravna vrijednost digitalnog potpisa može biti rezultat djelovanja samih poslužitelja elektroničke pošte na transportnom putu, a ne nužno rezultat lažirane poruke elektroničke pošte.

Preporuča se posebno označavanje poruka elektroničke pošte koje nemaju ispravan digitalni potpis (npr. dodavanjem određenih oznaka, stavljanjem u karantenu i sl.), ako je to moguće provesti.

Također, preporučuje se provjeru DKIM potpisa provoditi u kombinaciji s DMARC mehanizmom, kao što će biti opisano u zasebnom poglavlju.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

5. DMARC

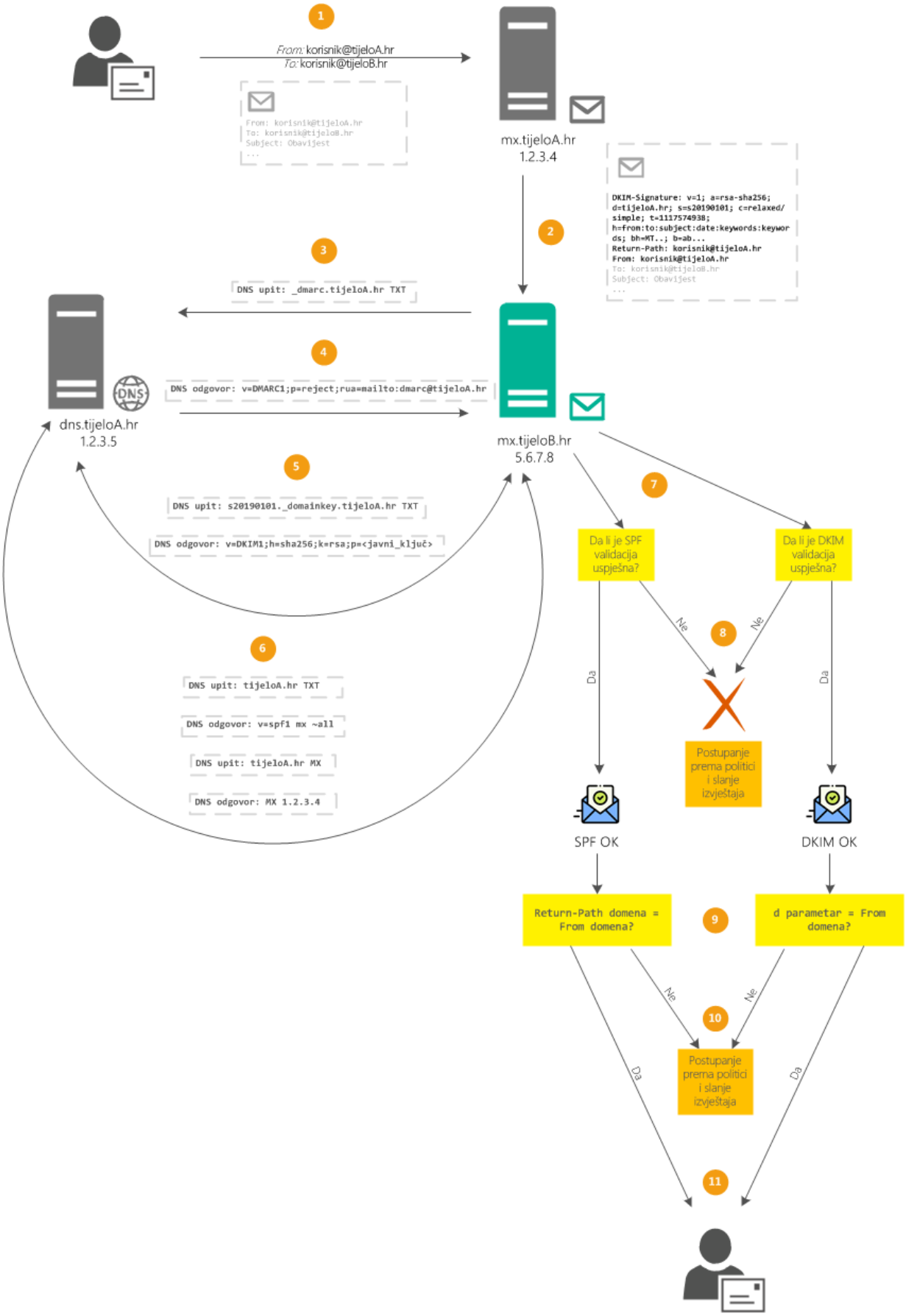
Nakon postavljanja SPF i/ili DKIM mehanizama na strani pošiljatelja, organizacija se susreće s dvije nepoznanice – da li je uspostava mehanizama uzrokovala nemogućnost isporuke legitimnih poruka koje su upućene određenim primateljima te koliko su mehanizmi zapravo učinkoviti (u kontekstu blokiranih ili specifično označenih lažiranih poruka koje bi bile isporučene kada mehanizmi ne bi postojali).
Postojeći mehanizmi odluku o daljnjoj sudbini poruke koja nije zadovoljila provjeru prepuštaju organizaciji na strani primatelja, pri čemu izvorišni poslužitelj, odnosno organizacija, najčešće nemaju nikakvu povratnu informaciju o tome da li je poruka isporučena ili ne.
Također, SPF mehanizam obuhvaća samo adresu pošiljatelja u omotnici poruke (`Return-Path`), dok adresa pošiljatelja u zaglavlju poruke (`From`) nije obuhvaćena djelovanjem mehanizma. Budući da se u klijentu elektroničke pošte primatelju prikazuje adresa iz zaglavlja poruke (`From`), napadač može lažirati poruku elektroničke pošte i poslati je s vlastite domene koja ima ispravno postavljene SPF parametre (TXT zapis koji odgovara MX poslužitelju te domene), dok u polje pošiljatelja može upisati proizvoljnu (lažnu vrijednost).

Zbog navedenih ograničenja, razvijen je novi mehanizam pod nazivom **DMARC** (engl. *Domain-based Message Authentication, Reporting and Conformance*). Navedeni mehanizam još nije službeno prihvaćen kao tehnički standard, no vrlo je raširen među najpoznatijim pružateljima usluge elektroničke pošte, a podrška za navedeni mehanizam je u stalnom porastu. Slično SPF i DKIM mehanizmima, DMARC predstavlja mehanizam za autentifikaciju poruke elektroničke pošte koji se oslanja na SPF i DKIM mehanizme (zahtijeva postojanje barem jednog od njih) te pruža dodatne mogućnosti:

- DMARC zapisom organizacija označava da su poruke elektroničke pošte zaštićene SPF i/ili DKIM mehanizmom – uz činjenicu da poruke moraju zadovoljiti barem jednu provjeru (ako se koriste oba mehanizma), DMARC mehanizmom se dodatno uspoređuje rezultat SPF ili DKIM provjere s `From` poljem (tzv. *usklađenost poruke* – engl. *identifier alignment*).
- Preporučenu politiku upravljanja porukama koje ne zadovoljavaju provjeru definira izvorišna organizacija – poruke mogu biti prihvaćene unatoč neuspješnoj provjeri, preusmjerene u karantenu ili odbačene.
- Izvorišna organizacija ima mogućnost primitka sažetog ili vrlo detaljnog (tzv. *forenzičkog*) izvješća o svim porukama elektroničke pošte za koje rezultat DMARC provjere (točnije, SPF i/ili provjere te provjere usklađenosti) nije bio uspješan.

Pojednostavljeni prikaz djelovanja DMARC prikazan je na sljedećoj slici koja opisuje postupak slanja poruke elektroničke pošte iz *Tijela A* u *Tijelo B*, pri čemu *Tijelo A* ima uspostavljen DMARC mehanizam (te SPF i DKIM mehanizme):

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110



Slika 4: Postupak slanja poruke elektroničke pošte i način rada DMARC mehanizma (u kombinaciji sa SPF i DKIM mehanizmima)

Koraci su detaljno opisani u nastavku:

1. Korisnik informacijskog sustava u *Tijelu A* (adresa: *korisnik@tijeloA.hr*) šalje poruku elektroničke pošte prema korisniku u *Tijelu B* (adresa: *korisnik@tijeloB.hr*) na uobičajen način, koristeći se klijentom/preglednikom elektroničke pošte (npr. *Outlook*).
2. Poslužitelj elektroničke pošte u *Tijelu A* imena *mx.tijeloA.hr* i IP adrese 1.2.3.4 zaprima poruku elektroničke pošte te digitalno potpisuje poruku dodajući `DKIM-Signature` element zaglavlja.
3. Prilikom primitka poruke elektroničke pošte, poslužitelj elektroničke pošte u *Tijelu B* (*mx.tijeloB.hr* s adresom 5.6.7.8) provjerava da li *Tijelo A* ima uspostavljen DMARC mehanizam - postavlja DNS upit prema DNS poslužitelju autoritativnom za *Tijelo A* u kojem traži zapis tipa TXT, s nazivom u obliku `_dmarc.domena` (u gornjem primjeru `_dmarc.tijeloA.hr`).
4. DNS poslužitelj *dns.tijeloA.hr* odgovara s odgovarajućim zapisom. U opisanom slučaju, kao odgovor na upit šalje se zapis sadržaja `v=DMARC1;p=reject;rua=mailto:dmarc@tijeloA.hr`. Pojedini elementi navedenog zapisa bit će opisani u nastavku poglavlja.
5. Poslužitelj elektroničke pošte u *Tijelu B* provjerava postojanje DKIM mehanizma slanjem odgovarajućeg DNS upita. DNS poslužitelj *Tijela A* odgovara na DNS upit s odgovarajućim DKIM zapisom (više informacija dostupno u poglavlju 4).
6. Poslužitelj elektroničke pošte u *Tijelu B* provjerava postojanje SPF mehanizma slanjem odgovarajućeg DNS upita. DNS poslužitelj *Tijela A* odgovara na DNS upit s odgovarajućim SPF zapisom (više informacija dostupno u poglavlju 3).
7. Na temelju dohvaćenih TXT zapisa koji odgovaraju DKIM mehanizmu (javni ključ poslužitelja) odnosno SPF mehanizmu (popis adresa MX poslužitelja), provodi se provjera digitalnog potpisa (DKIM) i adrese izvorišnog MX poslužitelja (SPF).

   Napomena: Potrebno je naglasiti da se provjere SPF/DKIM mehanizama najčešće provode simultano i neovisno jedna o drugoj (njihovi rezultati se uspoređuju kasnije). U kasnijoj usporedbi rezultata, isti se uzimaju neovisno te stoga i sliku treba razmatrati u tom kontekstu u svim ostalim koracima (7 – 11). Npr. negativan rezultat SPF provjere samostalno ne znači nužno odbacivanje poruke – potrebno je najprije utvrditi rezultat DKIM provjere te u ovisnosti o tome odlučiti o daljnjim koracima u prihvaćanju poruke (u ovisnosti o postavljenoj DMARC politici).
8. U slučaju kada **niti jedan** od mehanizma ne rezultira uspješnom provjerom (npr. neispravan digitalni potpis, adresa MX poslužitelja ne odgovara onoj u SPF zapisu), s porukom se postupa na način koji je utvrđen *DMARC politikom* koju je *Tijelo A* navelo u TXT zapisu. U gornjem primjeru, politika je postavljena na vrijednost `reject`, što će uzrokovati odbijanje isporuke poruke. O rezultatima SPF i/ili DKIM provjere stvara se „izvješće“ koje sadržava informacije o rezultatima provjere mehanizama, a izvješće se šalje na adresu elektroničke pošte navedenu u DNS zapisu.
9. Ako **barem jedan** od mehanizama rezultira uspješnom provjerom, provodi se *provjera usklađenosti.* U provjeri usklađenosti, uspoređuje se vrijednost domene navedene u adresi iz zaglavlja poruke (`From`) s domenom koja je navedena u parametru `d` (ako se koristi DKIM mehanizam i ako je provjera digitalnog potpisa bila uspješna) ili s domenom koja je prisutna u adresi iz omotnice poruke (`Return-Path`), ako se koristi SPF mehanizam i SPF provjera je bila uspješna.
10. Ako provjera usklađenosti nije bila uspješna **niti za jedan** korišteni mehanizam (SPF i/ili DKIM), ponovno se s porukom postupa u skladu s objavljenom politikom te se stvara izvješće za *Tijelo A*.
11. Ako je provjera usklađenosti uspješna za **barem jedan** od mehanizama, poruka se isporučuje primatelju (*korisnik@tijeloB.hr*).

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Postoji li obaveza istovremenog postojanja SPF i DKIM mehanizama kao preduvjeta za implementaciju DMARC mehanizma?

DMARC mehanizam temelji se na SPF i DKIM mehanizmima te u obzir uzima njihove rezultate, uz dodatnu provjeru usklađenosti domene.

Istovremeno postojanje oba mehanizma **nije preduvjet** za implementaciju DMARC mehanizma − dovoljno je korištenje samo jednog od spomenutih mehanizama.

Preporuka je koristiti oba mehanizma kao potporu DMARC mehanizmu, zbog dodatne razine provjere.

U slučaju korištenja samo jednog mehanizma, preporuča se korištenje DKIM mehanizma, zbog činjenice da isti pruža veću razinu sigurnosti i eliminira pojedine sigurnosne probleme prisutne kod SPF mehanizma.

Ako implementacija DKIM mehanizma nije moguća zbog neadekvatne i nekompatibilne programske podrške, dozvoljeno je korištenje SPF mehanizma.

Slično opisanim mehanizmima, temelj DMARC mehanizma predstavlja odgovarajući TXT zapis u autoritativnom DNS poslužitelju koji ima oblik jedne linije u posebnom formatu.

Implementacijske smjernice za DMARC mehanizam na strani pošiljatelja i primatelja navedene su u nastavku.

5.1. Konfiguracija na strani pošiljatelja (izlaz poruka)

Slično SPF mehanizmu, postavke DMARC mehanizma na strani pošiljatelja svode se na dodavanje odgovarajućeg (ispravnog) TXT zapisa na DNS poslužitelj koji je autoritativan za zonu u kojoj se nalaze i SPF i/ili DKIM zapisi.

U prethodnom primjeru komunikacije između *Tijela A* i *Tijela B*, prisutan je sljedeći DMARC zapis u DNS poslužitelju *Tijela A*:

```
tijeloA.hr.  TXT  "v=DMARC1;p=reject;rua=mailto:dmarc@tijeloA.hr"
```

Elementi zapisa opisani su u sljedećoj tablici:

`v=DMARC1`	Oznaka korištene inačice DMARC mehanizma. Trenutno uvijek `v=DMARC1`.
`p=reject`	Oznaka politike koja daje naputak poslužitelju na strani primatelja o načinu postupanja s porukama koje rezultiraju neuspješnom DMARC provjerom. DMARC mehanizam razlikuje sljedeće vrijednosti politike: • `none` - tzv. nadzorni način rada, bez obzira na neuspješne DMARC provjere, izvorišni poslužitelj ne zahtijeva od poslužitelja na strani primatelja nikakvu dodatnu akciju. **Ova vrijednost politike preporuča se prilikom inicijalnog postavljanja DMARC mehanizma**. • `quarantine` - izvorišni poslužitelj poslužitelju na strani primatelja daje naputak da posebno označi poruke koje su rezultirale neuspješnom DMARC provjerom (npr. kao neželjenu ili sumnjivu poštu)

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

	• `reject` - izvorišni poslužitelj sugerira poslužitelju na strani primatelja da sve poruke koje su rezultirale neuspješnom DMARC provjerom eksplicitno odbaci i ne isporuči primatelju
`rua=` `mailto:dmarc@tijeloA.hr`	Lista adresa elektroničke pošte odvojenih zarezom na koje će poslužitelj elektroničke pošte na strani primatelja slati *skupno izvješće* (engl. *aggregated feedback report*) o porukama elektroničke pošte koje su bile poslane, rezultatima njihove SPF i/ili DKIM provjere te rezultatu DMARC provjere (tj. provjere usklađenosti). Navedena adresa elektroničke pošte zaprimat će skupna izvješća sa svih poslužitelja elektroničke pošte koji su bili odredište poruka i imaju implementiran DMARC mehanizam. Skupna izvješća se šalju jednom dnevno (moguće mijenjati kroz posebnu postavku, no postavljena vrijednost je zadovoljavajuća).

Službeni prijedlog DMARC standarda razlikuje i niz drugih elemenata zapisa (potpuni popis dostupan je u službenoj dokumentaciji - [6]), a u tablici u nastavku prikazani su i dodatni elementi koji se često koriste:

`adkim`	Vrijednost ovog parametra definira način usporedbe domene pošiljatelja u adresi pošiljatelja u zaglavlju (`From`) s domenom pošiljatelja navedenom u `d` parametru `DKIM-Signature` elementa zaglavlja. Dvije moguće vrijednosti su: • `s (strict)` – domene u navedenim elementima moraju biti identične • `r (relaxed)` – prilikom usporedba domena, određuje se *organizacijska domena* adrese pošiljatelja u zaglavlju te se ista uspoređuje s vrijednošću parametra `d` u `DKIM-Signature` elementu. *Organizacijska domena* određuje se relativno jednostavnim algoritmom koji eliminira sve dijelove domene koji se odnose na pojedine poddomene – npr. *organizacijska domena* domene `a.b.c.d.tijeloA.hr` je `tijeloA.hr`. Ovakva "slobodnija" usporedba koristi se npr. u slučajevima kada je poruka elektroničke pošte poslana s adrese `korisnik@uredN.tijeloA.hr`, a DKIM zapis je uspješno provjeren za domenu `tijeloA.hr`. Slobodnija usporedba rezultira uspješnom provjerom usklađenosti, dok bi stroga usporedba rezultirala neuspješnom provjerom. Inicijalna vrijednost parametra je `r` (`relaxed`).

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

`aspf`	Slično `adkim` parametru, ovim parametrom se opisuje način usporedbe domene pošiljatelja u adresi pošiljatelja u zaglavlju (`From`) s domenom pošiljatelja u omotnici (`Return-Path`). Također su dozvoljene vrijednosti `strict` i `relaxed`, koje imaju isto značenje kao i kod `adkim` parametra. Inicijalna vrijednost parametra je `r` (`relaxed`).
`sp`	Slično parametru `p`, koji daje naputak poslužitelju na strani primatelja na koji način se postupa s porukama koje ne zadovoljavaju DMARC provjeru, parametar `sp` određuje politiku koja se primjenjuje na poddomene (engl. *subdomain policy*). Moguće vrijednosti su istovjetne onima za parametar `p`. Ako vrijednost parametra nije navedena, primjenjuje se vrijednost navedena za parametar `p`.
`ruf`	Slično parametru `rua`, koji određuje adrese elektroničke pošte na koje se šalju skupna izvješća, parametar `ruf` određuje adrese elektroničke pošte na koje se šalju detaljna/forenzička izvješća.

Skupna ili detaljna/forenzička izvješća?

Skupna izvješća šalju se automatski jednom dnevno (prema standardnim postavkama) na adrese specificirane u `rua` parametru, od strane svih poslužitelja elektroničke pošte na strani primatelja koji su postavljeni na odgovarajući način. U skupnim izvješćima nalaze se sljedeće informacije:

- osnovni podaci o organizaciji koja šalje izvješće i vremenski interval izvješća
- DMARC TXT zapis organizacije koja prima izvješće, aktualan u vremenskom intervalu za koji je izvješće izrađeno
- sažetak rezultata provjere (IP adrese s koje su poruke poslana, broj poruka poslanih s tih adrese i rezultati SPF i/ili DKIM provjera te provjera usklađenosti)

Forenzička izvješća, uz gornje informacije, sadržavaju i dodatne podatke poput naslova poruke, zaglavlja poruke i URL poveznica koje se nalaze u tijelu poruke. Za razliku od skupnih izvješća, poslužitelji elektroničke pošte na strani primatelja mogu poslati forenzička izvješća odmah nakon primitka poruke koja ne zadovoljava DKIM mehanizam. Broj forenzičkih izvješća koje organizacija zbog toga može primiti na adrese specificirane u `ruf` parametru može biti iznimno velik, osobito ako organizacija intenzivno koristi elektroničku poštu i šalje ju prema drugim organizacijama čiji poslužitelji imaju mogućnost slanja DMARC izvješća.

Zbog navedenog, kao i činjenice da forenzička izvješća pri inicijalnom uvođenju DMARC mehanizma ne pružaju značajniju dodanu vrijednost te mogu sadržavati osjetljive (osobne) podatke, **preporuča se omogućavanje primitka skupnih izvješća**, tj. podešavanje `rua` parametra. Naravno, ako organizacija ima potrebu za detaljnijim izvješćima o porukama koje su primile druge organizacije i koje ne zadovoljavaju DMARC provjeru, dozvoljava se i omogućavanje primitka forenzičkih izvješća.

Popis organizacija čiji poslužitelji elektroničke pošte imaju omogućenu izradu izvješća dostupan je na sljedećim adresama:

- https://us.dmarcian.com/dmarc-data-providers/

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

- https://dmarc.io/sources/

Budući da DMARC mehanizam može uzrokovati prekide u isporuci legitimnih poruka elektroničke pošte, njegovu implementaciju je potrebno provoditi u barem dvije faze. Konkretne preporuke navedene su u nastavku:

Preporuke za implementaciju DMARC mehanizma

Implementacija DMARC mehanizma na strani pošiljatelja svodi se na dodavanje prethodno opisanog, odgovarajućeg TXT zapisa u DNS poslužitelj.

U prvoj fazi implementacije, preporuča se dodavanje sljedećeg zapisa:

```
v=DMARC1;p=none;rua=mailto:dmarc@domena.hr
```

Navedenim zapisom, DMARC politika postavlja se u nadzorni način rada, što znači da poruke elektroničke neće biti odbijene u slučaju neuspješne DMARC provjere. Također, postavljanjem `rua` parametra omogućit će se primitak skupnih izvješća na odgovarajuću adresu elektroničke pošte. Adresa elektroničke pošte mora postojati, a izvješća koja će pristizati na tu adresu potrebno je koristiti kao temelj za donošenje daljnjih odluka o postavljanju strožijih politika.

Vrijednost politike **svakako se u početnoj fazi preporuča postaviti na vrijednost `p=none`**. Tek nakon inicijalnog perioda i prepoznavanja mogućih problema s isporukom legitimnih poruka elektroničke pošte (npr. prosljeđivanje poruka, *mailing liste* i sl.), prijeći na strožiju politiku. Prijelaz ne treba biti brz – primjena `p=quarantine` ili `p=reject` politike **preporuča se nakon 3-12 mjeseci**, uz pretpostavku da se čitavo vrijeme analiziraju informacije koje se primaju putem skupnih izvješća.

Ako organizacija pri slanju poruka elektroničke pošte koristi isključivo vlastitu vršnu domenu (npr. *domena.hr*) i poruke se nikada ne šalju s poddomena (npr. *poddomena.domena.hr*), onda je odmah moguće postaviti strožiju politiku za poddomene na sljedeći način:

```
v=DMARC1;p=none;sp=reject;rua=mailto:dmarc@domena.hr
```

Paralelno s prelaskom na strožije politike, organizacija može postaviti strožije vrijednosti parametara `aspf` i `adkim`, tj. umjesto inicijalnih vrijednosti `r` (`relaxed`) postaviti vrijednost `s` (`strict`).

Konačne preporučene vrijednosti, nakon perioda testiranja DMARC politika te ako ne postoje uočeni problemi u isporuci poruka navedene su u nastavku:

```
v=DMARC1;p=reject;aspf=s;adkim=s;rua=mailto:dmarc@domena.hr
```

Prema potrebi, organizacija može omogućiti stvaranje forenzičkih izvještaja, iako njihovo korištenje u operativnom radu nema značajniju dobrobit.

5.2. Konfiguracija na strani primatelja (ulaz poruka)

Kao i u slučaju prethodno opisanih mehanizama, osnovni preduvjet za provođenje DMARC provjere jest podrška za DMARC mehanizam od strane poslužitelja elektroničke pošte, odnosno postojanje odgovarajuće programske podrške.

Provjera DMARC mehanizma na strani primatelja

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Većina popularnih inačica poslužitelja elektroničke pošte podržava DMARC mehanizam – neke inačice zahtijevaju dodatne programske pakete (najčešće je riječ o *OpenDMARC* programskom paketu), dok ostale inačice (osobito veliki pružatelji usluga elektroničke pošte, npr. Office 365) podršku za DMARC imaju automatski ugrađenu i omogućenu.

Konfiguracija DMARC mehanizma na strani poslužitelja svodi se na omogućavanje ili onemogućavanje izrade skupnih, odnosno forenzičkih izvještaja za primljene poruke elektroničke pošte te omogućavanje dodatnih mogućnosti za upravljanje porukama za koje DMARC validacija nije bila uspješna (ovisno o postavljenoj politici).

Za konkretne postavke potrebno je proučiti službenu dokumentaciju autora poslužitelja elektroničke pošte ili DMARC programske podrške za konkretnu inačicu poslužitelja elektroničke pošte.

Preporuča li se stvaranje skupnih i/ili forenzičkih izvještaja na strani primatelja?

Iako se omogućavanje izrade izvještaja i njihovo slanje na adrese koje su navedene u `rua`/`ruf` parametrima **u općenitom slučaju preporučuje**, prilikom postavljanja takve mogućnosti, treba uzeti u obzir moguće negativne posljedice.

Preporučuje se stvaranje skupnih izvještaja i njihovog slanja na odgovarajuće adrese, no omogućavanje te opcije će vrlo vjerojatno zahtijevati dodatnu programsku podršku na poslužitelju elektroničke pošte (npr. bazu podataka u koju će se pohranjivati agregirani statistički podaci vezani uz DMARC provjeru) te uzrokovati dodatno opterećenje poslužitelja, što u određenim slučajevima može biti neprihvatljivo.

Stvaranje forenzičkih izvještaja može biti vrlo intenzivno i može značajno opteretiti poslužitelj, a dodatni nedostatak predstavlja činjenica da forenzički izvještaj može sadržavati i potencijalno osjetljive (osobne) podatke koji nisu namijenjeni kontakt osobama navedenima u `ruf` parametru. Zbog navedenih nedostataka njihovo se omogućavanje preporuča samo uz dodatno provedena testiranja.

U slučaju korištenja vanjske usluge elektroničke pošte, vrlo velik broj pružatelja usluga ima automatski omogućenu izradu izvještaja na strani primatelja i nije potrebno provoditi nikakve dodatne korake.

Ima li smisla imati DMARC zapis u DNS poslužitelju bez validacije na strani primatelja poruka?

Slično SPF mehanizmu, u određenim slučajevima na strani primatelja poruka nije moguće implementirati DMARC mehanizam (npr. nedostatna programska podrška).

I u takvim slučajevima, **svakako se preporuča implementacija DMARC mehanizma na strani pošiljatelja** (tj. dodavanje odgovarajućeg DMARC zapisa s pripadnom politikom). U tom slučaju, potrebno je osigurati postojanje barem jednog dodatnog mehanizma na strani pošiljatelja (SPF i/ili DKIM).

Kao i kod SPF mehanizma, postojanje DMARC zapisa smatra se sastavnim dijelom *sigurnosne higijene* i dobrom sigurnosnom praksom.

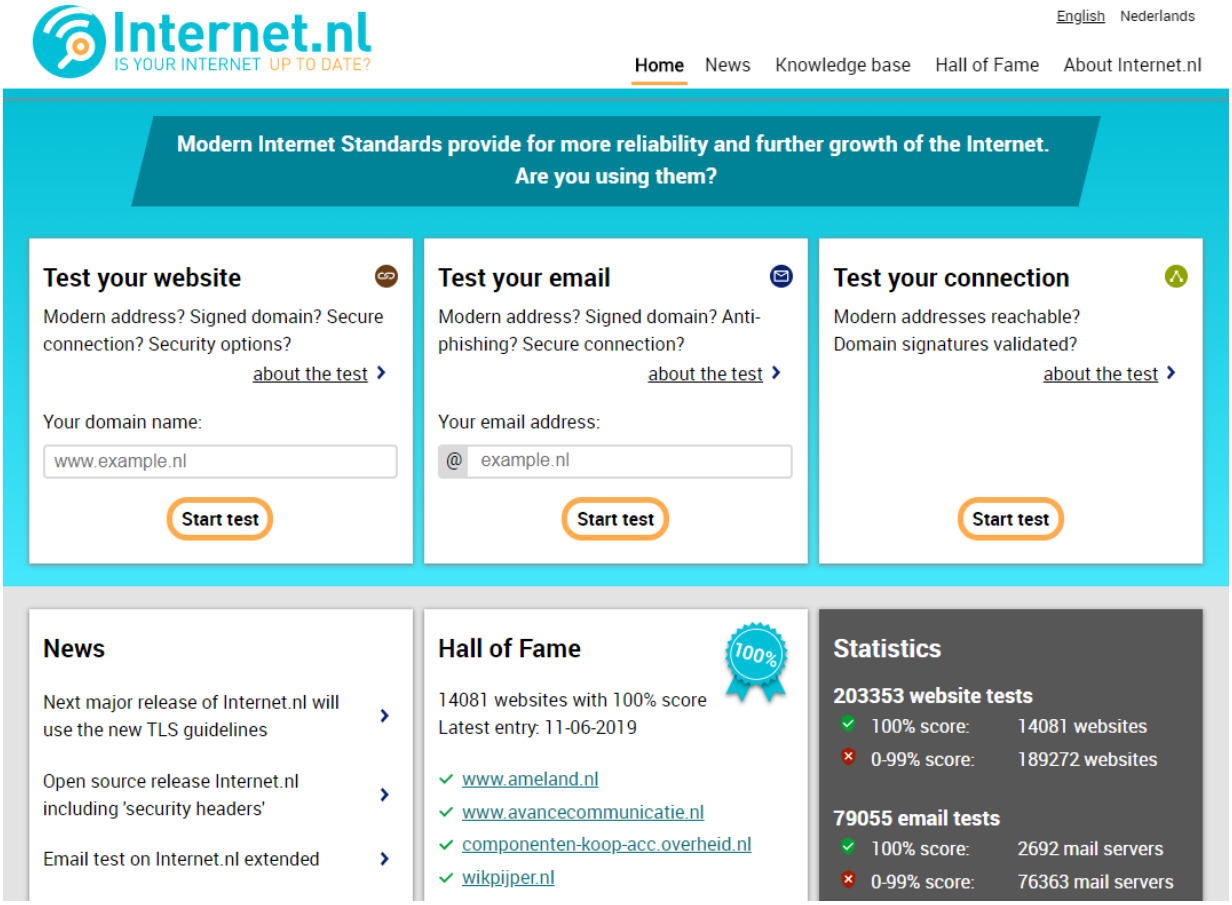
Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

6. Provjera dostupnosti i ispravnosti mehanizama

Tijekom i nakon implementacije opisanih sigurnosnih mehanizama, često je potrebno provjeriti ispravnost njihove implementacije te koriste li se za sve mehanizme ispravne/preporučene postavke. Navedenu provjeru potrebno je provesti iz perspektive neovisne organizacije (tj. treće strane), kako bi se simulirali uvjeti slični uvjetima prilikom stvarnog prijenosa (primitka ili slanja) poruke elektroničke pošte. Iako je provjere moguće provesti i korištenjem komandno-linijskih alata, zbog jednostavnosti provjere pregledom su obuhvaćeni samo javno dostupni servisi u obliku web aplikacija.

Za općenitu provjeru implementacije navedenih mehanizama i postavki preporuča se korištenje sljedećih javno dostupnih i besplatnih servisa:

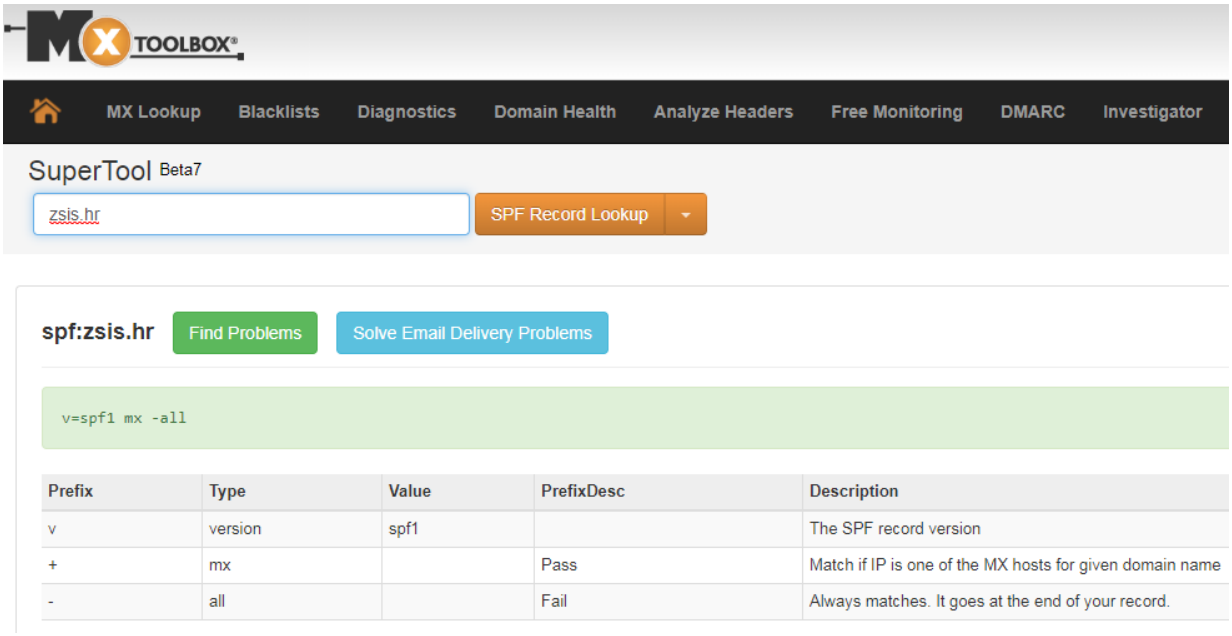
- **Internet.nl** (https://internet.nl) – inicijativa nizozemske Standardizacijske Platforme koja obuhvaća veći broj tijela zaduženih za informacijsku sigurnost i uvođenje informacijskih standarda u privatna i javna tijela. Web aplikacija omogućava provjeru implementacije standarda za sigurnu komunikaciju elektroničkom poštom koji su navedeni u dokumentu, uz detaljan opis postavljenih i preporučenih vrijednosti.



Slika 5: Internet.nl platforma

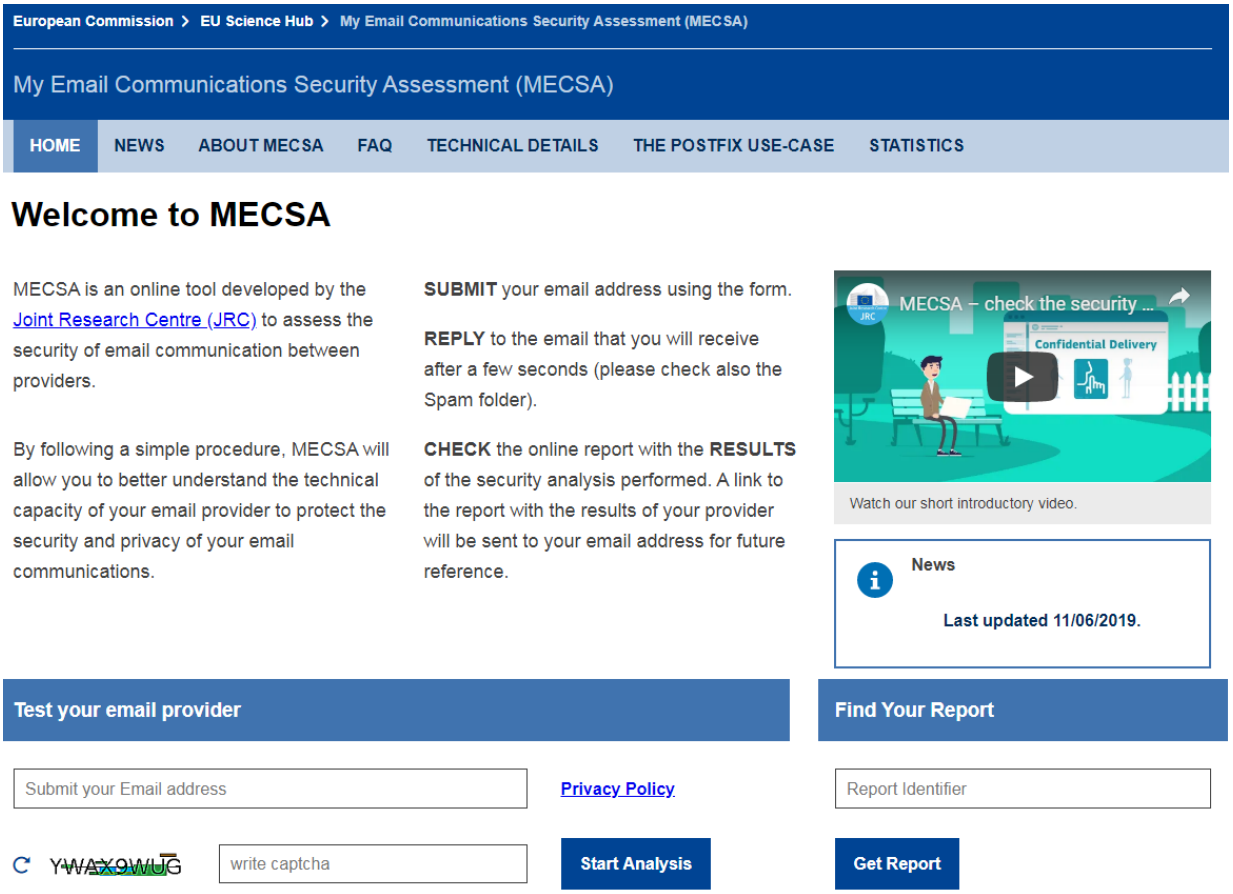
- **MxToolbox** (https://mxtoolbox.com) – skup dijagnostičkih alata koji uključuje veliki broj dostupnih provjera kojima je moguće provjeriti stanje implementacije pojedinih sigurnosnih mehanizama, uz dodatne preporuke za poboljšanja i nadogradnje.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110



Slika 6: MxToolbox – skup dijagnostičkih alata za provjeru implementacije sigurnosnih mehanizama

- **MECSA** (https://mecsa.jrc.ec.europa.eu/) – platforma razvijena od istraživačkog centra Europske komisije (JRC) koja na temelju razmijenjenih poruka elektroničke pošte ispituje stanje implementacije sigurnosnih mehanizama. Platforma također sadržava i vrlo detaljne implementacijske preporuke za uspostavu pojedinih sigurnosnih mehanizama. Također, platforma predstavlja nadopunu prethodno opisanih alata, jer se uz DNS zapise provjeravaju i stvarne poruke elektroničke pošte koje se tijekom provjere razmjenjuju s platformom.

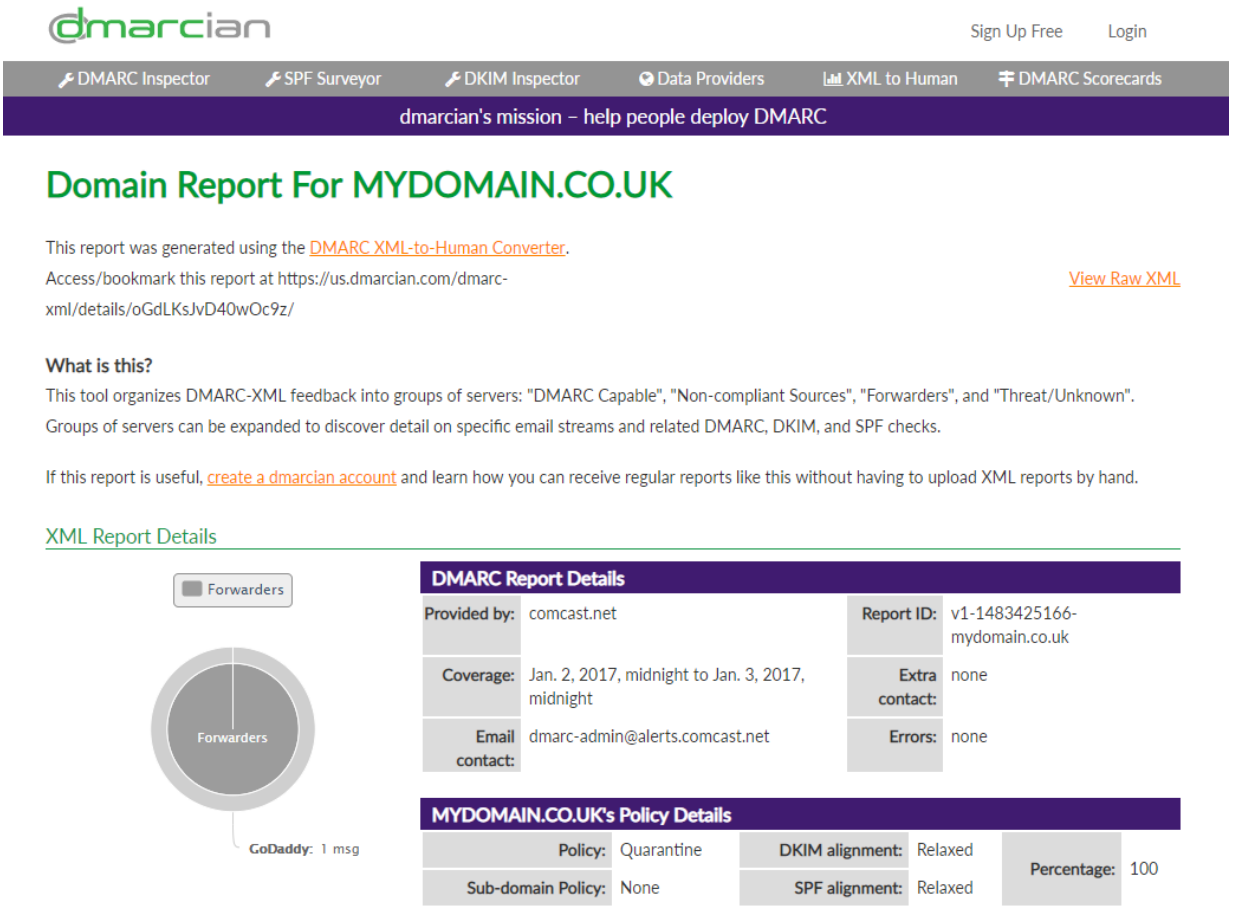


Slika 7: JRC MECSA – platforma za provjeru standarda sigurne komunikacije elektroničkom poštom

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

Osim javno dostupnih aplikacija za provjeru implementacije mehanizama, tijekom implementacije i korištenja DMARC mehanizma često se pojavljuje potreba za jednostavnim (čitljivim) ispisom primljenih skupnih izvještaja. U nastavku su prikazani primjeri javno dostupnih aplikacija za analizu DMARC izvještaja:

- **XML to Human** (https://us.dmarcian.com/xml-to-human-converter/) – aplikacija za pretvaranje skupnog izvještaja iz XML formata u čitljiv i jasno razumljiv oblik



7. Zaključak

Otkrivanje i sprječavanje primitka lažiranih poruka elektroničke pošte, ali i njihovog slanja u ime vlastite organizacije nije jednostavan zadatak. Opisani tehnički standardi i mehanizmi značajno umanjuju rizik od slanja i primitka lažiranih poruka te nastoje uspostaviti sigurni komunikacijski kanal između poslužitelja elektroničke pošte s ciljem sprječavanja mogućeg presretanja poruka u njihovom prijenosu.

Pojedini mehanizmi opisani u dokumentu nisu trivijalni za implementaciju i njihovo potpuno uvođenje zahtijeva dulje vrijeme. Također, razina sigurnosti (odnosno otpornosti na lažirane poruke) izravno ovisi o stupnju raširenosti primjene navedenih mehanizama.

Primjenom tehničkih smjernica, tj. ulaganjem u implementaciju standarda, ispravnim postavkama i raširenom upotrebom suvremenih standarda za sigurnu komunikaciju, organizacija čini korak u pravom smjeru te postaje dio globalne i sigurne komunikacijske mreže za razmjenu elektroničke pošte.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110

8. Reference

1. *IT Security Guidelines for Transport Layer Security (TLS)*, https://www.ncsc.nl/english/current-topics/factsheets/it-security-guidelines-for-transport-layer-security-tls.html, *National Cyber Security Centrum Netherlands*, travanj 2019.
2. *Cipherli.st*, https://cipherli.st/, lipanj 2019.
3. OpenSPF, http://www.open-spf.org/, lipanj 2019.
4. *Sender Policy Framework*, https://en.wikipedia.org/wiki/Sender_Policy_Framework, *Wikipedia*, lipanj 2019.
5. *DomainKeys Identified Mail (DKIM) Signatures*, https://tools.ietf.org/html/rfc6376, Internet Engineering Task Force (IETF) RFC 6376, rujan 2011.
6. *Domain-based Message Authentication, Reporting, and Conformance (DMARC)*, https://tools.ietf.org/html/rfc7489, Internet Engineering Task Force (IETF) RFC 7489, ožujak 2015.

Zavod za sigurnost informacijskih sustava, Fra Filipa Grabovca 3, Zagreb, tel. 01/4694-100, fax 01/4694-110