Epasta drošība

Kārlis Podiņš, CERT.LV

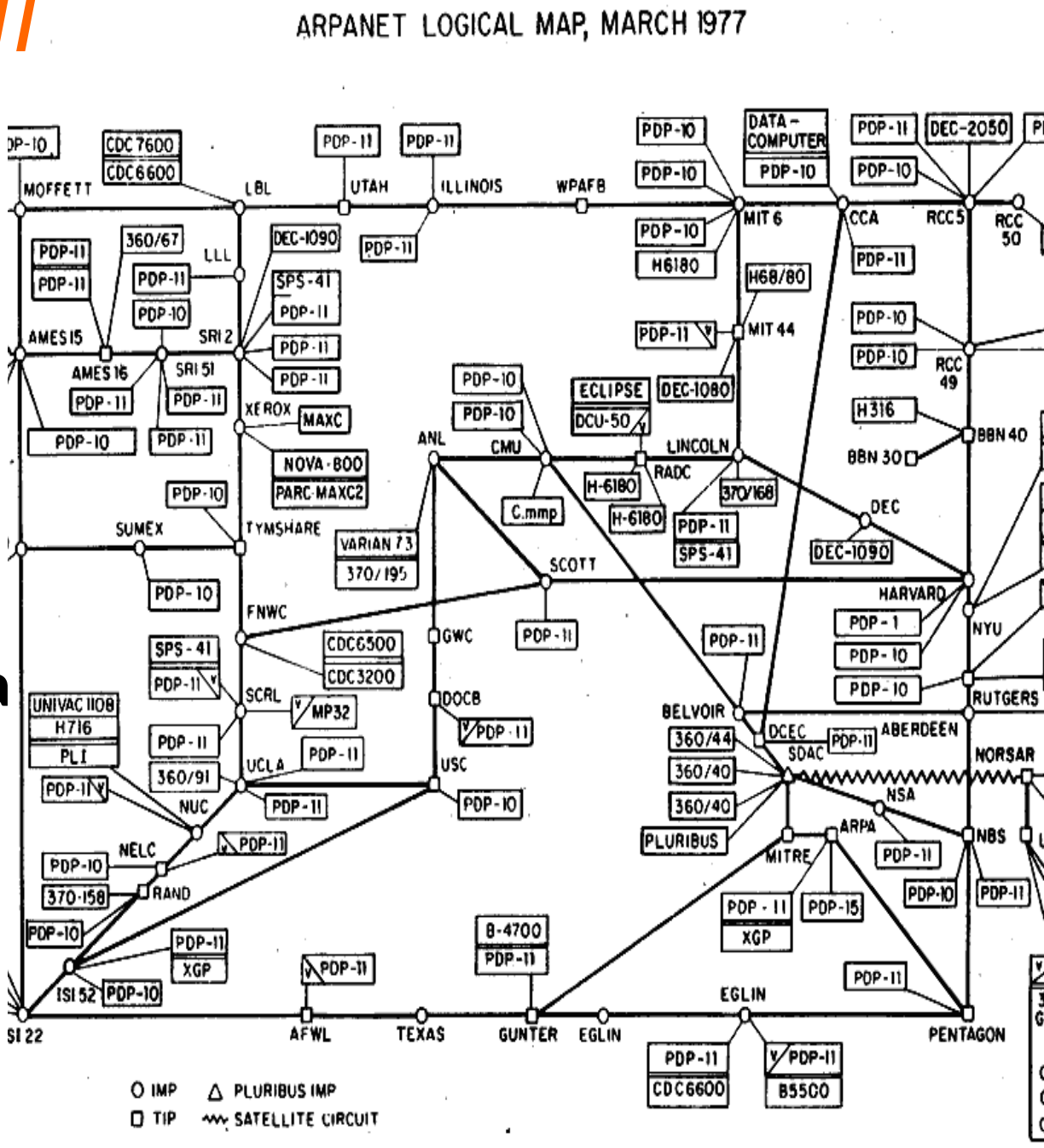
Elektroniskais pasts

- **Tvērums**
  - **Lieldators - *time sharing* mašīnas**
    - **1965. CTSS *mail* programma**
  - **Lokālais tīkls (80.gadi)**
  - **Izkliedēts tīks**
    - **1971. ARPANET email**
      - **1977. standartizēts RFC733**
  - **1983. MCI Mail – pirmais komerciālais publiskais epasta pakalpojums izmantojot internetu**
    - **Piedāvā arī parasto pastu :)**


STATES
1775

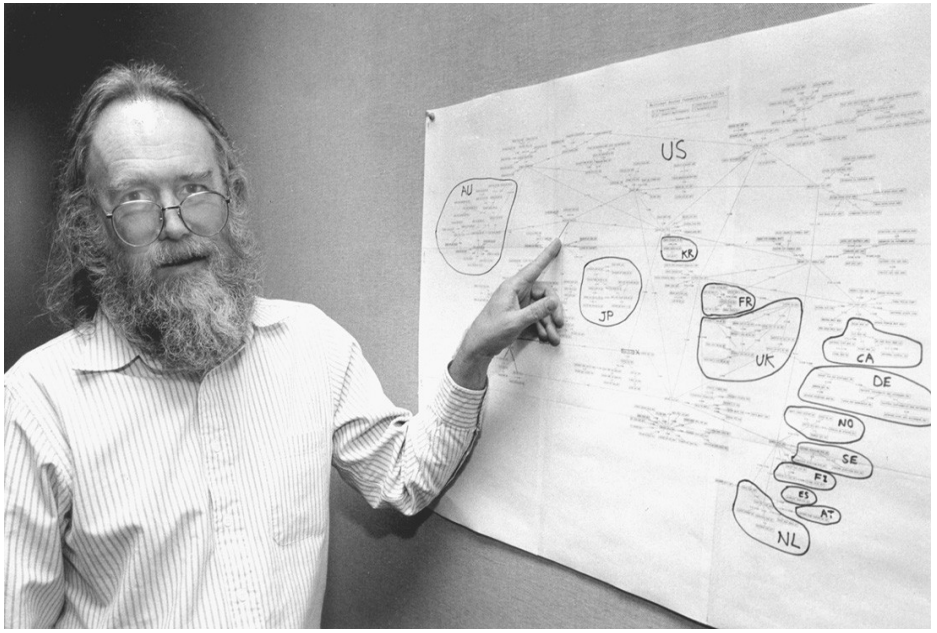
ARPANET mail

- 1969 ARPANET
- 1971 mail
- username@hostname
- 1983 DNS
  - usr@hst.dmn
- 1973 pasts 75% plūsma
- 1975 mailinglist
- 1979 -)



SMTP

- **Simple Mail Transfer Protocol**
- **1982 RFC 821**
- **Epasta mugurkauls**
  - **Epasta serveru savstarpējā komunikācija**



Художник В. Зарубин

АВИА

Индекс предприятия связи места назначения

© Министерство связи СССР, 1978 · 16/III-78 г. МТ Гознака. Зак. 2582. Ц. 6 к.

Куда

Кому

Индекс предприятия связи и адрес отправителя

SMTP

```
telnet mail.x.gov.lv 25
Trying 10.___.___.105...
Connected to mail.x.gov.lv.
Escape character is '^]'.
220 mail.x.gov.lv ESMTP Postfix
helo test
250 mail.x.gov.lv
mail from:<admin@somebody.gov.lv>
250 2.1.0 Ok
rcpt to:<upuris@somebody.gov.lv>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Labdien!
Vai vari atvērt šo saiti? http://...
```

Der 10-Millionen-Golf.

Auf diesen Rekord haben wir uns ganz besonders gefreut. Und weil der Golf seit 1975 ununterbrochen die Zulassungsstatistiken in Deutschland anführt, haben wir uns natürlich auch schon langfristig darauf vorbereitet.

Und zwar nicht nur aufs Feiern, sondern vor allem darauf, den treuen Golf-Freunden ganz herzlich „Dankeschön" zu sagen.

Denn erst die besonders hohen Ansprüche, die Sie als kritischer Autokäufer an ein Automobil stellen, haben den Golf zum Golf gemacht.

Deshalb wollen wir den Produktionsrekord von 10 Millionen Golf zum Anlaß nehmen, uns bei Ihnen mit einem ganz besonderen Angebot zu bedanken: dem 10-Millionen-Golf.

Und das heißt mit einem Golf, der eine serienmäßige Ausstattung hat, die eines Multimillionärs würdig ist.

Der dabei im Preis aber so günstig ist, daß Sie kein solcher sein müssen, um ihn sich zu leisten.

Schon auf den ersten Blick können Sie erkennen, daß hier zur Feier des Tages ein ganz besonderer Golf vor Ihnen steht. Zum Beispiel an der extra zu diesem Anlaß geschaffenen Sonderlackierung in Starblue metallic. Oder an den blaugetönten Scheiben. An den lackierten Gehäusen der von innen einstellbaren Außenspiegel. Den farbig ausgelegten 6 J × 14-Leichtmetallrädern mit breiten Reifen. Und vielen weiteren Details bis zum „10 Millionen"-Emblem an de Seite und am Heck.

Kurz: Der 10-Millionen-Go ist schon von außen ein Grun zum Feiern.

Aber es kommt noch bess wenn Sie die Tür öffnen und P nehmen.


ADAC


001717VG01
ADAC

Atpakaļsavietojamība

Risinājumi


GARDA
gardacashlogistics.com
CASH. LOGISTICS.
SMART. TECHNOLOGY.
GARDA CL GREAT LAKES
USDOT 163997
GVW 26,000

Risinājumi

- **Servera puses risinājumi**

  Domain-based Message Authentication, Reporting and Conformance DMARC

- **Klienta puses risinājumi - C,I**
  - **PKI**
    - **EID**
    - **PGP**

DMARC

- **2015 RFC 7489**
- **Servera puses risinājums**
- **Ienākošās epastu plūsmas pārbaude/filtrēšana**
- **Mērķis - atklāt un novērst nosūtītāja adreses viltošanu (*spoofing*)**
  - **cīnīties ar pikšķerēšanu mēstuļošanu**

Nonrepudiation + Integrity

DMARC

- Autori - interneta milži
  - AOL, Bank of America, Comcast, Facebook, Google, JPMorgan Chase & Company, LinkedIn, Microsoft, Paypal, Yahoo! u.c.
- Informācija, kā izmantot SPF un DKIM informāciju
- DNS ierakstā paziņo, kādus mehānismus izmanto
  - TXT Resource Record (RR)

    SPF, DKIM, SPF+DKIM

DMARC

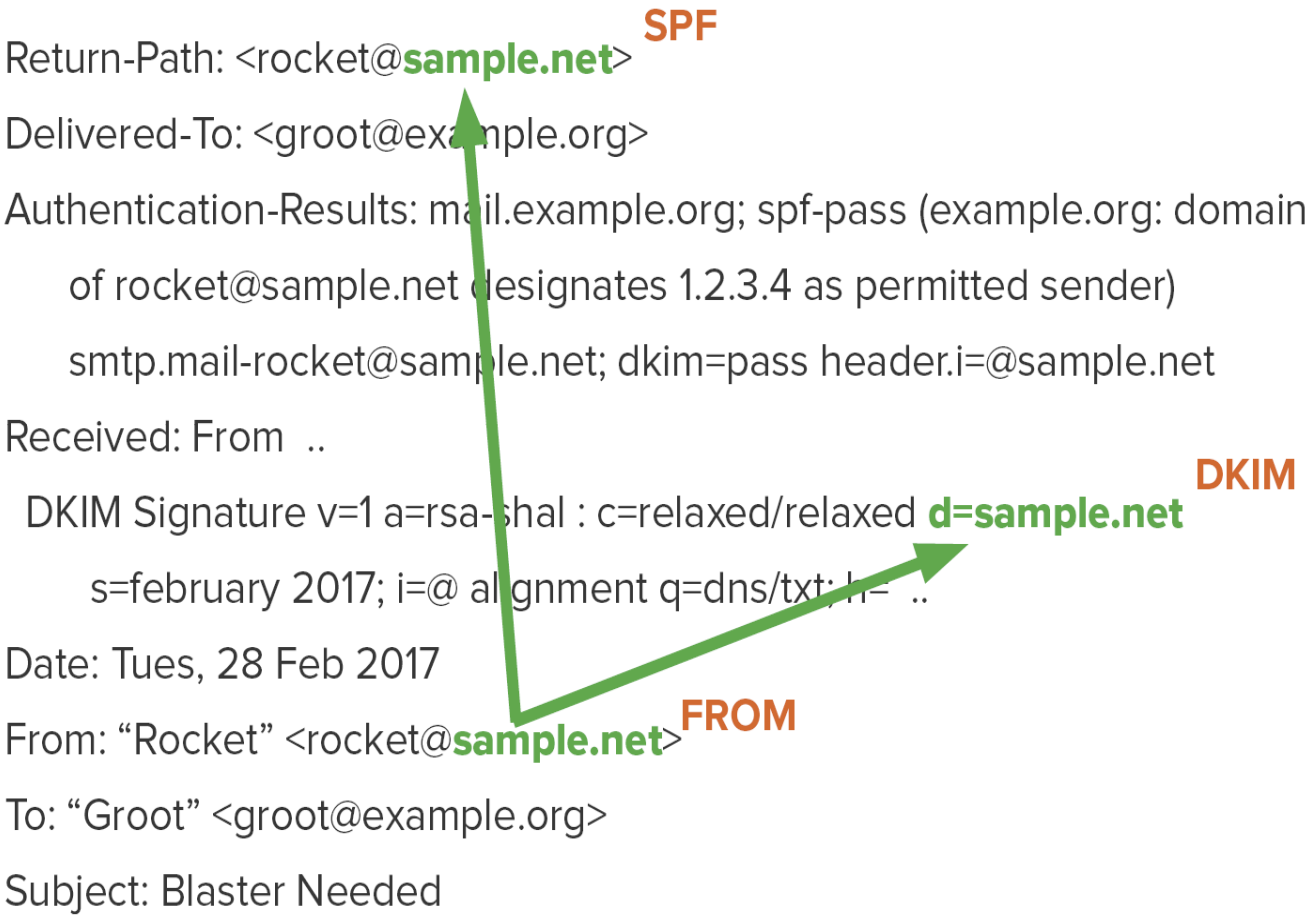
- **Kā apstrādāt *From*: lauku?**
  - user**@domain.lol**
- **Telemetrija**
  - **Statistiski ziņojumi**
  - **Incidentu ziņojumi - detalizēti**

DMARC

- **Darbības ar kļūdainiem(*not aligned*) epastiem (*policy*)**
  - ***None***
    - **monitorēšana**
  - ***Quarantine***
    - **Atkarīga no saņēmēja konfigurācijas**
  - ***Reject***

DMARC

- **DMARC = SPF + DKIM + from: alignment**
- **DMARC pārbauda 5322.From atbilstību (*alignment) ar* 5321.MailFrom un DKIM ierakstu**



DMARC darbībā

```
<record>
  <row>
    <source_ip>81.198.[redacted]1</source_ip>
    <count>9</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>fail</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>[redacted]cert.lv</header_from>
  </identifiers>
  <auth_results>
    <spf>
      <domain>[redacted].lv</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
```

Postmark

Weekly DMARC Digest

domain-test123.com

Nov 05 – Nov 12

10	10%	90%
Emails processed	SPF or DKIM aligned	SPF and DKIM not aligned

Your sources

These are sources that we know belong to you based on the DNS checks we do.

domain-test123.com	TOTAL	SPF ALIGNED	DKIM ALIGNED
119.133.111.105	1	100%	0%

⚠ Set up a DKIM record to get DMARC alignment on domain-test123.com.

Other sources

versanetonline.de	TOTAL	SPF ALIGNED	DKIM ALIGNED
84.19.199.201	4	0%	0%

Not Resolved	TOTAL	SPF ALIGNED	DKIM ALIGNED
106.12.211.206	1	0%	0%
115.211.221.230	1	0%	0%

Alignment

- ***Atbilstība***
- ***From:* lauks**
  - user**@domain.lol**
- **Atbilstība(*alignment*)**
  - **aspf un adkim - r|s**
  - **s - strict**
  - **r – relaxed**
    - **atļauti apakšdomēni (foo.edu.lv un bar.foo.edu.lv)**

SPF

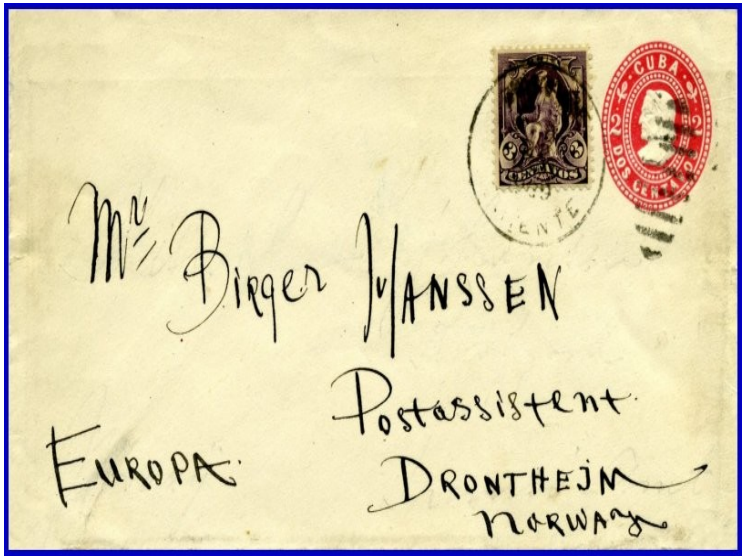
- **Sender Policy Framework**
  - **RFC 7208 2014**
- **Izsūtītāja IP adrese ir deklarēta attiecīgā domēna (SMTP mail from: lauka) DNS ierakstā**

SPF

- **dig txt cert.lv**
  cert.lv. 300 IN TXT "v=spf1 mx ip4:92.240.66.0/24 [……] ip4:145.0.2.40 ip4:38.111.193.7 -all"
- **dig txt bank.lv**
- bank.lv. 3106 IN TXT "v=spf1 include:spf.bank.lv -all"
- **dig txt spf.bank.lv**
- spf.bank.lv. 3094 IN TXT "v=spf1 mx ip4:94.100.11.107 ip4:191.237.221.25 ip4:80.233.167.9 ip4:80.233.167.5 ip4:172.30.0.0/16 ip4:194.153.79.0/24 ip4:91.194.176.0/24 ip4:172.31.223.0/24 ip4:194.14.205.140 include:spf.protection.outlook.com -all"

DKIM

- RFC 4870 2007.
- Epasts kriptogrāfiski parakstīts
  - Paraksta serveris izsūtot
    - Izsūtošās pasta nodaļas zīmogs
  - Parakstītajos datos jābūt iekļautam *From:* laukam
- DKIM-Signature mail header norāda kur DNS ir publiskā atslēga
  - d= (domain) un s= (selector)
- Korekti parakstīts epasts:
  - sūtītājs = domēna īpašnieks
  - *from* lauks nav mainīts



DKIM (2)

- Vienam epastam var būt vairākai DKIM paraksti
  - vismaz vienam jābūt derīgam
- Derīgs paraksts
  - DKIM d lauks atbilst (*aligns*) *from* laukam
  - Parakstīts ar atbilstošo privāto atslēgu
- DKIM ieraksts
  - o - outbound signing policy
    - "o=-"visi epasti no šī domēna ir parakstīti
    - "o=~" daļa epastu no sī domēna ir parakstīti
  - r - reporting email address
  - t - testing mode
    - y|n

DKIM praksē

`dig _domainkey.[domēns] txt`

Lai pilnībā pārbaudītu DKIM, nepieciešams epasts no domēna, kurā norādīta atslēgas atrašanās vieta (*selector*)

ergvsk.lv ,"v=DKIM1\; o=~"

suntazuvsk.lv ,"v=DKIM1\; o=~"

vecsaulespsk.lv ,"v=DKIM1\; o=~"

stakuskola.lv ,"v=DKIM1\; o=~"

neretasskola.lv ,"v=DKIM1\; o=~"

t2psk.lv ,"v=DKIM1\; o=~"

kraslavaspsk.lv ,"v=DKIM1\; o=~"

j6vsk.lv ,"v=DKIM1\; o=~"

herderagrizinkalnavsk.lv ,"v=DKIM1\; o=~"

incukalnamms.lv ,"v=DKIM1\; o=~"

incukalnapsk.lv ,"v=DKIM1\; o=~"

blidenesskola.lv ,"v=DKIM1\; o=~"

deksaruskola.lv ,"v=DKIM1\; o=~"

DMARC lietderība

From Me <ivo@[redacted]
Subject [redacted] been hacked! Change your password immediately!
To Me <ivo@[redacted]

Hello!

I have very bad news for you.
03/08/2018 - on this day I hacked your OS and got full access to your account ivo@[redacted]
On this day your account ivo@[redacted] has password: [redacted]

So, you can change the password, yes.. But my malware intercepts it every time.

How I made it:
In the software of the router, through which you went online, was a vulnerability.
I just hacked this router and placed my malicious code on it.
When you went online, my trojan was installed on the OS of your device.

After that, I made a full dump of your disk (I have all your address book, history of viewing sites, al

A month ago, I wanted to lock your device and ask for a not big amount of btc to unlock.
But I looked at the sites that you regularly visit, and I was shocked by what I saw!!!
I'm talk you about sites for adults.

I want to say - you are a BIG pervert. Your fantasy is shifted far away from the normal course!

And I got an idea....
I made a screenshot of the adult sites where you have fun (do you understand what it is about, huh?).
After that, I made a screenshot of your joys (using the camera of your device) and glued them together.

Scaremailing

- **Noplūdušo paroļu datubāzu monetizācija (cits resurss, epasts + parole)**
- **viltota *from*: adrese - lietotāja epasts**
- **Saturs**
  - **noplūdusī parole**
    - **paroļu atkalizmantošana, nemainīšana**
  - **fiktīvs izspiešanas teksts**

Kas tālāk?

- **Konfidencialitāte, integritāte**
  - **STARTTLS - oportūnistiska šifrēšana**
    - **StripTLS**
      - **aktīvs MitM**
  - **DANE - STARTTLS atbalstu paziņo caur DNS**
  - **DNSSEC - kriptogrāfiski aizsargāts DNS ieraksti**
  - **SMTP MTA Strict Transport Security(MTA-STS)**
    - **trust on first use**

DMARC piemēri

- **_dmarc.example.com**
- **v=DMARC1;p=none;sp=quarantine;pct=100;rua=mailto:dmarcreports@example.com;**
- **p=policy**
- **sp=subdomain policy**
- **pct=uz kādu daļu slikto epastu attiecināt politiku**
- **rua=statistisko ziņojumu epasts**
- **ruf=detalizēto incidentu ziņojumu epasts (*forensics*)**
- **apakšdomēnam var būt individuāla politika,**
  - **hierarhiska kāpšanās atpakaļ**
- **kļūdu epastus var apstrādāt cits domēns; jādeklarē lai nebūtu spam amplification**
  - **sender.example._report._dmarc.thirdparty.example IN TXT "v=DMARC1;"**

DMARC piemēri

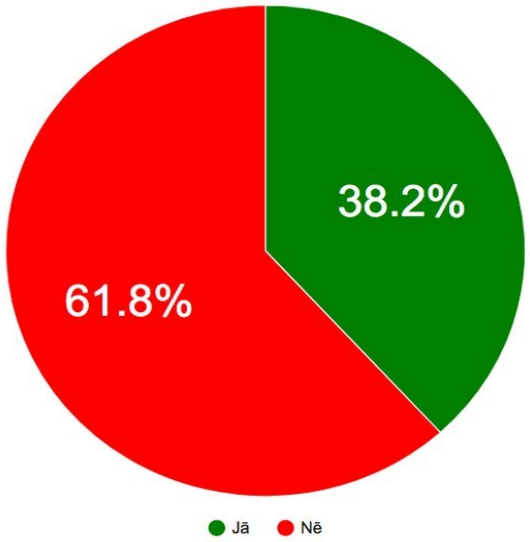
- **dig txt _dmarc.cert.gov.lv**
  _dmarc.cert.gov.lv. 1800 IN TXT"v=DMARC1; p=none; pct=100; rua=mailto:dmarc@cert.lv; ruf=mailto:dmarc@cert.lv; sp=none; aspf=r;"
- **dig cert.gov.lv._report._dmarc.cert.lv txt**
  - ;cert.gov.lv._report._dmarc.cert.lv. IN TXT

Problēmas

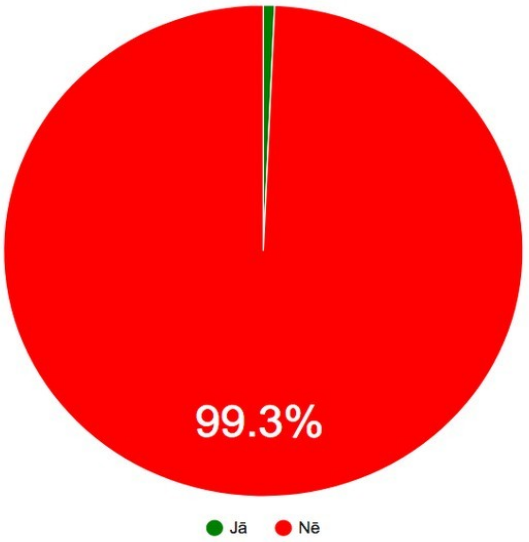
- **Forwarding**
  - **DKIM OK**
  - **SPF salūzt (fw IP nav oriģinālā from: epasta servera IP)**
- **Mailing lists**
  - **from: izmaiņas**
    - **From: John Doe <user@example.com.INVALID>**
    - **From: John Doe <243576@mailinglist.example.org>**
    - **From: John Doe via MailingList <list@mailinglist.example.org>**
      Reply-To: John Doe <user@example.com>
- **3. puses izmantošana spam kampaņai**
- **Epasta avotu apzināšana**
  - **Monitorings**
  - **Reti notikumi**
    - **Github**

Stats *.gov.lv

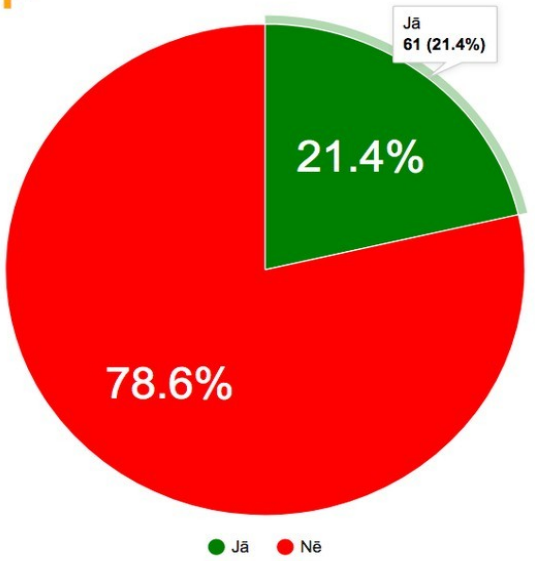
STARTTLS



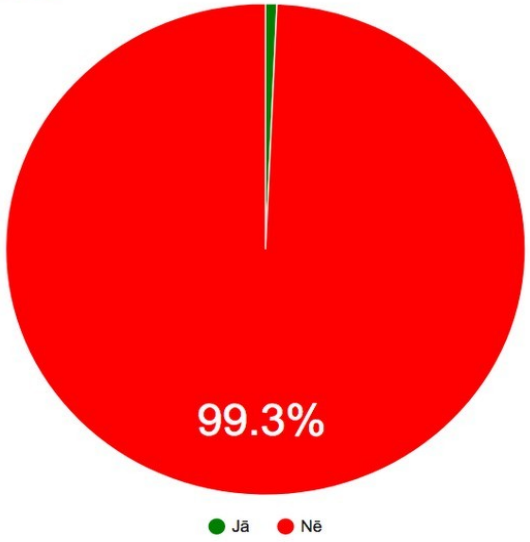
DMARC



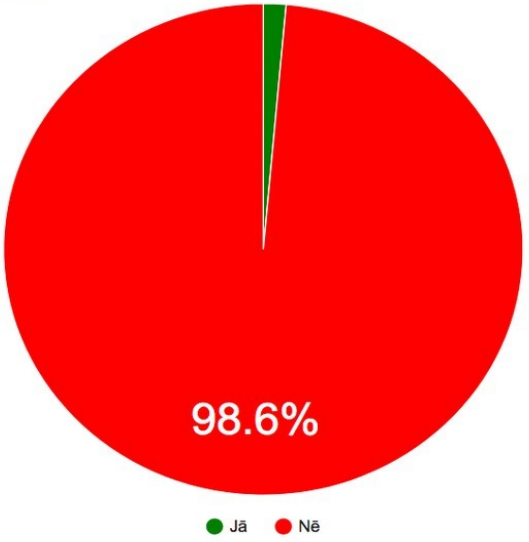
SPF



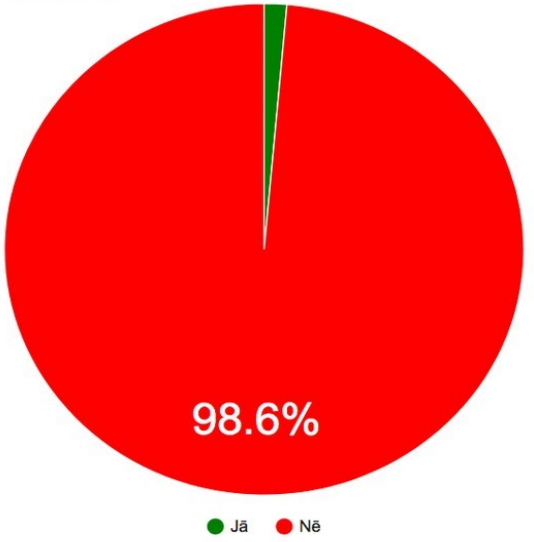
DKIM



CAA

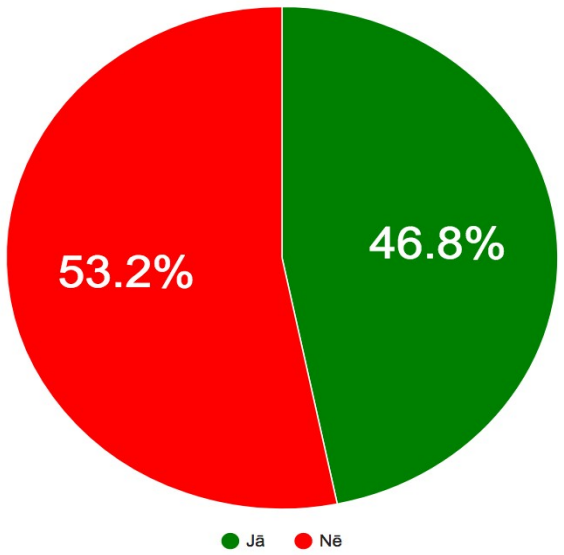


DNSSEC

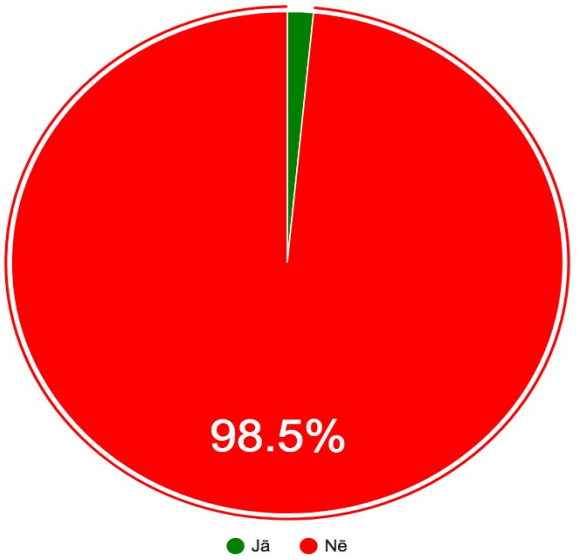


Publiskais sektors

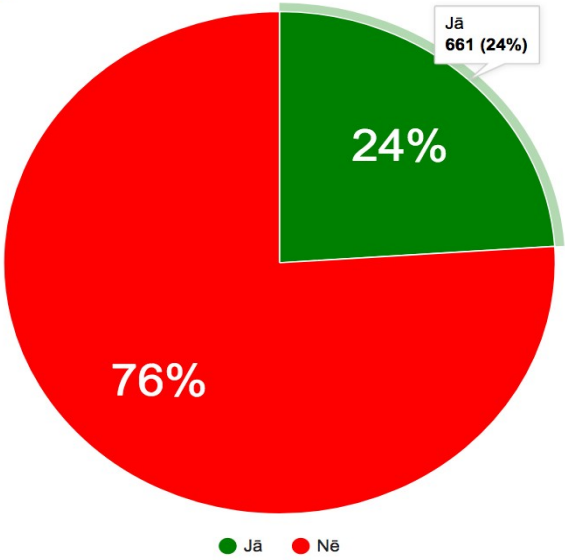
STARTTLS



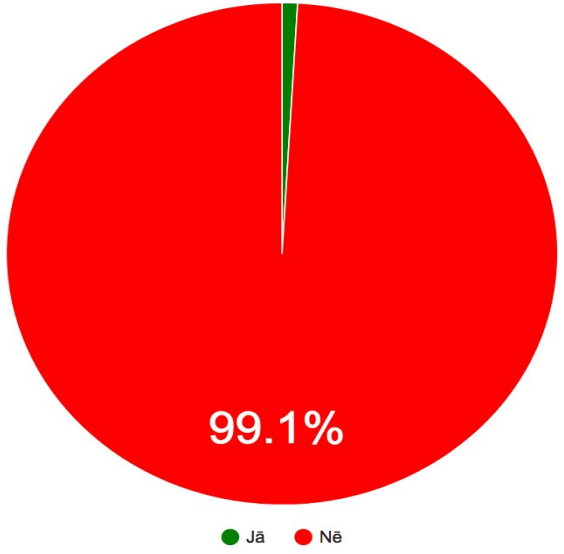
DMARC



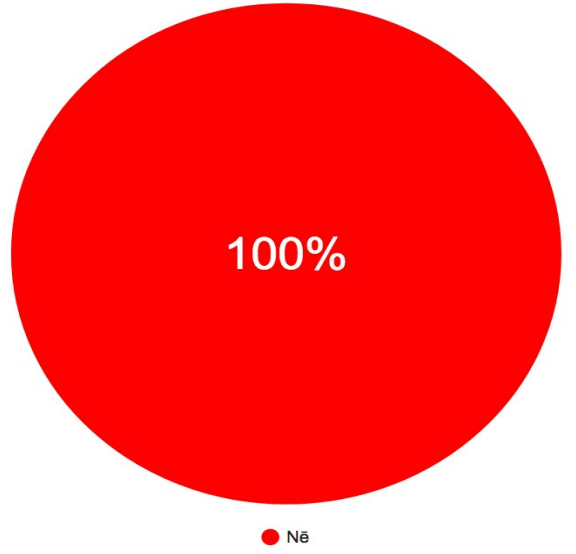
SPF



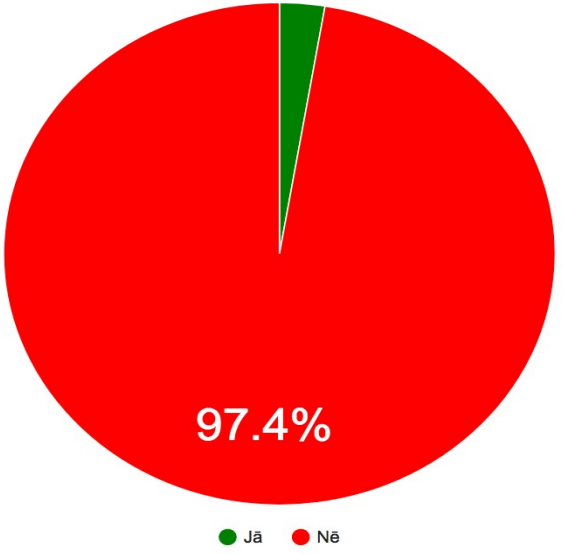
DKIM



CAA



DNSSEC



Publiskais sektors

daug12vsk.lv ,"v=DMARC1\; p=none\;"

dnd.lv ,"v=DMARC1\; p=none"

kandavastehnikums.lv ,"v=DMARC1\; p=none"

tuk3psk.lv ,"v=DMARC1\; p=none\; sp=quarantine\; rua=mailto:mailauth-reports@clientele.tech"

ruvs.lv ,"v=DMARC1\; p=none"

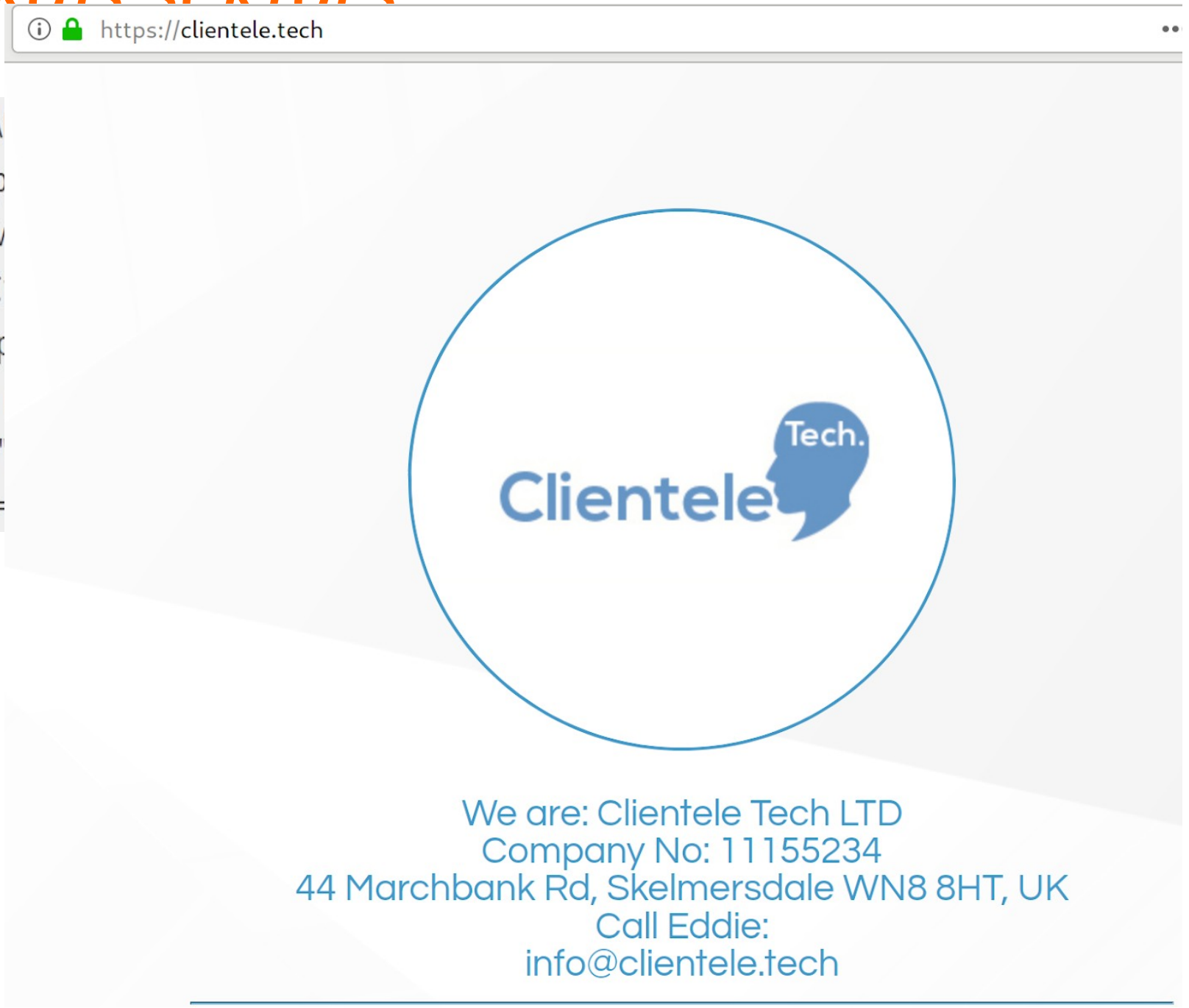
bank.lv ,"v=DMARC1\; p=reject\; rua=mailto:dmarcreport@bank.lv\; ruf=mailto:dmarcfail@bank.lv\;fo=1"

ogressportacentrs.lv ,"v=DMARC1\; p=none"

rtu.lv ,"v=DMARC1\; p=none"

Publiskais sektors

daug12vsk.lv ,"v=DMA
dnd.lv ,"v=DMARC1\; p
kandavastehnikums.lv
tuk3psk.lv ,"v=DMARC
ruvs.lv ,"v=DMARC1\; p
bank.lv ,"v=DMARC1\;
ogressportacentrs.lv ,"
rtu.lv ,"v=DMARC1\; p=



Noderīgas saites

https://hardenize.com
https://dmarc.org
https://dmarcian.com/dmarc-inspector/
https://dnsviz.net
https://ssl-tools.net/tlsa-generator
https://sslmate.com/caa/


Paldies!