HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Caller ID za poruke elektroničke pošte

CCERT-PUBDOC-2004-07-82

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Spam poruke, najčešće definirane kao neželjena elektronička pošta, postaju sve ozbiljniji problem informacijskih sustava. Borbi protiv spama posljednjih je godina posvećeno mnogo pažnje i danas postoje brojne tehnike, servisi i alati koji olakšavaju prepoznavanje i filtriranje spam poruka. Danas na tržištu postoje brojni komercijalni i besplatni antispam alati kojima se korisnici Interneta služe kako bi što efikasnije prepoznali i reducirali količinu spam poruka. Iako je potpuno suzbijanje spam poruka gotovo nemoguće, ohrabruje činjenica da se i dalje svakodnevno razvijaju nova rješenja koja će, nadamo se, uspjeti smanjiti količinu spam poruka na prihvatljivu razinu.

Jedan od nedostataka sustava elektroničke pošte koji dodatno otežava detekciju izvora nelegitimnih e-mail poruka je taj da se poruke mogu vrlo lako lažirati, odnosno poslati s adrese neke domene bez dozvole njenog vlasnika (eng. *spoofed address* ili *spoofed domain name*). Ovaj nedostatak *spammeri* vrlo vješto koriste kako bi prikrili izvor slanja poruke, tako da većina spam poruka danas u svom zaglavlju sadrži lažne podatke o pošiljaocu te izvoru poruke općenito. Osim prikrivanja izvora, lažiranje poruka stvara probleme i za vlasnike domena budući da se adrese s njihove domene koriste u nelegitimne svrhe.

Budući da vlasnici domena žele kontrolirati poruke koje sadrže naziv njihove domene, razvijene su metode koje to omogućuju. Kao rješenje problema lažiranja naziva domena, Microsoft je razvio *Caller ID* sustav za poruke elektroničke pošte. Ovo rješenje ima namjenu vlasnicima domena omogućiti zaštitu svojih domena od krivotvorenja, a primateljima poruke omogućuje identifikaciju neželjenih poruka. *Caller ID* za poruke elektroničke pošte stoga ima dvojnu funkciju. Primarna funkcija je borba protiv lažiranja naziva domena te lažnog predstavljanja, a sekundarna funkcija je borba protiv spam poruka.

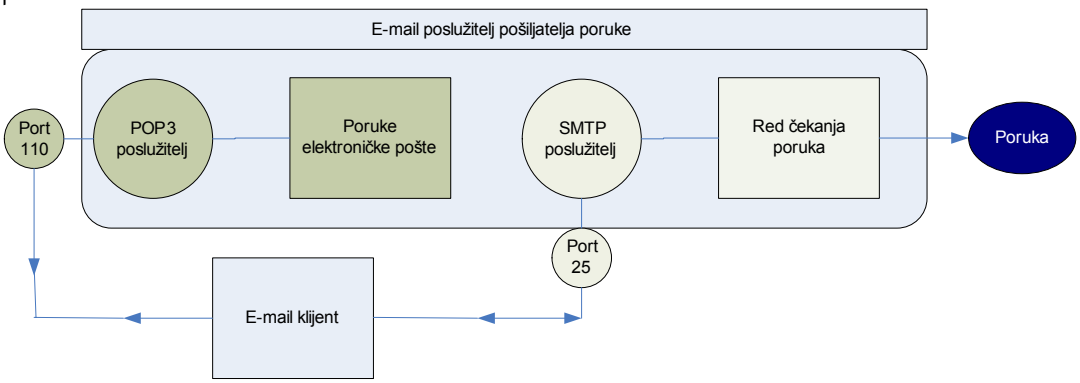
Dokument donosi kratki pregled sustava elektroničke pošte te opisuje *Caller ID* sustav opisujući način njegovog funkcioniranja i korištenja.

2. Promet poruka elektroničke pošte

Radi boljeg razumijevanja prijedloga *Caller ID* sustava za poruke elektroničke pošte u nastavku dokumenta ukratko će biti opisan sustav komunikacije porukama elektroničke pošte.

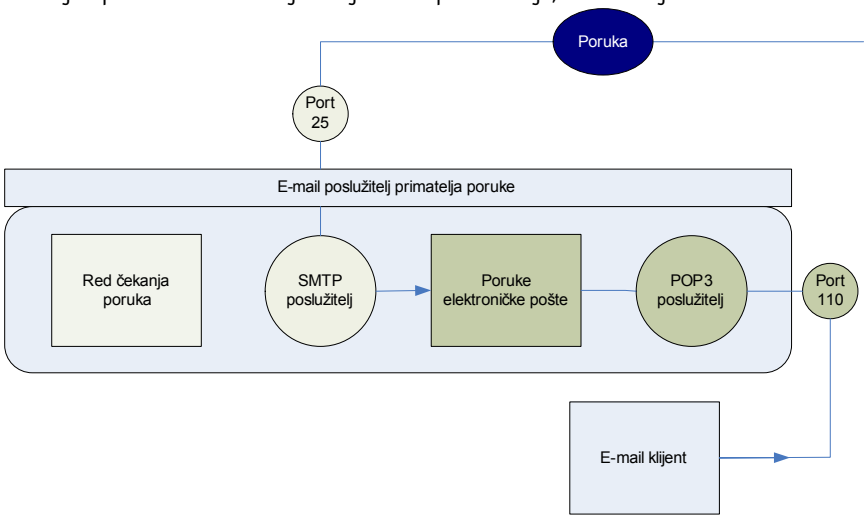
Sustav elektroničke pošte temelji se na izmjeni poruka između dva sustava koji imaju ostvarenu međusobnu komunikaciju. Sustav elektroničke pošte sastoji se od dva tipa poslužitelja. Prvi su POP3 (eng. *Post Office Protocol*) ili IMAP poslužitelji (eng. *Internet Mail Access Protocol*) koji klijentima omogućuju pristup elektroničkoj pošti, a drugi je SMTP poslužitelj (eng. *Simple Mail Transfer Protocol*) zadužen za primanje i slanje poruka elektroničke pošte.

Promet poruka odvija se tako da klijent kada želi poslati poruku elektroničke pošte, uspostavlja dvosmjernu komunikaciju sa SMTP poslužiteljem. SMTP poslužitelj preuzima odgovornost poslati poruku jednom ili više SMTP poslužitelja ili uzvratiti klijentu poruku da proces slanja nije uspio. SMTP poslužitelj osluškuje TCP port broj 25. Slika 1 prikazuje princip rada poslužitelja poruka elektroničke pošte.



Slika 1: E-mail poslužitelj pošiljatelja poruke

Kada *e-mail* klijent pošalje poruku elektroničke pošte, SMTP poslužitelj ostvaruje komunikaciju s ciljnim SMTP poslužiteljem kako bi se izvršila isporuka poruke. Prijenos poruka izvodi se putem SMTP protokola. Ono što SMTP poslužitelj šalje je objekt poruke sastavljen od omotnice (engl. *envelope*) i sadržaja poruke(engl. *body*). Omotnica poruka sastavljena je od niza zaglavlja SMTP protokola koja sadrže adresu izvorišta poruke, jednu ili više adresa primatelja poruke te druge elemente protokola koji pomažu u procesu slanja i obrade poruka.
Pri primanju poruke, SMTP poslužitelj adresu primatelja rastavlja na dijelove, na korisničko ime primatelja i na naziv domene. U slučaju da je poruka poslana na adresu `zmarkic@domena.hr` adresa se rastavlja na korisničko ime `zmarkic` i na domenu `domena.hr`. Slijedeći korak SMTP poslužitelja je ostvarivanje komunikacije s DNS poslužiteljem (eng. *Domain Name Server*) autoritativnog za domenu `domena.hr` s upitom za IP adresom SMTP poslužitelja domene `domena.hr`. Ova IP adresa u DNS sustavu sadržana je putem MX (engl. *Mail Exchanger*) zapisa. SMTP poslužitelj pošiljatelja, nakon dobivene IP adrese, ostvaruje komunikaciju s ciljnim SMTP poslužiteljem putem porta 25, isporučuje poruku nakon čega se ista pohranjuje u poštanski sandučić krajnjeg korisnika. Pohranjene poruke korisniku se stavljaju na raspolaganje putem ranije spomenutih POP (TCP/110) i IMAP (TCP/143) servisa.
Slika 2 prikazuje opisanu komunikaciju dvaju SMTP poslužitelja, nadovezujući se na sliku 1.



Slika 2: *E-mail poslužitelj primatelja poruke*

2.1. Nazivi domena

Kada korisnik šalje poruku elektroničke pošte, on koristi određeni naziv domene (eng. *domain name*). Primjer naziva domene u ovom dokumentu je `domena.hr` pri čemu korisnik ima oblik adrese elektroničke pošte `korisnicko_ime@domena.hr`. Ovako napisan naziv domene čitljiv je ljudima, međutim, računala nazive domena prepoznaju u obliku IP adresa, npr. 213.183.101.152. Pretvaranje naziva domene iz oblika čitljivog ljudima u 32-oktetni numerički oblik funkcija je DNS poslužitelja. Uloga DNS poslužitelja u procesu slanja poruka elektroničke pošte je ta da na temelju e-mail adrese korisnika odredi IP adresu mail poslužitelja zaduženog za primanje elektroničke pošte za tu domenu (engl. *Mail Exchanger*). Trenutna specifikacija SMTP protokola omogućuje vrlo jednostavno lažiranje poruka elektroničke pošte, što predstavlja iznimno velik problem s obzirom na stroge sigurnosne zahtjeve koji se danas predstavljaju pred informacijske sustave. Mogućnost slanja poruke sa proizvoljno postavljenim vrijednostima njenog pošiljatelja neovlaštenim korisnicima otvara brojne mogućnosti za zloupotrebu e-mail servisa što je vrlo često i slučaj. *Caller ID* sustav za poruke elektroničke pošte je Microsoftov prijedlog rješenja kojim će se onemogućiti lažiranje naziva domena te smanjiti broj spam poruka. U nastavku dokumenta biti će ukratko opisan osnovni koncept *Caller ID* sustava i načela na kojima se isti bazira.

3. *Caller ID* za poruke elektroničke pošte

Caller ID sustav za poruke elektroničke pošte (eng. *Caller ID for E-mail*), kao i *SPF* (eng. *Sender Policy Framework*), je prijedlog kojim se pokušava riješiti problem lažiranja adresa elektroničke pošte, odnosno naziva domena, koje je prema trenutnoj specifikaciji SMTP protokola vrlo lako lažirati. Ujedno se pokušava riješiti problem spam poruka jer većina takvih poruka lažira adresu pošiljatelja kako bi se otežala detekcija izvora poruke. Za rješavanje problema spam poruka filtri trebaju dodatne informacije koje u današnjim porukama nisu dostupne. S ovog stajališta ponuđeno je novo tehnološko rješenje koje čini jednostavne promjene u strukturi elektroničke pošte, ali koje su potrebne kako bi se podigla razina sigurnosti sustava elektroničke pošte te omogućilo jasno razlikovanje od potencijalnih pošiljatelja spam poruka. Ovaj koncept bazira se na tri opća prijedloga unaprjeđenja filtriranja poruka, a to su: uspostava potvrde identiteta pošiljatelja poruke korištenjem *Caller ID* sustava, omogućiti pošiljateljima velikog broja poruka potvrdu legitimnosti poslanih poruka te kreirati prepoznatljive elemente koji će pošiljatelje malih količina poruka razlikovati od pošiljatelja spam poruka.

Koncept identifikacije pošiljatelja, kao i identifikacija telefonskog poziva, sastoji se od autentikacije pošiljatelja na način da pošiljatelji poruka objave IP adrese njihovih odlaznih poslužitelja za elektroničku poštu u DNS sustav (eng. *Domain Name System*) u formatu koji je točno specificiran. Primateljev sustav ispituje svaku pristiglu poruku kako bi se ustanovilo da li označava ispravnu domenu tako da šalje upit DNS sustavu za listom svih prijavljenih IP adresa odlaznih poslužitelja za elektroničku poštu. Na temelju analize dobivenih adresa odobrava se ili odbija odgovarajuća poruka.

Promet poruka koristi prije spomenuti SMTP protokol koji provjerava naziv domene u DNS sustavu te koristi MX (eng. *Mail Exchanger*) zapis za dolazak do IP adrese SMTP poslužitelja zaduženog za primanje elektroničke pošte na određenoj domeni. To znači da svaka domena treba specificirati koji su poslužitelji zaduženi za primanje elektroničke pošte te ih u obliku MX zapisa pohraniti u autoritativni DNS poslužitelj.

Za razliku od adrese elektroničke pošte koju je iznimno lako krivotvoriti, s IP adresama je to mnogo veći problem. Lažiranje IP adresa (engl. *IP Spoofing*) postupak je koji zahtjeva prilično visoku razinu znanja i stručnosti i smatra se da se u okviru detekcije legitimnih izvora poruka IP adresa može smatrati vjerodostojnom.

U današnje vrijeme vrlo je korisno znati koja računala određene domene, odnosno s koje IP adrese, je dopušteno slanje poruka. Ukoliko primateljev dolazni poslužitelj može usporediti IP adresu s koje poruka dolazi s IP adresom koja je označena od strane vlasnika domene s koje je poslana poruka, tada je poruka ispravna, a u protivnom može biti odbijena. Ovakvim načinom rada, i pošiljatelj i primatelj imaju beneficije. Pošiljatelji na ovaj način specificiraju legitimne IP adrese svojih odlaznih mail poslužitelja te onemogućuju slanje poruka sa adresama svoje domene putem bilo kojeg drugog mail poslužitelja. Primatelji poruka mogu isti koncept iskoristiti za detekciju lažiranih poruka te ih odbiti umjesto da ih obrađuju kao što je to najčešće slučaj.

3.1. Politika elektroničke pošte i objava domene

Caller ID sustav za poruke elektroničke pošte temelji se, kao što je prije spomenuto, na prepoznavanju IP adresa pošiljatelja poruka. Iz tog razloga, svaka organizacija koja želi da njezine poruke budu obrađene kao ispravne, mora objaviti IP adrese odlaznih mail poslužitelja u DNS sustav putem dokumenta koji se naziva politika elektroničke pošte (eng. *e-mail policy document*). Svaki vlasnik domene treba politiku elektroničke pošte objaviti kao DNS tekstualni zapis koji sadrži slobodnu formu teksta te je spremljen kao tekstualni tip datoteke (eng. *txt*). *Caller ID* za poruke elektroničke pošte koristi tekstualni zapis za spremanje politike elektroničke pošte u *XML* formatu (eng. *eXtensible Markup Language*).

Da bi se izvršila objava IP adrese odlaznog poslužitelja za poruke elektroničke pošte potrebno je najprije identificirati poslužitelj i njegovu IP adresu. Ukoliko se u ovu svrhu koristi više poslužitelja, postupak je potrebno provesti za svaki poslužitelj zasebno. Ako se za ovu svrhu koriste usluge treće strane kao pružatelja usluge, potrebno je znati nazive njihovih domena. Nakon identifikacije poslužitelja treba izraditi politiku elektroničke pošte za svaku domenu i poddomenu koja služi za slanje poruka iz organizacije.

Primjer politike elektroničke pošte s parametrima izgleda ovako:

```
<ep xmlns='http://dmn.net/1' testing='true'><out>
<m><a>192.168.0.123</a></m>
</out></ep>
```

Oznake korištene u tekstualnom zapisu su slijedeće:

- `ep` oznaka indicira na vrstu dokumenta (eng. *e-mail policy*),
- `xmlns` parametar označava *XML* prostor imena koji identificira vrstu elementa i imena atributa, a u ovom slučaju to je najčešće *URL* (eng. *Uniform Resource Locator*),
- `testing` atribut upućuje na to da određena domena trenutno testira politiku elektroničke pošte dok se primanje poruka i dalje odvija kao da ovaj dokument nije objavljen,
- `out` element je spremnik koji opisuje poslužitelj za slanje poruka elektroničke pošte,
- `m` element je spremnik koji sadrži informacije o poslužitelju,
- `a` element sadrži *IP* adresu jednog poslužitelja za poruke elektroničke pošte.

Predlošci za izradu politike elektroničke pošte obuhvaćaju nekoliko scenarija. Mogući scenariji i primjeri politike elektroničke pošte pojedinog scenarija su:

1. domena nema odlazne poslužitelje za poruke elektroničke pošte, a želi se zaštiti od krivotvorenja,

```
<ep xmlns='http://dmn.net/1'><out>
<noMailservers>
</out></ep>
```

2. odlazni i dolazni poslužitelj poruka elektroničke pošte su isti,

```
<ep xmlns='http://dmn.net/1'><out>
<m><mx/></m>
</out></ep>
```

3. jedan odlazni poslužitelj poruka elektroničke pošte,

```
<ep xmlns='http://dmn.net/1' testing='true'><out>
<m><a>192.168.0.123</a></m>
</out></ep>
```

4. nekoliko odlaznih poslužitelja poruka elektroničke pošte,

```
<ep xmlns='http://dmn.net/1' testing='true'><out><m>
<a>192.168.0.123</a>
<a>192.168.0.124</a>
<a>192.168.0.126</a>
</m></out></ep>
```

5. nekoliko odlaznih poslužitelja poruka elektroničke pošte u rangu adresa,

```
<ep xmlns='http://dmn.net/1' testing='true'><out>
<m><r>192.168.0.1/25</r></m>
</out></ep>
```

6. direktne poruke elektroničke pošte,

```
<ep xmlns='http://dmn.net/1' testing='true'>
<out directOnly='true'><m>
<a>192.168.0.123</a></m>
</out></ep>
```

7. pružanje usluga odlaznog poslužitelja poruka elektroničke pošte treće strane,

```
<ep xmlns='http://dmn.net/1'><out><m>
<indirect>provider.hr</indirect></m>
</out></ep>
```

8. pružanje usluge smještanja poslužitelja poruka elektroničke pošte,

```
<ep xmlns='http://dmn.net/1'><out><m>
<indirect>provider.hr</indirect></m>
</out></ep>
```

Nakon kreiranja politike elektroničke pošte slijedi objava dokumenta. Prije je spomenuto da se objava izvodi kao DNS tekstualni zapis. DNS sustav definira nekoliko tipova zapisa koji mogu biti objavljeni. Kako bi se ovaj zapis za *Caller ID* funkciju razlikovao od ostalih zapisa, potrebno ga je spremiti s prefiksom `_ep`. Na primjer, ukoliko je određena organizacija objavila svoju domenu imena `domena.hr` , tada je politiku elektroničke pošte potrebno objaviti pod imenom `_ep.domena.hr`. Veličina datoteke mora biti najviše 2K.

Za domenu se neće smatrati da ima izjavu o odlaznim poslužitelja za poruke elektroničke pošte ukoliko ne postoji politika elektroničke pošte, odnosno ukoliko politika postoji, ali nema elemente `ep/out/m` ili elemente `ep/out/noMailServers`.

Skup *IP* adresa s kojih određena domena ima mogućnost poslati poruke elektroničke pošte označava se funkcijom `OutGoing(d)`, gdje `d` predstavlja domenu, a koja se definira na slijedeći način:

- ukoliko u politici postoje elementi `ep/out/noMailServers` domene `d`, tada je funkcija `OutGoing(d)` prazan skup,
- ukoliko postoji barem jedan element `ep/out/m` u politici, tada je funkcija `OutGoing(d)` definirana kao udruženje svih `ep/out/m` elemenata `m`, tako da se funkcija definira kao OutGoing(m,d) za svaki pojedini element `m`,
- u protivnom, rezultat funkcije `OutGoing(d)` je nedefiniran.

3.2. Identifikacija odgovorne domene za poruke elektroničke pošte

Svaka poruka elektroničke pošte koja se šalje kroz SMTP poslužitelj jedne organizacije drugoj, ima odgovornu adresu koja je određena iz prvog od nekoliko podataka od kojih barem jedan mora biti prisutan u poruci i ne može biti prazan. Ti podaci su:

- prvo polje `Resent-Sender` u poruci koje prethodi polju `Resent-From`,
- prvi poštanski sandučić (eng. *mailbox*) u prvom polju `Resent-From` ,
- polje `Sender`,
- prvi poštanski sandučić u polju `From`,

Svaka poruka elektroničke pošte ima barem jedno od navedenih polja. Ukoliko primatelj dobije poruku koja ne sadrži niti jedno od navedenih polja, poruka je sigurno spam.

Značenja polja od kojih barem jedno mora biti prisutno u poruci elektroničke pošte su:

- `Resent-Sender: adresa1@domena.hr`,
  - poruka je prethodno dostavljena u poštanski sandučić krajnjeg odredišta, ali je naknadno preusmjerena u transportni sustav poruka, a `adresa1@domena.hr` je agent koji je izvršio preusmjeravanje u ime korisnika navedenog u polju `Resent-From`, čija je želja bila da se poruka preusmjeri,
- `Resent-From: adresa2@domena.hr`,
  - poruka je prethodno dostavljena u poštanski sandučić krajnjeg odredišta, ali je naknadno preusmjerena u transportni sustav poruka, a `adresa2@domena.hr` je korisnik čija je želja bila da se poruka preusmjeri,
- `Sender: adresa3@domena.hr`,
  - `adresa3@domena.hr` je agent koji je odgovoran za prijenos poruke,
- `From: adresa4@domena.hr`,
  - `adresa4@domena.hr` je autor poruke.

Odgovorna domena za poruke elektroničke pošte definira se kao oznaka domene kao dijela poruke koja je poslana sa značajno odgovorne adrese. Primjer odgovorne domene za poruke poslane s adrese `korisnicko_ime@domena.hr` je `domena.hr`.

3.3. Provjera odgovorne domene za poruke elektroničke pošte

Kada je identificirana odgovorna domena `p` za poruku `m`, IP adresa s koje je poruka `m` primljena treba biti provjerena u popisu IP adresa s koje je slanje poruke `m` iz domene `p` očekivano. Funkcija

`OutGoing(p)` analizira politiku elektroničke pošte kako bi saznala skup mogućih IP adresa s kojih određena domena može postali poruku. Taj skup IP adresa uspoređuje se s IP adresom SMTP klijenta koji šalje poruku s ciljem identifikacije da li je ime domene lažirano ili nije. Rezultat ove provjere odgovorne domene je formiranje podatka koji prolazi kroz filtar elektroničke pošte. Ukoliko se ustanovi da je domena krivotvorena, sustav za primanje poruke ne smije slati status o rezultatu dostavljanja poruke.
Komplikacije nastaju kada se provjera odgovorne domene odvija na strani e-mail klijenta koji su unutar organizacije. Općenito, takvim aplikacijama je teško ustanoviti s koje IP adrese je stigla poruka u organizaciju. Međutim, ova informacija može biti sakupljena kroz pažljivu obradu polja `Received` u zaglavlju poruke.

4. Licenciranje

Microsoft ima za cilj široku implementaciju i proširenje rješenja *Caller ID* za poruke elektroničke pošte. Licenca za implementaciju ovog rješenja je besplatna, no kao povlastica (eng. *royalty free license*), što znači da je potrebno na referentnoj adresi http://download.microsoft.com/download/6/0/a/60a02573-3c00-4ee1-856bafa39c020a95/callerid_license.pdf doći do dokumenta te svojim vlastoručnim potpisom i nekim dodatnim elementima potvrditi suglasnost s licenčnim dogovorom. Potpisan dokument potrebno je poslati Microsoftu, a svaki korisnik biti će na popisu licenciranih korisnika na Web stranici. Dokument sadrži kontakt informacije i načine na koje se licenčni dokument može poslati.

5. Zaključak

Caller ID za poruke elektroničke pošte predstavlja rješenje koje onemogućuje krivotvorenja poruka elektroničke pošte te smanjuje promet spam poruka. Iako ovo rješenje ne sprječava slanje spam poruka, prema opisanom načinu funkcioniranja može se zaključiti kako je ovim putem moguće uvelike smanjiti njihov broj. Prednost ovog prijedloga jest onemogućavanje lažiranja poruka elektroničke pošte, no ujedno je i nedostatak što se svaka domena mora prijaviti politikom elektroničke pošte, ukoliko želi da se poruke poslane s te domene obrađuju kao normalne poruke, te da ne budu odbijene kao spam. Ukoliko određena domena ne bude prijavljena, ista će se tretirati kao krivotvorena domena ili kao pošiljatelj neželjene pošte.
Caller ID za poruke elektroničke pošte biti će testiran na javnom servisu Hotmail gdje će se uvidjeti sve prednosti te eventualni nedostaci ovog prijedloga.

6. Reference

MTA Authentication Records in DNS, Junde 2004, work in progress
http://download.microsoft.com/download/d/a/2/da2821f5-6acb-4058-8974-5a3c7d187794/senderid.pdf

Protecting Domain Names from Spoofing: A guide for E-mail Senders, Microsoft, February 2004
http://download.microsoft.com/download/8/e/4/8e4bf400-a91f-49f0-9910-a291e489dc8b/callerid_senders.pdf

Caller ID for E-mail
http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf