Protecting Global Email. Status & The Road Ahead.

Per Thorsheim
@thorsheim

GodPraksis

```
ngrep –i password tcp port 25
```

Short Timeline Of Events

(Very short!)

January 1999: RFC 2487
SMTP Service Extension for
Secure SMTP over TLS

February 2002: RFC 3207
SMTP Service Extension for Secure
SMTP over Transport Layer Security

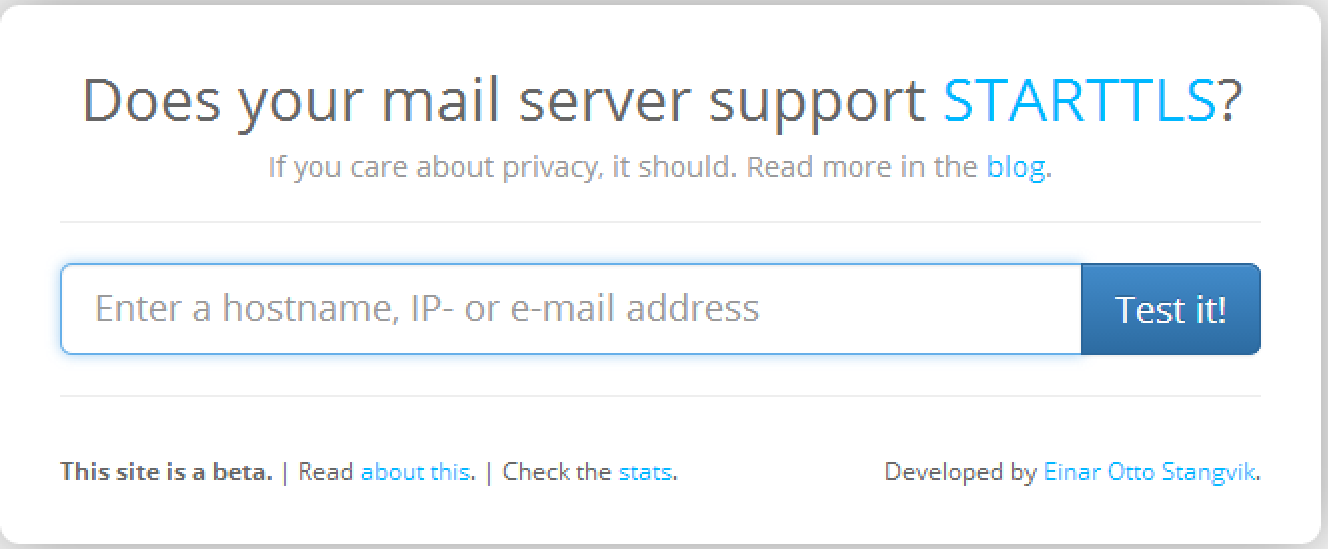
Mail server exchange

```
S: <waits for connection on TCP port 25>
C: <opens connection>
S: 220 mail.example.org SMTP service ready
C: EHLO mail.example.com
S: 250-mail.example.org Hi there. No spam, plz.
S: 250 STARTTLS
C: STARTTLS
S: 220 Go ahead
C: <starts TLS negotiation>
C & S: <negotiate a TLS session>
C & S: <transmit data>
```

Mailheader received

Received: from mail.example.com ([172.16.16.16]) by mail.isp.com with **ESMTP/TLS/DHE-RSA-AES256-SHA**; 10 Jul 2015 16:45:35 +0200

https://starttls.info/



Does your mail server support STARTTLS?

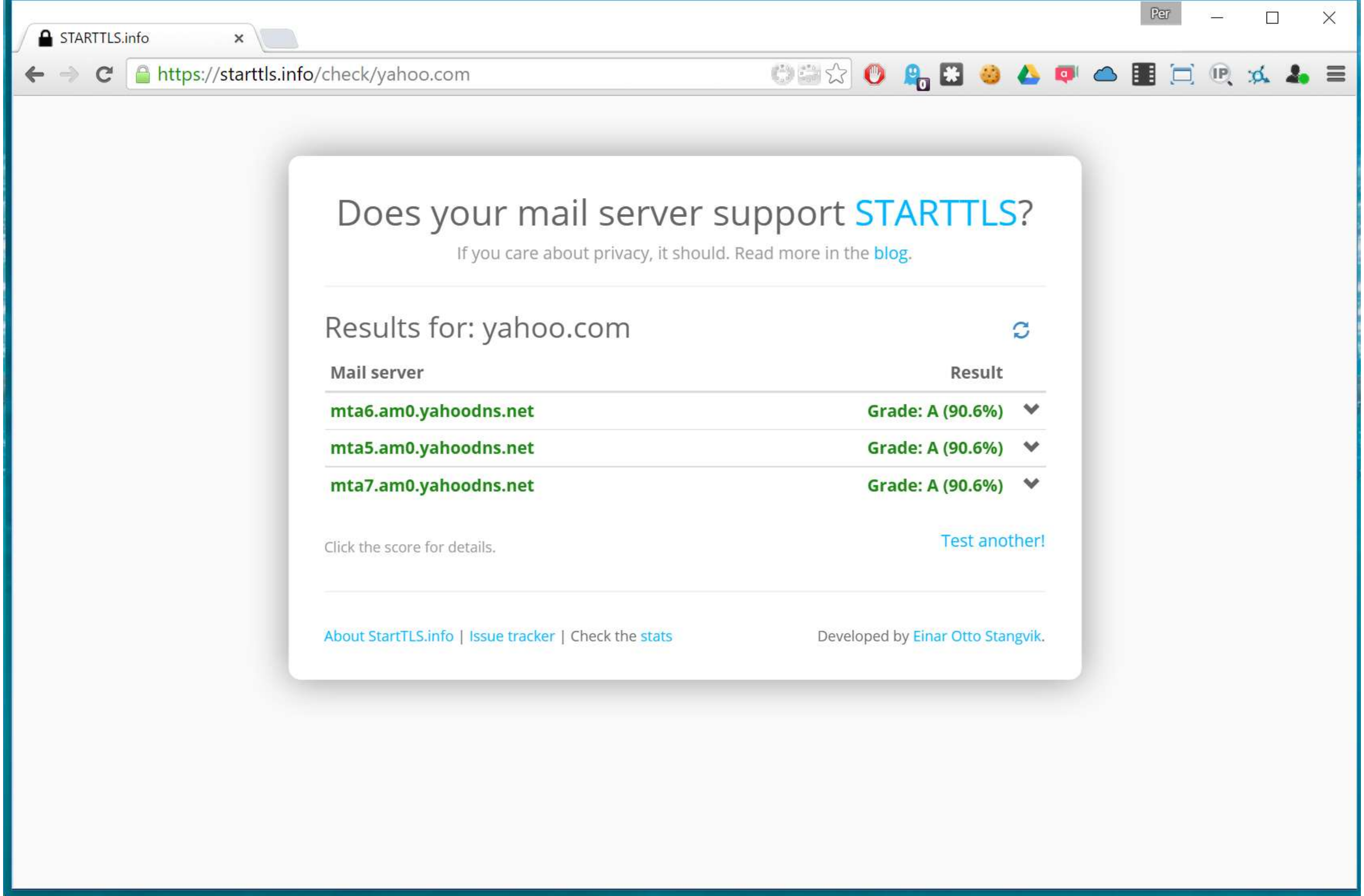
If you care about privacy, it should. Read more in the blog.

This site is a beta. | Read about this. | Check the stats.

Developed by Einar Otto Stangvik.

Made by @einaros!

Tweet him a «thank you!»



Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: yahoo.com

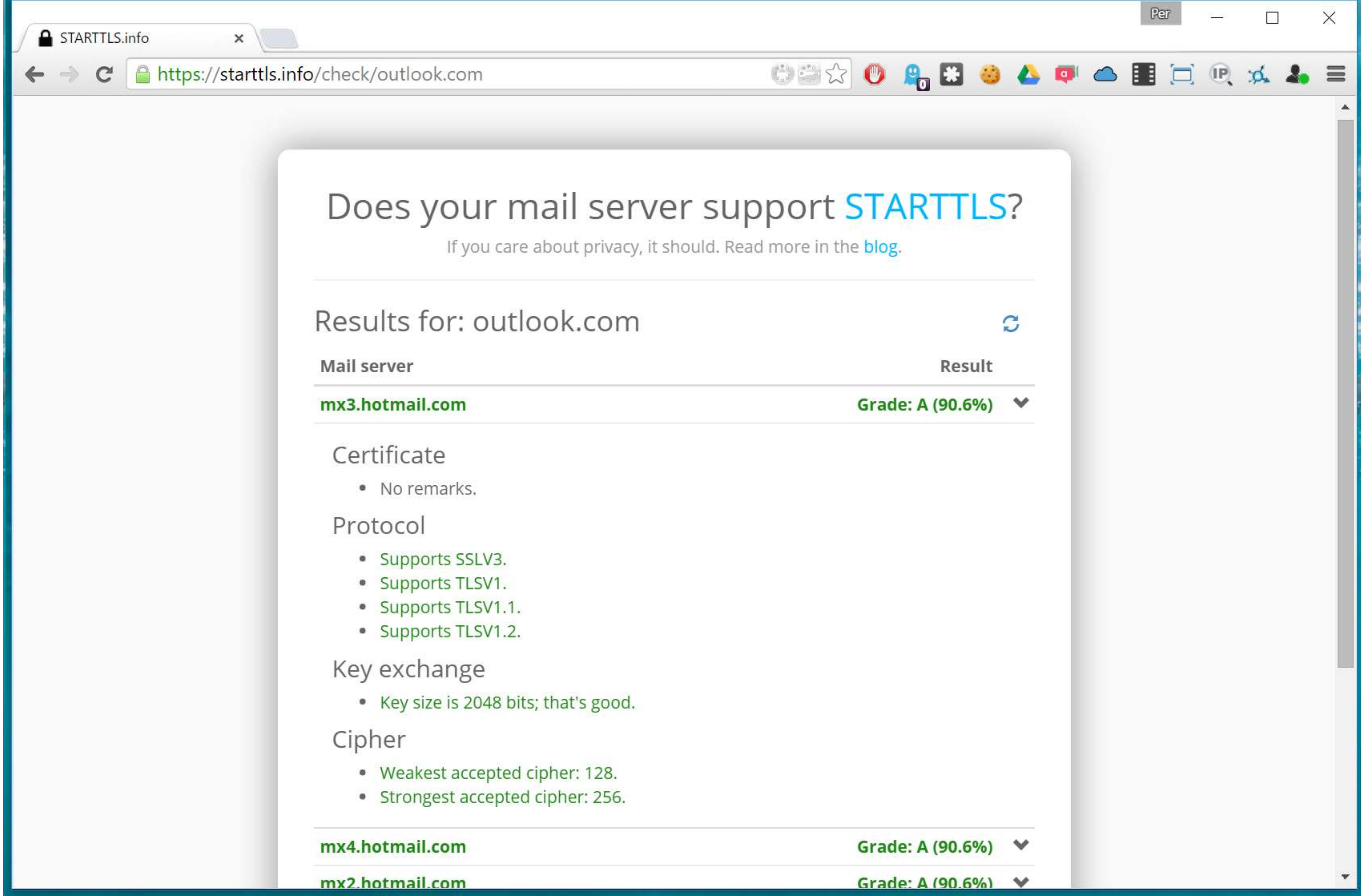
Mail server	Result
mta6.am0.yahoodns.net	Grade: A (90.6%)
mta5.am0.yahoodns.net	Grade: A (90.6%)
mta7.am0.yahoodns.net	Grade: A (90.6%)

Click the score for details.

Test another!

About StartTLS.info | Issue tracker | Check the stats

Developed by Einar Otto Stangvik.



Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: outlook.com

Mail server	Result
mx3.hotmail.com	Grade: A (90.6%)

Certificate

- No remarks.

Protocol

- Supports SSLV3.
- Supports TLSV1.
- Supports TLSV1.1.
- Supports TLSV1.2.

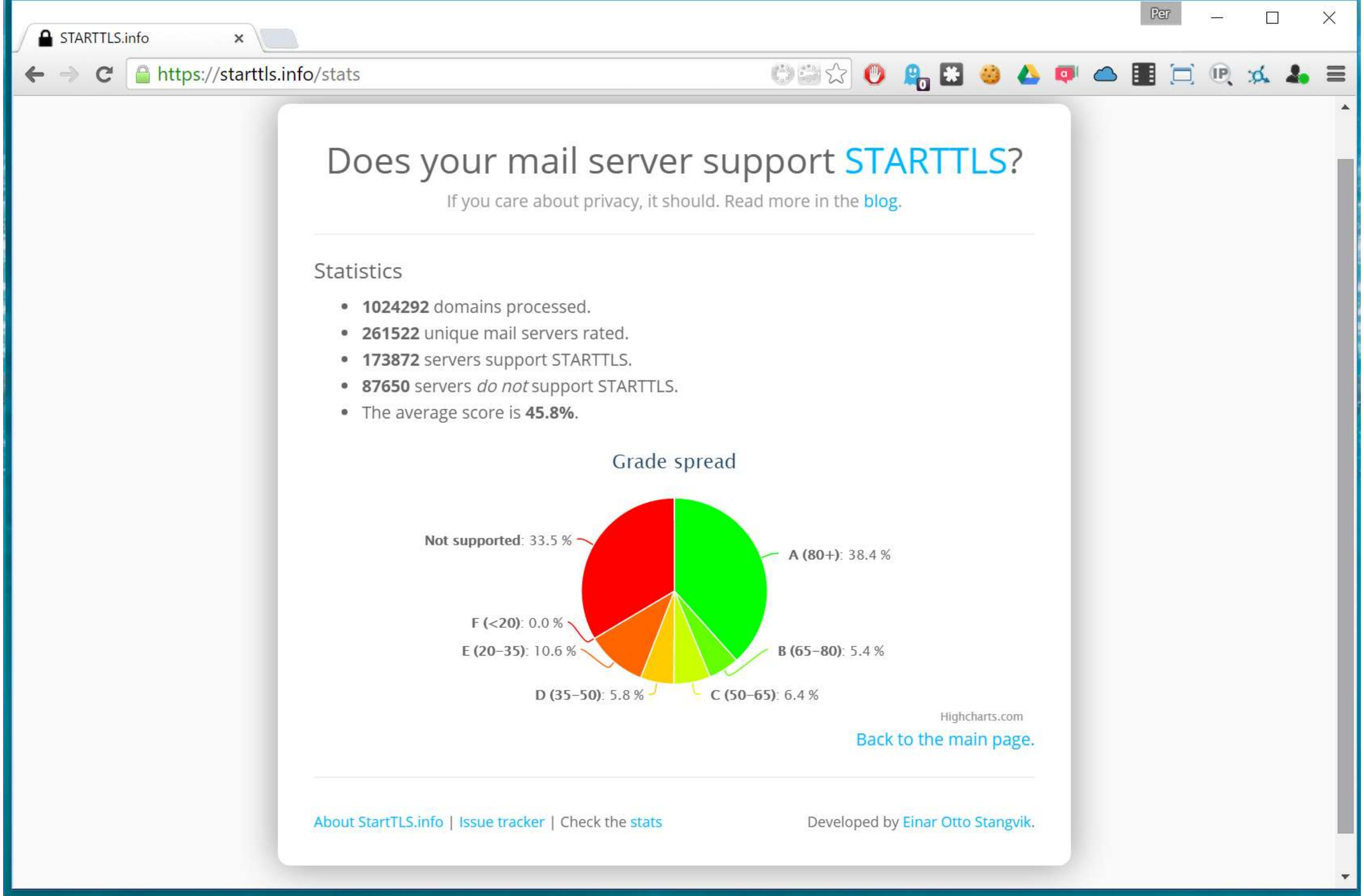
Key exchange

- Key size is 2048 bits; that's good.

Cipher

- Weakest accepted cipher: 128.
- Strongest accepted cipher: 256.

Mail server	Result
mx4.hotmail.com	Grade: A (90.6%)
mx2.hotmail.com	Grade: A (90.6%)



Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Statistics

- **1024292** domains processed.
- **261522** unique mail servers rated.
- **173872** servers support STARTTLS.
- **87650** servers *do not* support STARTTLS.
- The average score is **45.8%**.

Grade spread

Back to the main page.

About StartTLS.info | Issue tracker | Check the stats

Developed by Einar Otto Stangvik.

Nasjonal sikkerhetsmyndighet

IT-veiledning for ugradert nr 2 (U-02)
Oppdatert: 2014-02-03

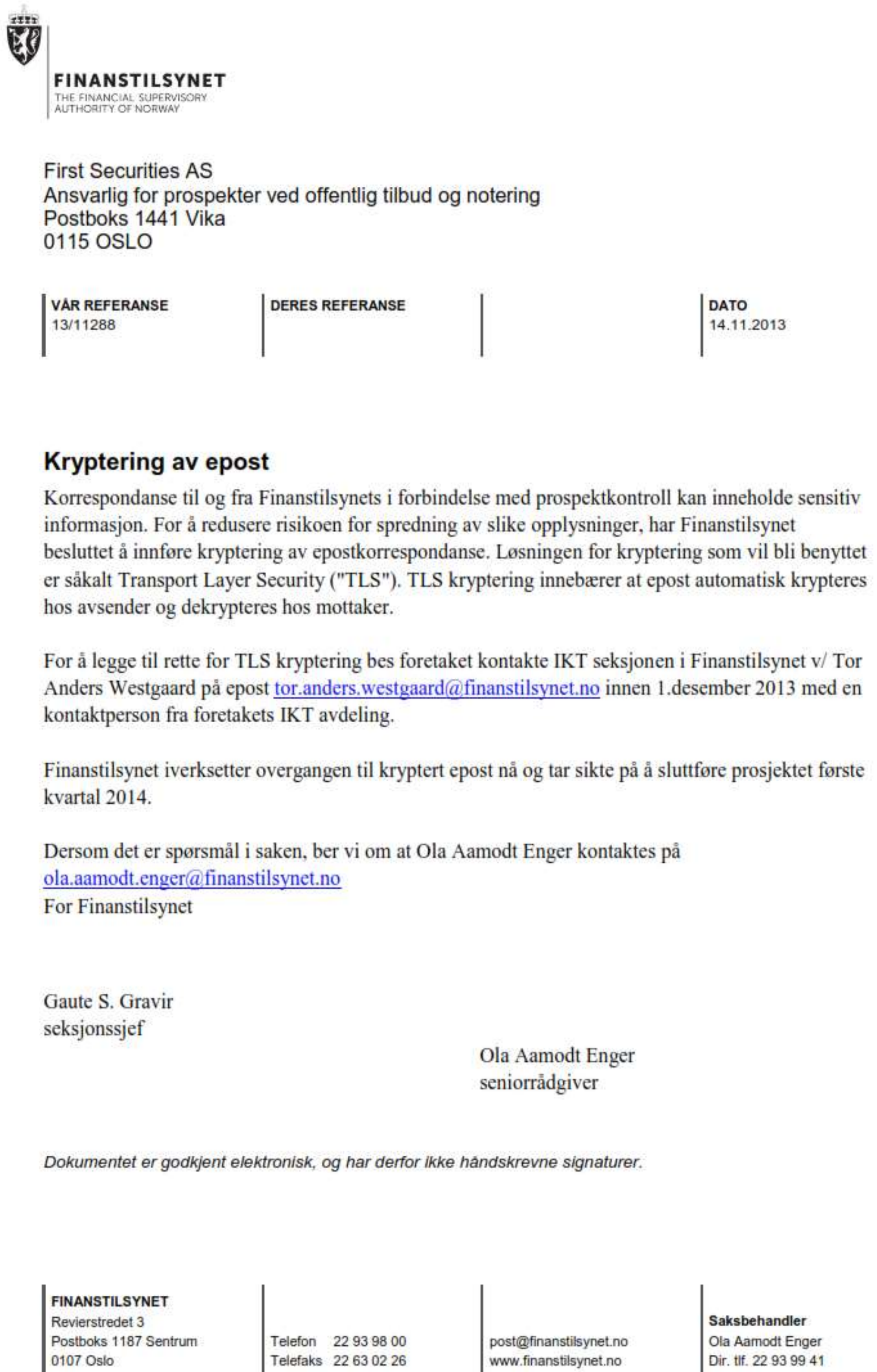
NSM

E-post

Kryptering av e-postoverføring

Beskrivelse av grunnleggende tiltak for sikring av overføring av e-post mellom e-posttjenere

Dette dokumentet er NSMs anbefaling for grunnleggende sikring av overføring av e-post mellom e-posttjenere. Målgruppen er personell som utvikler og forvalter ugraderte systemer i offentlig forvaltning. Dokumentet er ikke ment brukt ifm formell sikkerhetsgodkjenning av graderte systemer.



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

First Securities AS
Ansvarlig for prospekter ved offentlig tilbud og notering
Postboks 1441 Vika
0115 OSLO

VÅR REFERANSE	DERES REFERANSE		DATO
13/11288			14.11.2013

Kryptering av epost

Korrespondanse til og fra Finanstilsynets i forbindelse med prospektkontroll kan inneholde sensitiv informasjon. For å redusere risikoen for spredning av slike opplysninger, har Finanstilsynet besluttet å innføre kryptering av epostkorrespondanse. Løsningen for kryptering som vil bli benyttet er såkalt Transport Layer Security ("TLS"). TLS kryptering innebærer at epost automatisk krypteres hos avsender og dekrypteres hos mottaker.

For å legge til rette for TLS kryptering bes foretaket kontakte IKT seksjonen i Finanstilsynet v/ Tor Anders Westgaard på epost tor.anders.westgaard@finanstilsynet.no innen 1.desember 2013 med en kontaktperson fra foretakets IKT avdeling.

Finanstilsynet iverksetter overgangen til kryptert epost nå og tar sikte på å sluttføre prosjektet første kvartal 2014.

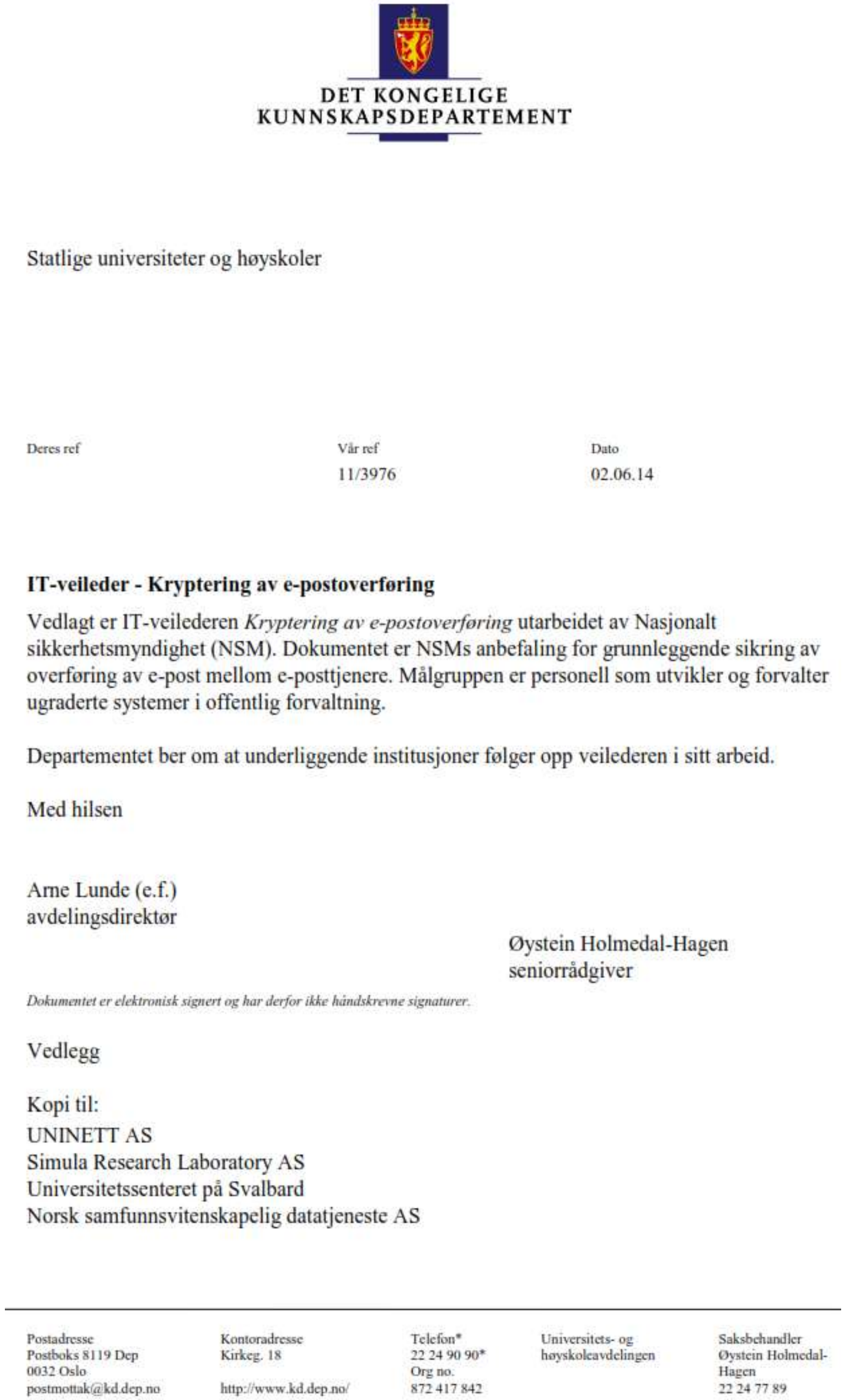
Dersom det er spørsmål i saken, ber vi om at Ola Aamodt Enger kontaktes på ola.aamodt.enger@finanstilsynet.no
For Finanstilsynet

Gaute S. Gravir
seksjonssjef

Ola Aamodt Enger
seniorrådgiver

Dokumentet er godkjent elektronisk, og har derfor ikke håndskrevne signaturer.

FINANSTILSYNET Revierstredet 3 Postboks 1187 Sentrum 0107 Oslo	Telefon 22 93 98 00 Telefaks 22 63 02 26	post@finanstilsynet.no www.finanstilsynet.no	Saksbehandler Ola Aamodt Enger Dir. tlf. 22 93 99 41



DET KONGELIGE
KUNNSKAPSDEPARTEMENT

Statlige universiteter og høyskoler

Deres ref	Vår ref	Dato
	11/3976	02.06.14

IT-veileder - Kryptering av e-postoverføring

Vedlagt er IT-veilederen *Kryptering av e-postoverføring* utarbeidet av Nasjonalt sikkerhetsmyndighet (NSM). Dokumentet er NSMs anbefaling for grunnleggende sikring av overføring av e-post mellom e-posttjenere. Målgruppen er personell som utvikler og forvalter ugraderte systemer i offentlig forvaltning.

Departementet ber om at underliggende institusjoner følger opp veilederen i sitt arbeid.

Med hilsen

Arne Lunde (e.f.)
avdelingsdirektør

Øystein Holmedal-Hagen
seniorrådgiver

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer.

Vedlegg

Kopi til:
UNINETT AS
Simula Research Laboratory AS
Universitetssenteret på Svalbard
Norsk samfunnsvitenskapelig datatjeneste AS

Postadresse Postboks 8119 Dep 0032 Oslo postmottak@kd.dep.no	Kontoradresse Kirkeg. 18 http://www.kd.dep.no/	Telefon* 22 24 90 90* Org no. 872 417 842	Universitets- og høyskoleavdelingen	Saksbehandler Øystein Holmedal-Hagen 22 24 77 89

Google Transparency Report

http://www.google.com/transparencyreport/saferemail/?hl=en

THANK YOU!

ACLU

AMERICAN CIVIL LIBERTIES UNION

@csoghoian

EFF

ELECTRONIC FRONTIER FOUNDATION

DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

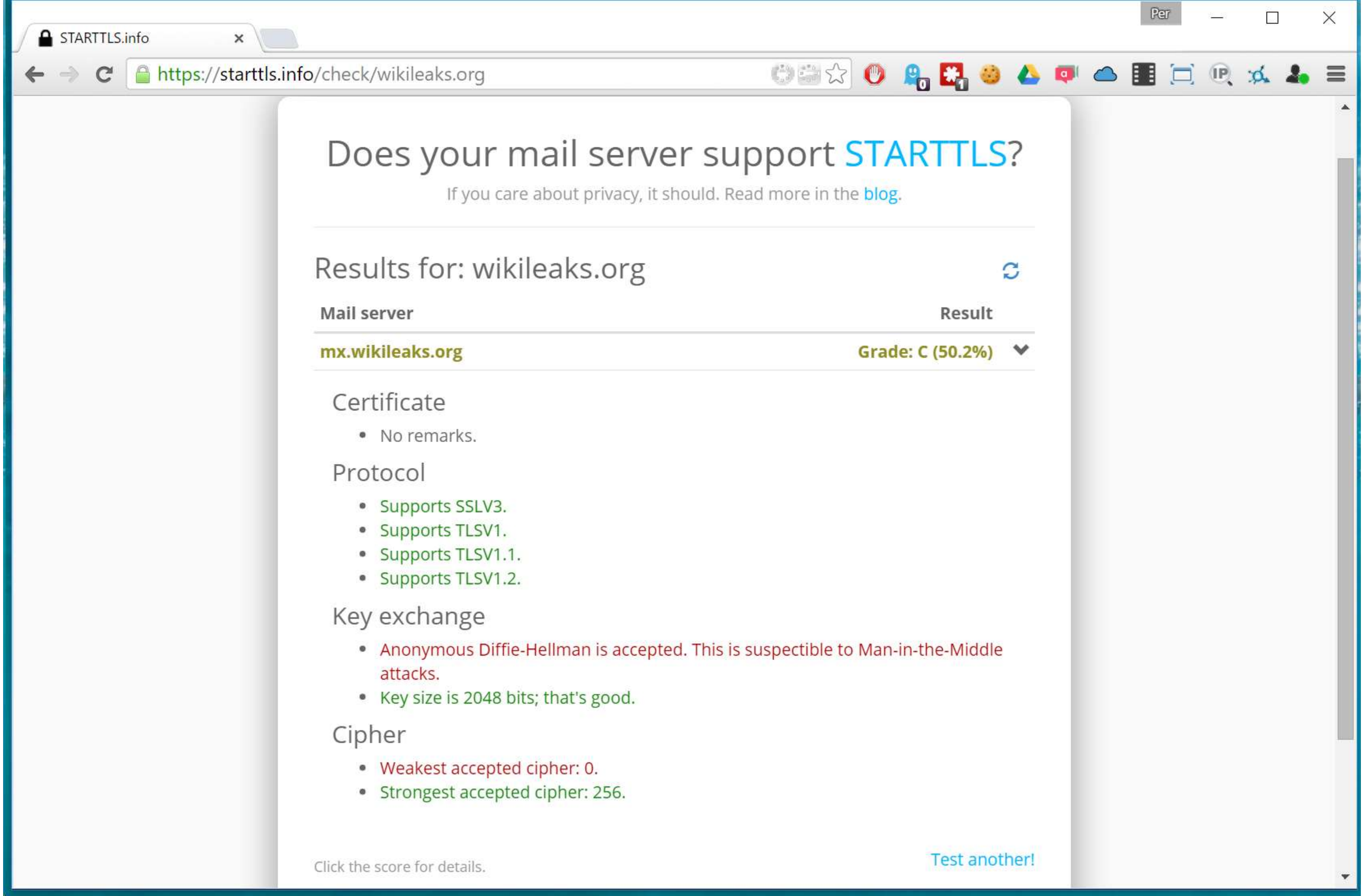
@j4cob

facebook®

Google

Challenges with RFC 3207

Short version: Opportunistic encryption. Use if available.



Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: wikileaks.org

Mail server	Result
mx.wikileaks.org	Grade: C (50.2%)

Certificate

- No remarks.

Protocol

- Supports SSLV3.
- Supports TLSV1.
- Supports TLSV1.1.
- Supports TLSV1.2.

Key exchange

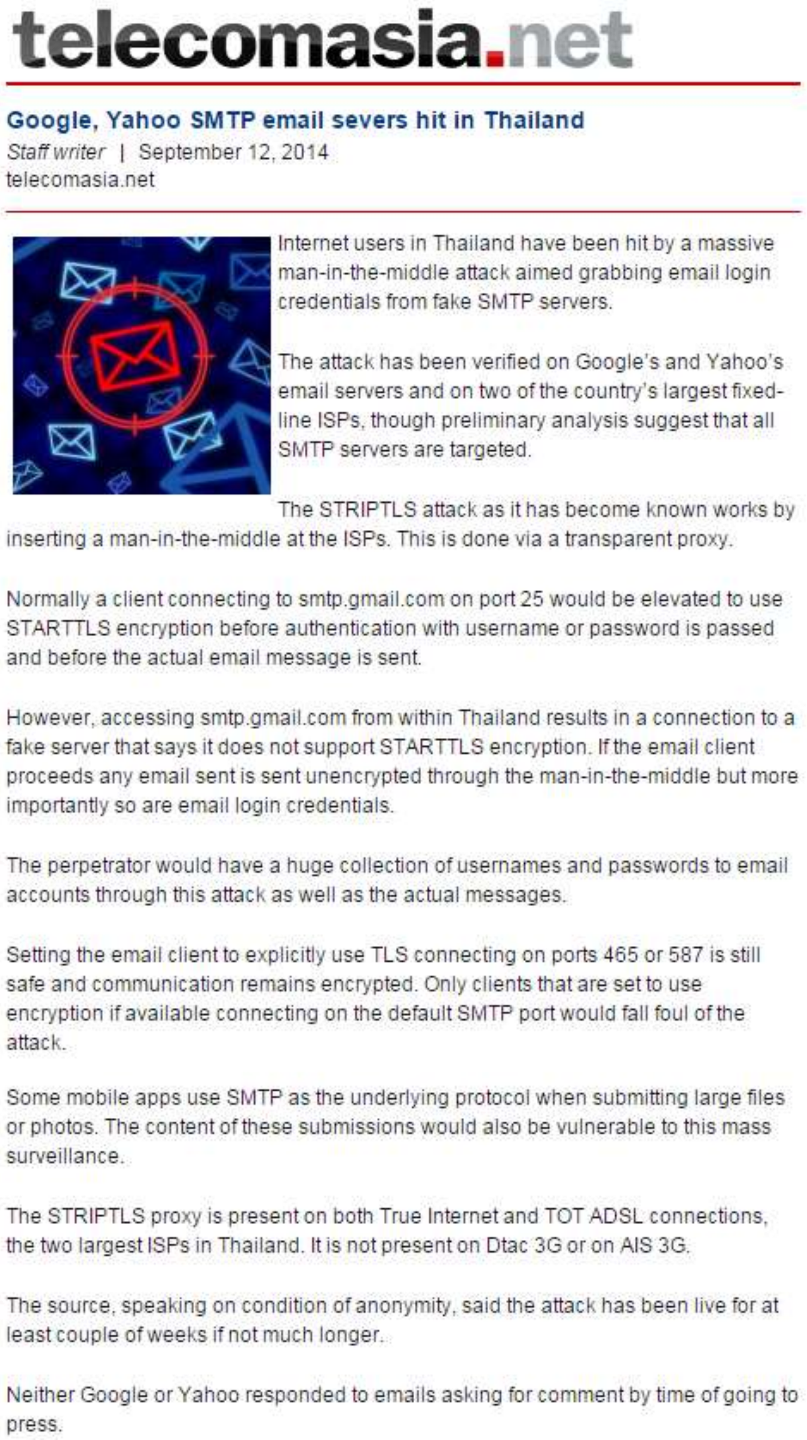
- Anonymous Diffie-Hellman is accepted. This is suspectible to Man-in-the-Middle attacks.
- Key size is 2048 bits; that's good.

Cipher

- Weakest accepted cipher: 0.
- Strongest accepted cipher: 256.

Click the score for details.

Test another!



telecomasia.net

Google, Yahoo SMTP email severs hit in Thailand

Staff writer | September 12, 2014
telecomasia.net

Internet users in Thailand have been hit by a massive man-in-the-middle attack aimed grabbing email login credentials from fake SMTP servers.

The attack has been verified on Google's and Yahoo's email servers and on two of the country's largest fixed-line ISPs, though preliminary analysis suggest that all SMTP servers are targeted.

The STRIPTLS attack as it has become known works by inserting a man-in-the-middle at the ISPs. This is done via a transparent proxy.

Normally a client connecting to smtp.gmail.com on port 25 would be elevated to use STARTTLS encryption before authentication with username or password is passed and before the actual email message is sent.

However, accessing smtp.gmail.com from within Thailand results in a connection to a fake server that says it does not support STARTTLS encryption. If the email client proceeds any email sent is sent unencrypted through the man-in-the-middle but more importantly so are email login credentials.

The perpetrator would have a huge collection of usernames and passwords to email accounts through this attack as well as the actual messages.

Setting the email client to explicitly use TLS connecting on ports 465 or 587 is still safe and communication remains encrypted. Only clients that are set to use encryption if available connecting on the default SMTP port would fall foul of the attack.

Some mobile apps use SMTP as the underlying protocol when submitting large files or photos. The content of these submissions would also be vulnerable to this mass surveillance.

The STRIPTLS proxy is present on both True Internet and TOT ADSL connections, the two largest ISPs in Thailand. It is not present on Dtac 3G or on AIS 3G.

The source, speaking on condition of anonymity, said the attack has been live for at least couple of weeks if not much longer.

Neither Google or Yahoo responded to emails asking for comment by time of going to press.

In the second instance, Golden Frog shows that a wireless broadband Internet access provider is interfering with its users' ability to encrypt their SMTP email traffic. This broadband provider is overwriting the content of users' communications and actively blocking STARTTLS encryption. This is a man-in-the-middle attack that prevents customers from using the applications of their choosing and directly prevents users from protecting their privacy.

https://www.techdirt.com/blog/netneutrality/articles/20141012/06344928801/revealed-isps-already-violating-net-neutrality-to-block-encryption-make-everyone-less-safe-online.shtml

One step ahead: EFF – STARTTLS Everywhere

https://github.com/EFForg/starttls-everywhere

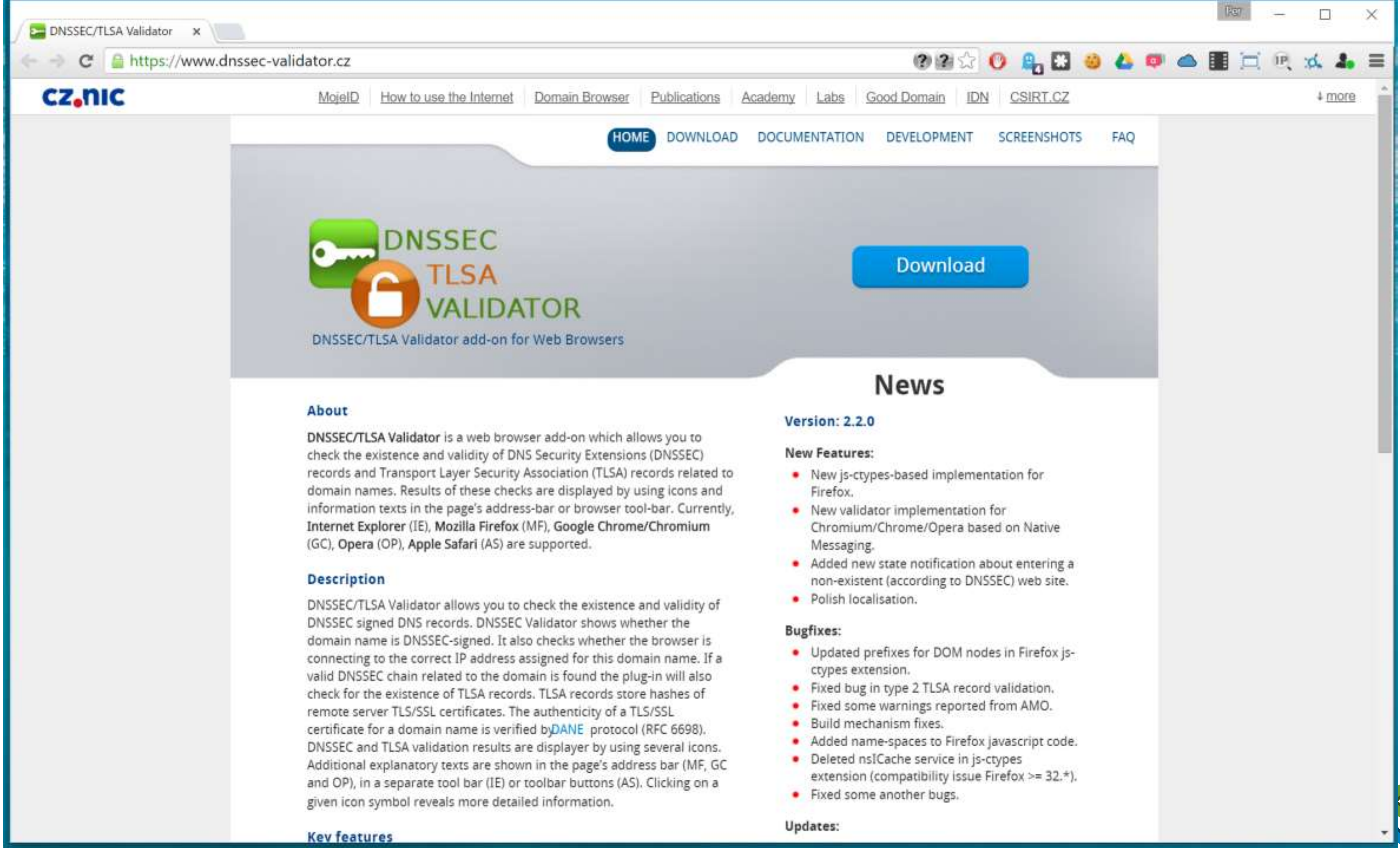
Central database with info on who supports STARTTLS, enabling a (somewhat) scalable enforced use of STARTTLS.

Other Challenges

- Secure IMAP *requires* RC4 support, to be RFC compliant
- POP / IMAP available «everywhere» unencrypted
- POP / IMAP can use STARTTLS or SSL/TLS

- Challenge:
  - Automate addition of pop/imap to the Mozilla list
  - Check all those servers for port & encryption support
  - Grade, name & shame?

So, what do we do now?



DNSSEC/TLSA Validator add-on for Web Browsers

News

About

DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNS Security Extensions (DNSSEC) records and Transport Layer Security Association (TLSA) records related to domain names. Results of these checks are displayed by using icons and information texts in the page's address-bar or browser tool-bar. Currently, **Internet Explorer** (IE), **Mozilla Firefox** (MF), **Google Chrome/Chromium** (GC), **Opera** (OP), **Apple Safari** (AS) are supported.

Description

DNSSEC/TLSA Validator allows you to check the existence and validity of DNSSEC signed DNS records. DNSSEC Validator shows whether the domain name is DNSSEC-signed. It also checks whether the browser is connecting to the correct IP address assigned for this domain name. If a valid DNSSEC chain related to the domain is found the plug-in will also check for the existence of TLSA records. TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified byDANE protocol (RFC 6698). DNSSEC and TLSA validation results are displayer by using several icons. Additional explanatory texts are shown in the page's address bar (MF, GC and OP), in a separate tool bar (IE) or toolbar buttons (AS). Clicking on a given icon symbol reveals more detailed information.

Key features

Version: 2.2.0

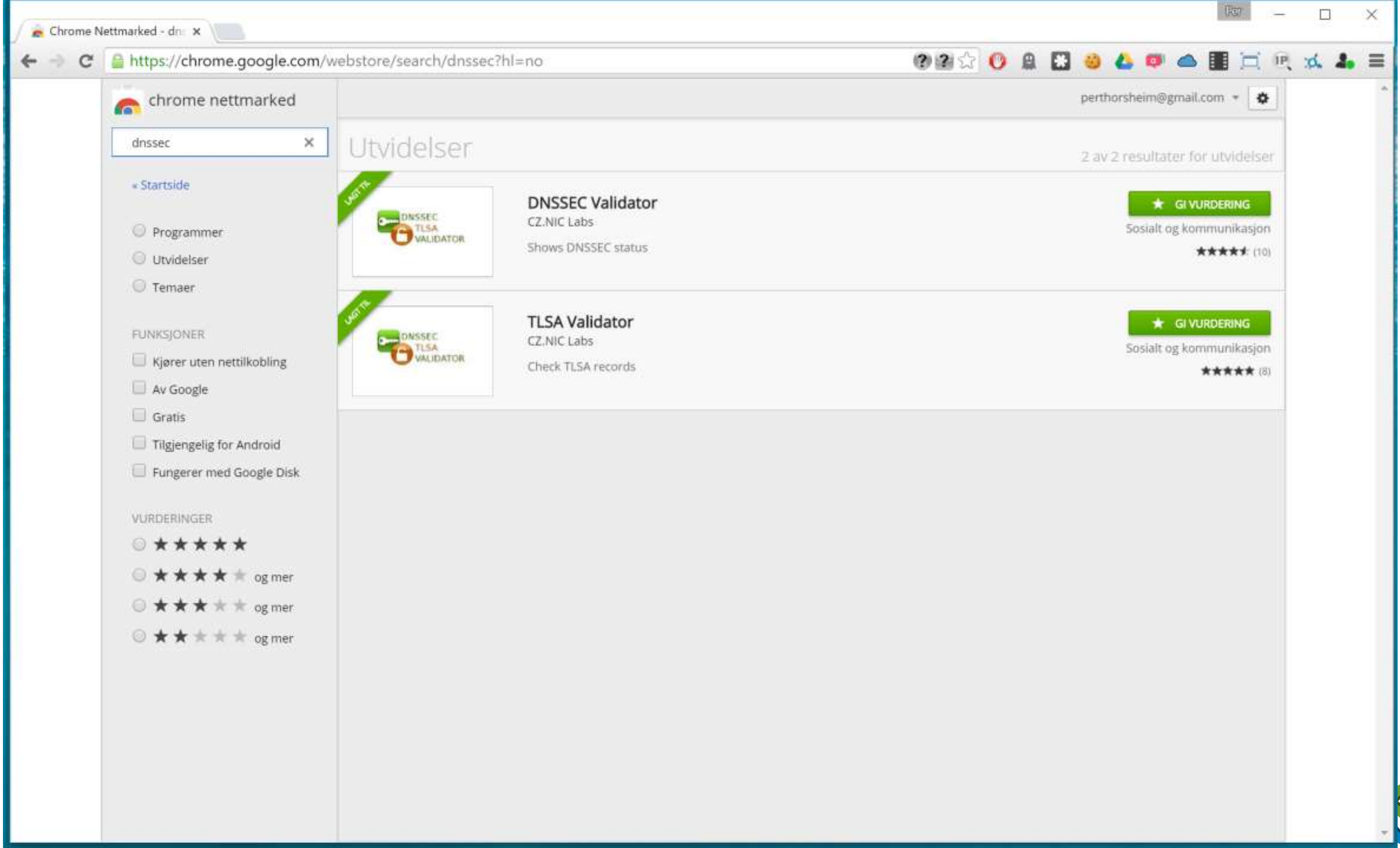
New Features:

- New js-ctypes-based implementation for Firefox.
- New validator implementation for Chromium/Chrome/Opera based on Native Messaging.
- Added new state notification about entering a non-existent (according to DNSSEC) web site.
- Polish localisation.

Bugfixes:

- Updated prefixes for DOM nodes in Firefox js-ctypes extension.
- Fixed bug in type 2 TLSA record validation.
- Fixed some warnings reported from AMO.
- Build mechanism fixes.
- Added name-spaces to Firefox javascript code.
- Deleted nsICache service in js-ctypes extension (compatibility issue Firefox >= 32.*).
- Fixed some another bugs.

Updates:



Chrome Nettmarked - dns ×

https://chrome.google.com/webstore/search/dnssec?hl=no

chrome nettmarked

dnssec ×

« Startside

○ Programmer

○ Utvidelser

○ Temaer

FUNKSJONER

□ Kjører uten nettilkobling

□ Av Google

□ Gratis

□ Tilgjengelig for Android

□ Fungerer med Google Disk

VURDERINGER

○ ★★★★★

○ ★★★★☆ og mer

○ ★★★☆☆ og mer

○ ★★☆☆☆ og mer

perthorsheim@gmail.com

Utvidelser

2 av 2 resultater for utvidelser

LAGT TIL

DNSSEC Validator

CZ.NIC Labs

Shows DNSSEC status

★ GI VURDERING

Sosialt og kommunikasjon

★★★★★ (10)

LAGT TIL

TLSA Validator

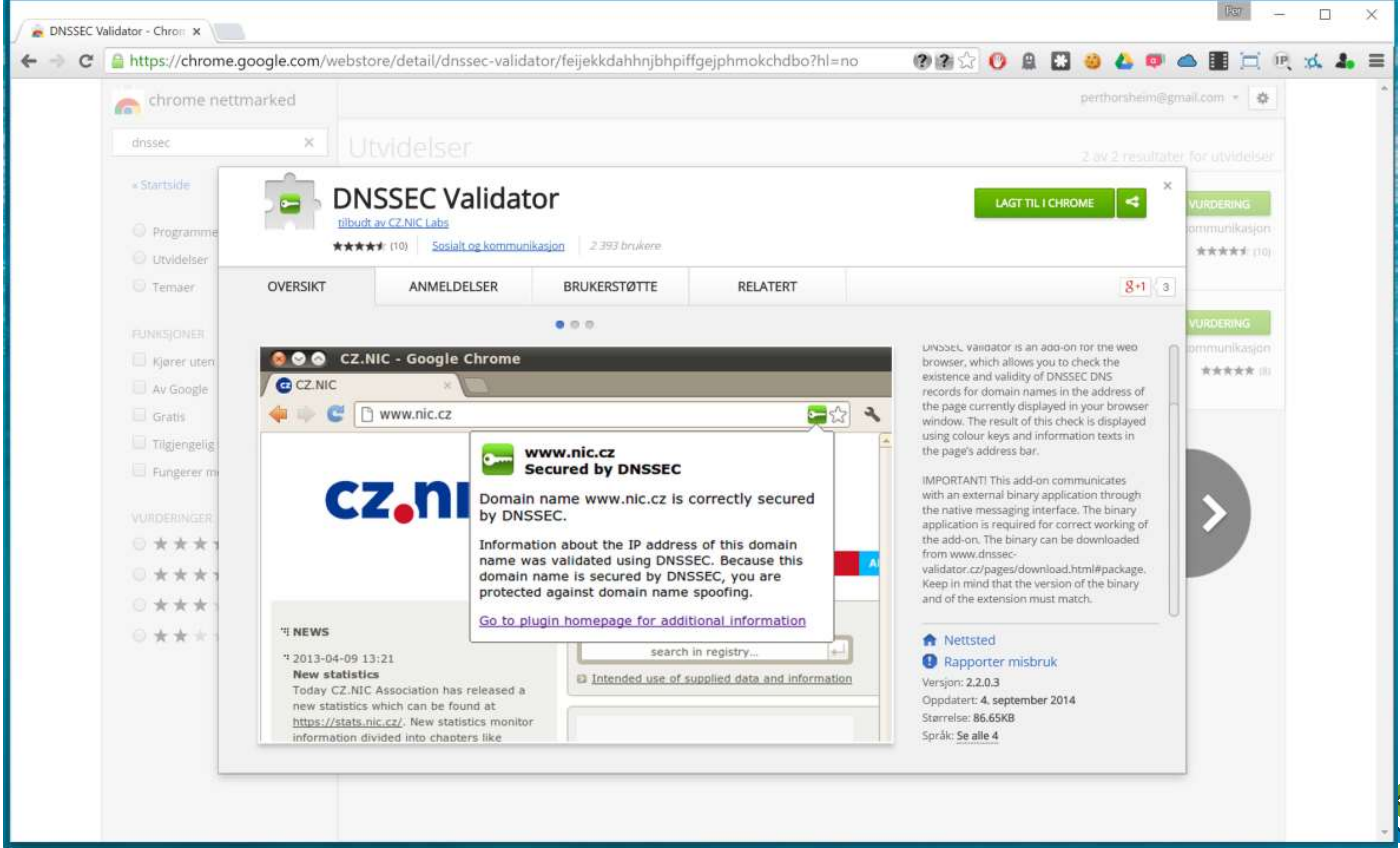
CZ.NIC Labs

Check TLSA records

★ GI VURDERING

Sosialt og kommunikasjon

★★★★★ (8)



DNSSEC Validator

tilbudt av CZ.NIC Labs

★★★★★ (10) | Sosialt og kommunikasjon | 2 393 brukere

www.nic.cz
Secured by DNSSEC

Domain name www.nic.cz is correctly secured by DNSSEC.

Information about the IP address of this domain name was validated using DNSSEC. Because this domain name is secured by DNSSEC, you are protected against domain name spoofing.

Go to plugin homepage for additional information

NEWS

2013-04-09 13:21
New statistics
Today CZ.NIC Association has released a new statistics which can be found at https://stats.nic.cz/. New statistics monitor information divided into chapters like

Intended use of supplied data and information

DNSSEC Validator is an add-on for the web browser, which allows you to check the existence and validity of DNSSEC DNS records for domain names in the address of the page currently displayed in your browser window. The result of this check is displayed using colour keys and information texts in the page's address bar.

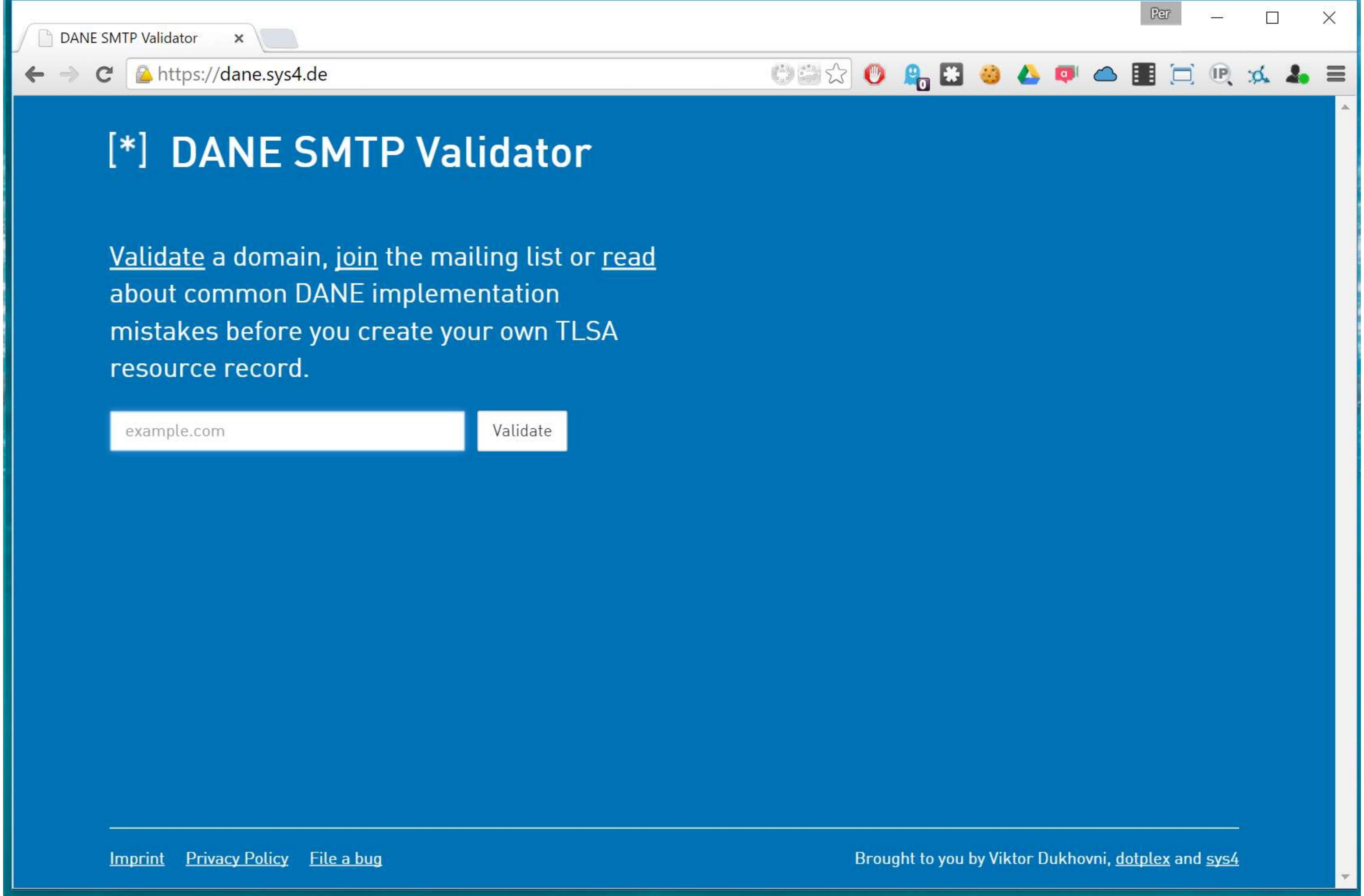
IMPORTANT! This add-on communicates with an external binary application through the native messaging interface. The binary application is required for correct working of the add-on. The binary can be downloaded from www.dnssec-validator.cz/pages/download.html#package. Keep in mind that the version of the binary and of the extension must match.

Nettsted
Rapporter misbruk
Versjon: 2.2.0.3
Oppdatert: 4. september 2014
Størrelse: 86.65KB
Språk: Se alle 4

DNSSEC + DANE TLSA

- TLD uses DNSSEC
  - Your DNS provider uses DNSSEC
    - Signs your domain
      - You create a certificate for your mailserver (Let’s Encrypt!)
      - You put info on your certificate into your signed DNS

- Server X look up your DNSSEC info
- Server X look up your DANE TLSA record
- Server X uses that cert info to encrypt mail to your mailserver



[*] DANE SMTP Validator

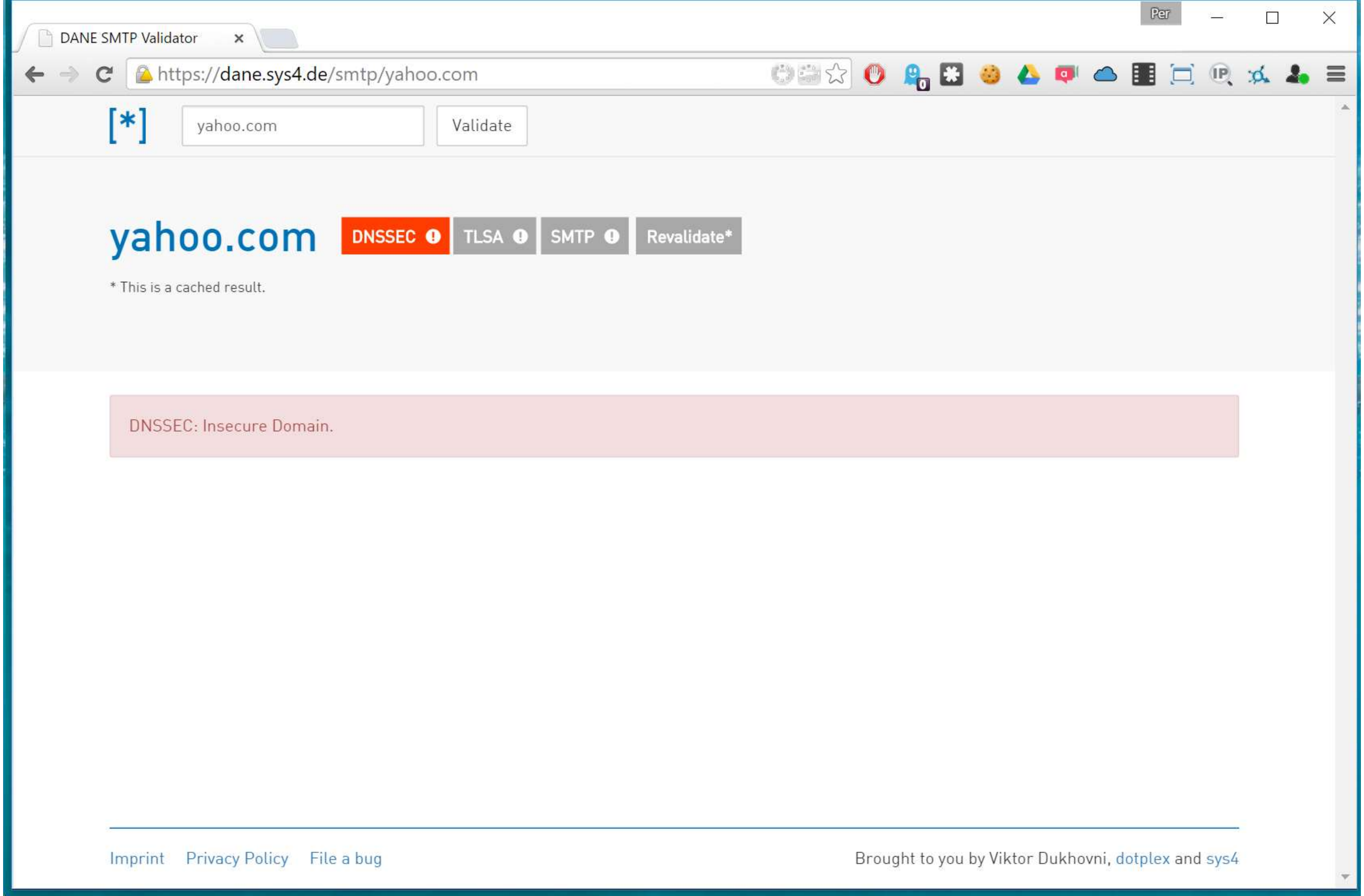
Validate a domain, join the mailing list or read about common DANE implementation mistakes before you create your own TLSA resource record.

example.com

Validate

Imprint Privacy Policy File a bug

Brought to you by Viktor Dukhovni, dotplex and sys4

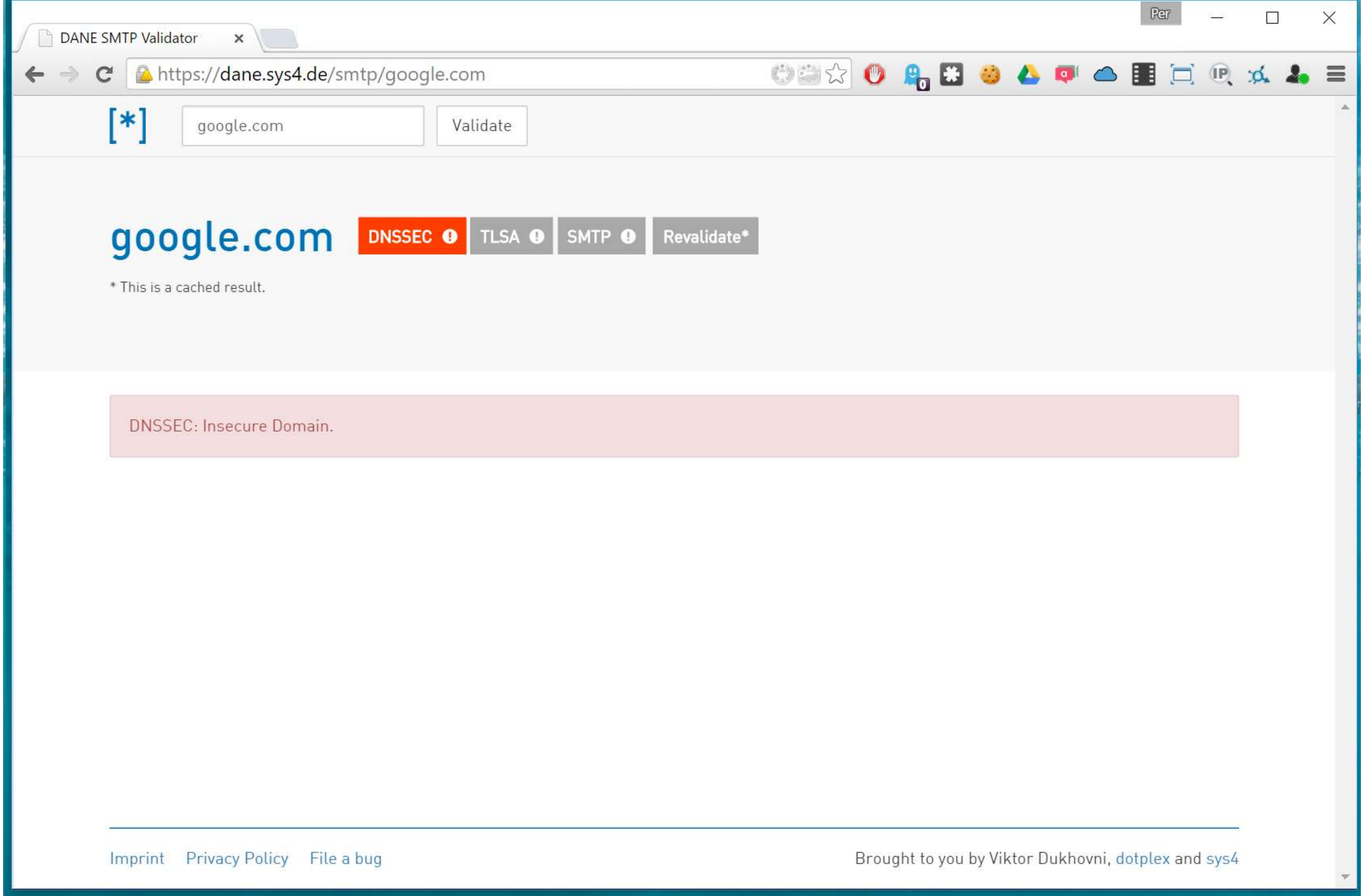


yahoo.com

* This is a cached result.

DNSSEC: Insecure Domain.

Brought to you by Viktor Dukhovni, dotplex and sys4


DANE SMTP Validator
https://dane.sys4.de/smtp/google.com
Per
[*]
google.com
Validate

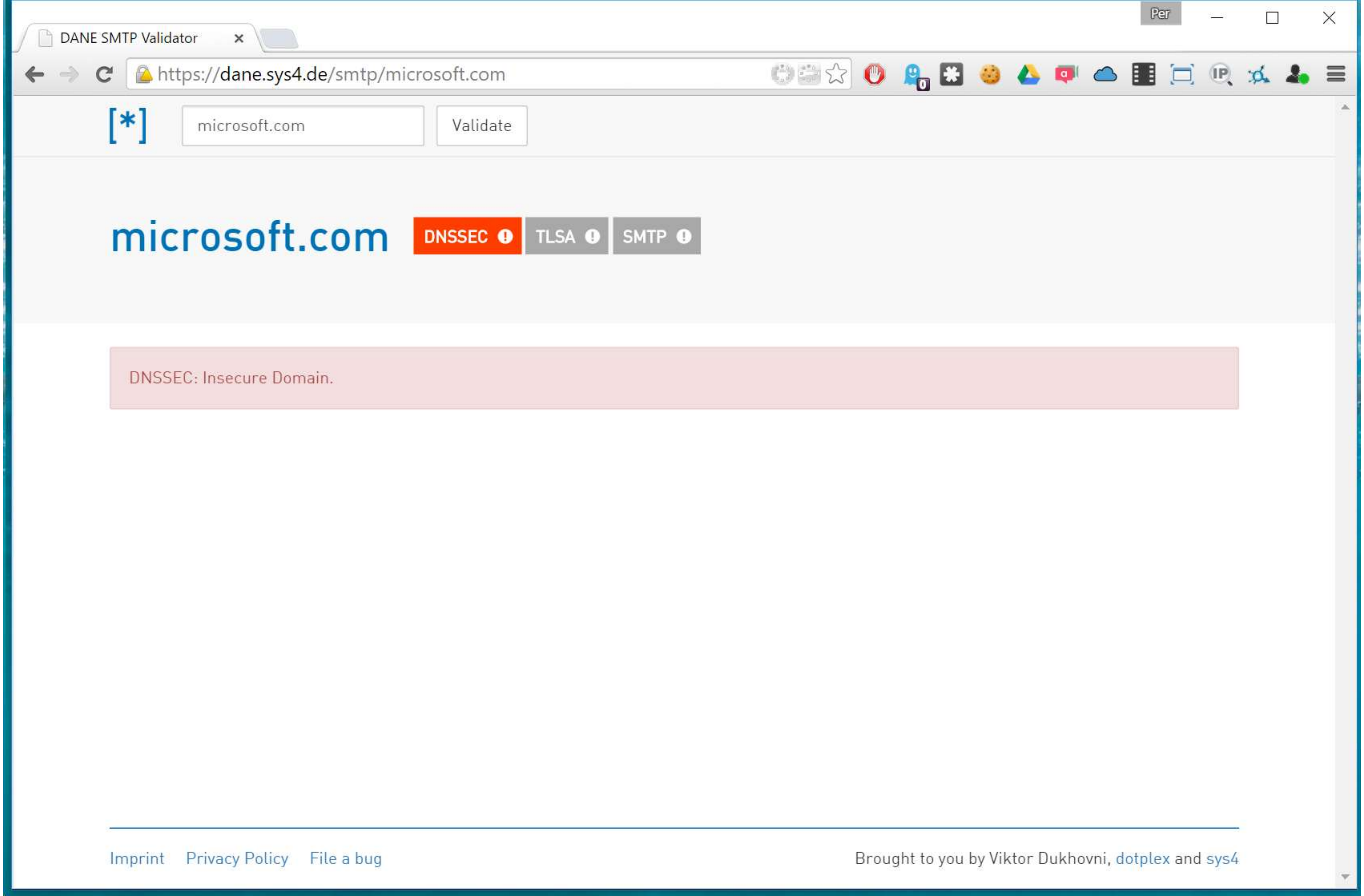
google.com

DNSSEC ! TLSA ! SMTP ! Revalidate*

* This is a cached result.

DNSSEC: Insecure Domain.

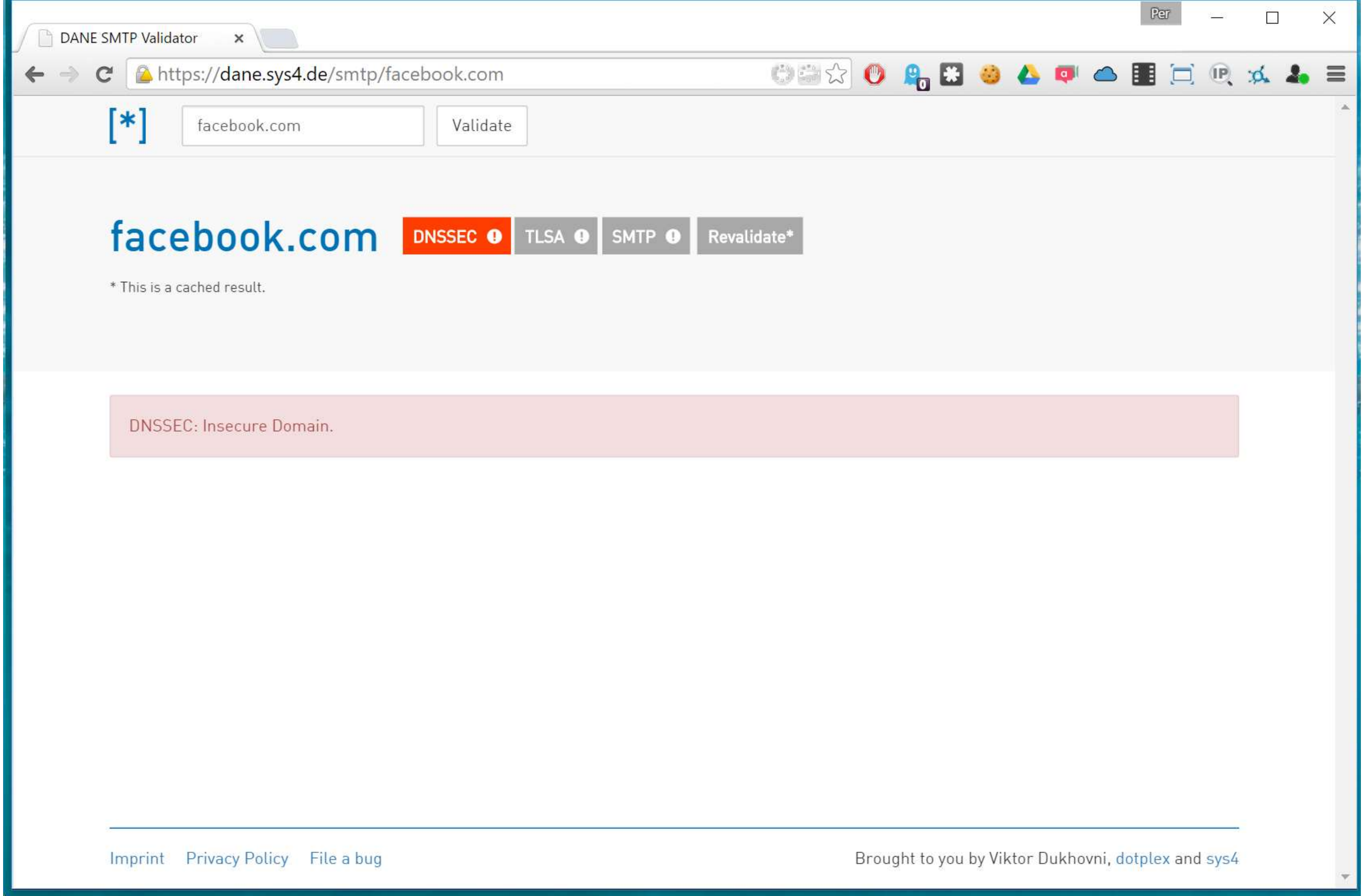
Imprint
Privacy Policy
File a bug
Brought to you by Viktor Dukhovni, dotplex and sys4



microsoft.com

DNSSEC: Insecure Domain.

Brought to you by Viktor Dukhovni, dotplex and sys4

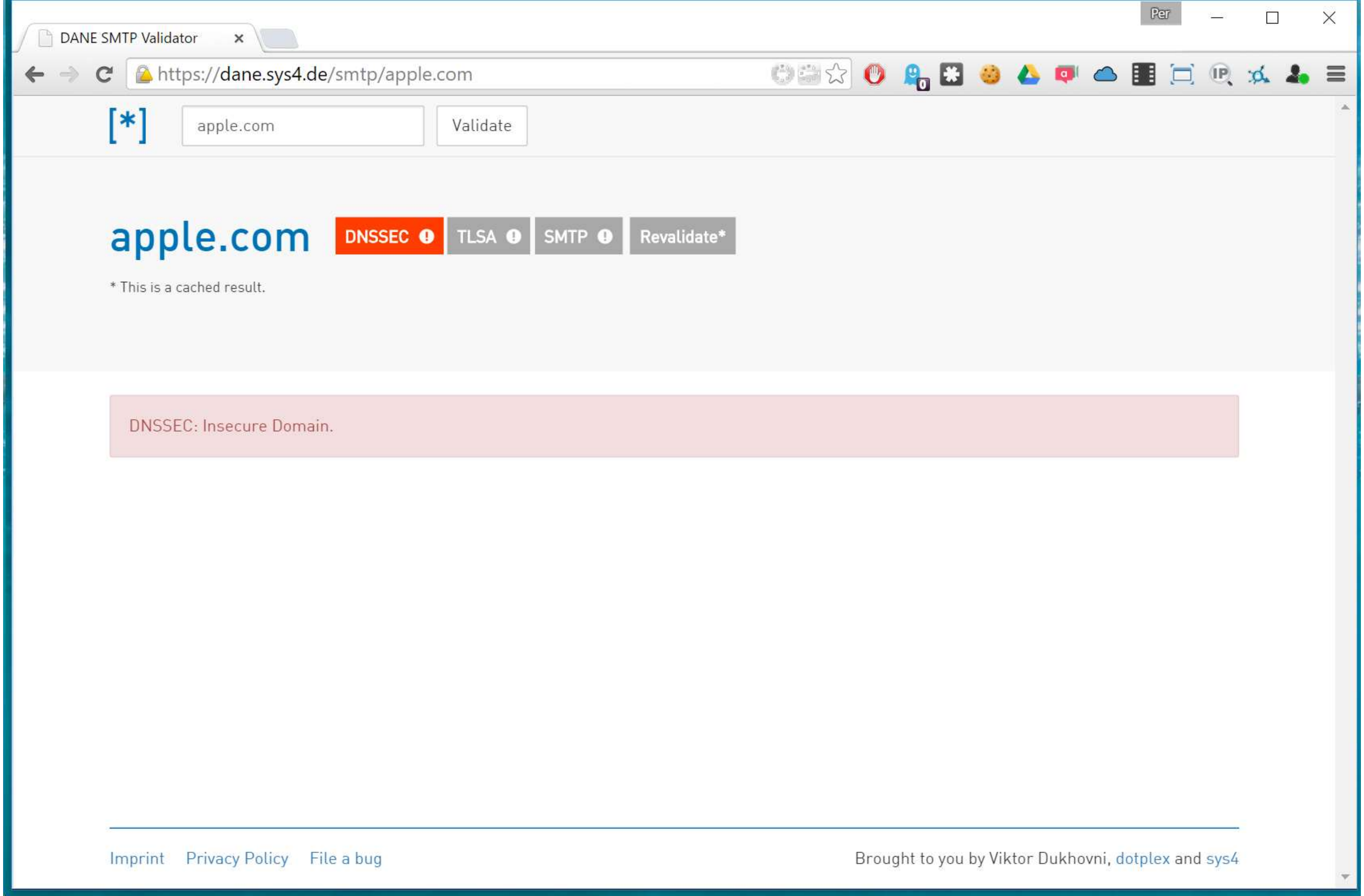


facebook.com

* This is a cached result.

DNSSEC: Insecure Domain.

Brought to you by Viktor Dukhovni, dotplex and sys4

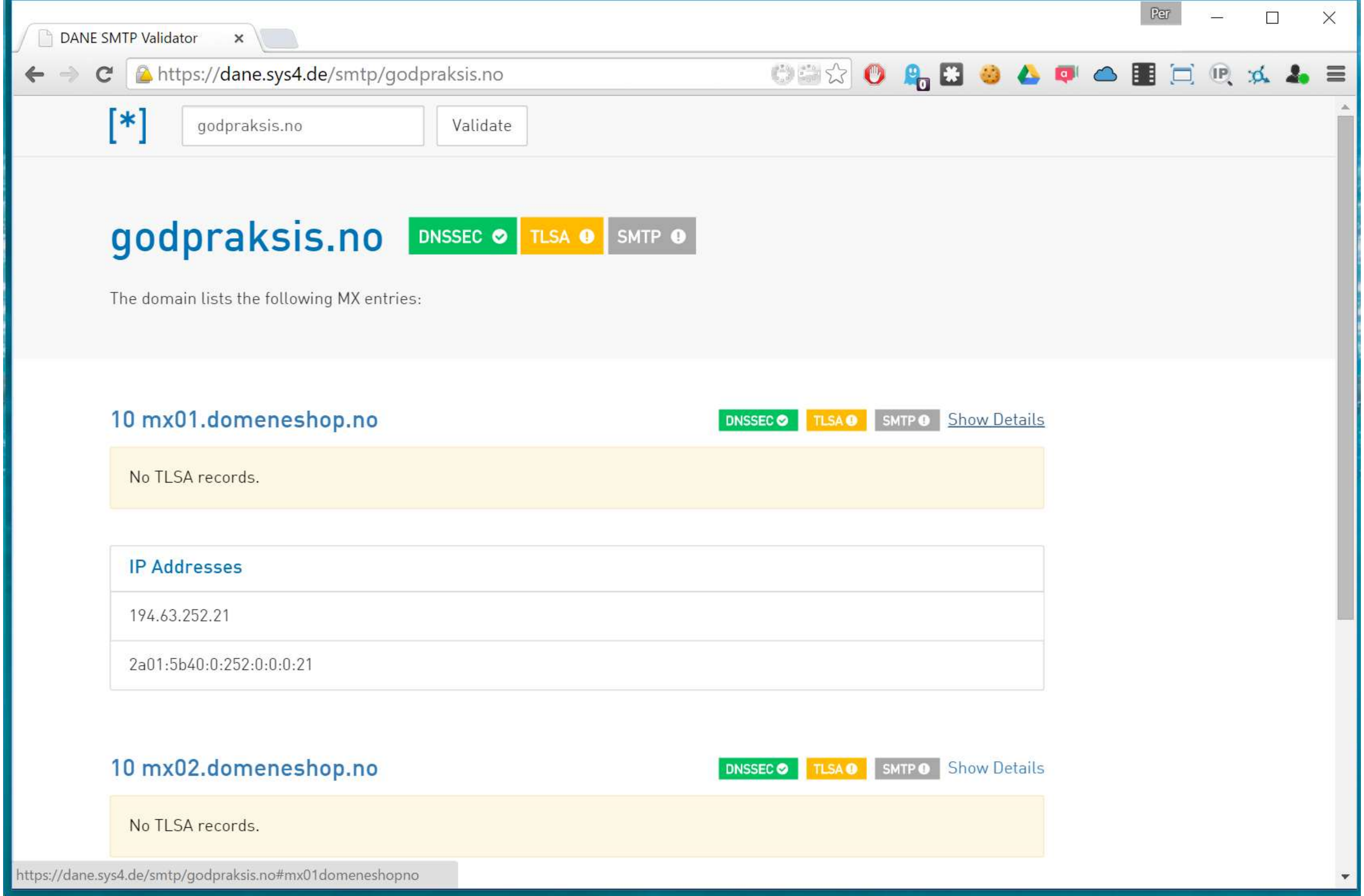


apple.com

* This is a cached result.

DNSSEC: Insecure Domain.

Brought to you by Viktor Dukhovni, dotplex and sys4


DANE SMTP Validator
Per
https://dane.sys4.de/smtp/godpraksis.no
[*]
godpraksis.no
Validate

godpraksis.no

DNSSEC ✓ TLSA ! SMTP !

The domain lists the following MX entries:

10 mx01.domeneshop.no

DNSSEC ✓ TLSA ! SMTP ! Show Details

No TLSA records.

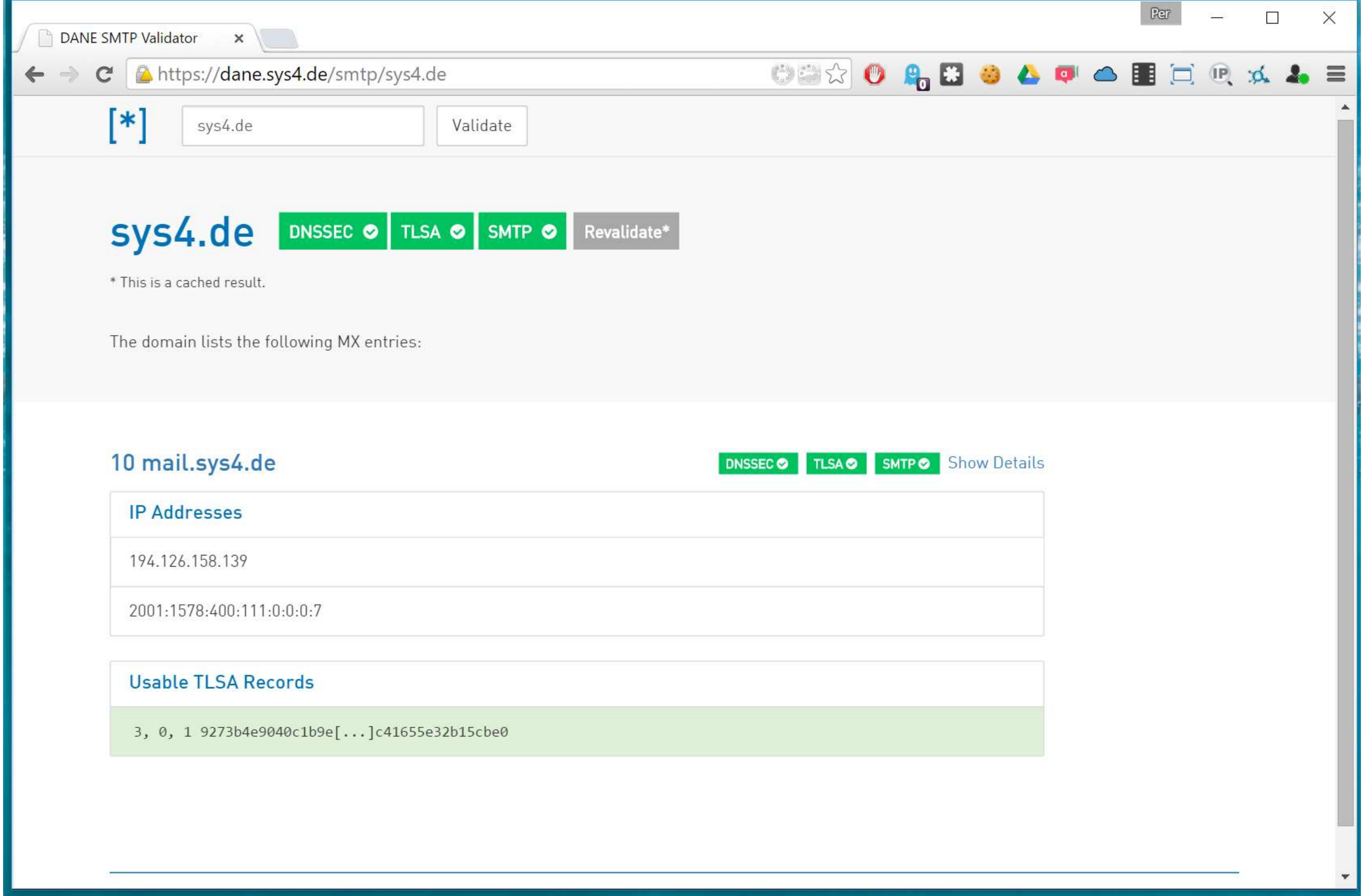
IP Addresses
194.63.252.21
2a01:5b40:0:252:0:0:0:21

10 mx02.domeneshop.no

DNSSEC ✓ TLSA ! SMTP ! Show Details

No TLSA records.

https://dane.sys4.de/smtp/godpraksis.no#mx01domeneshopno



sys4.de

* This is a cached result.

The domain lists the following MX entries:

10 mail.sys4.de

IP Addresses

194.126.158.139

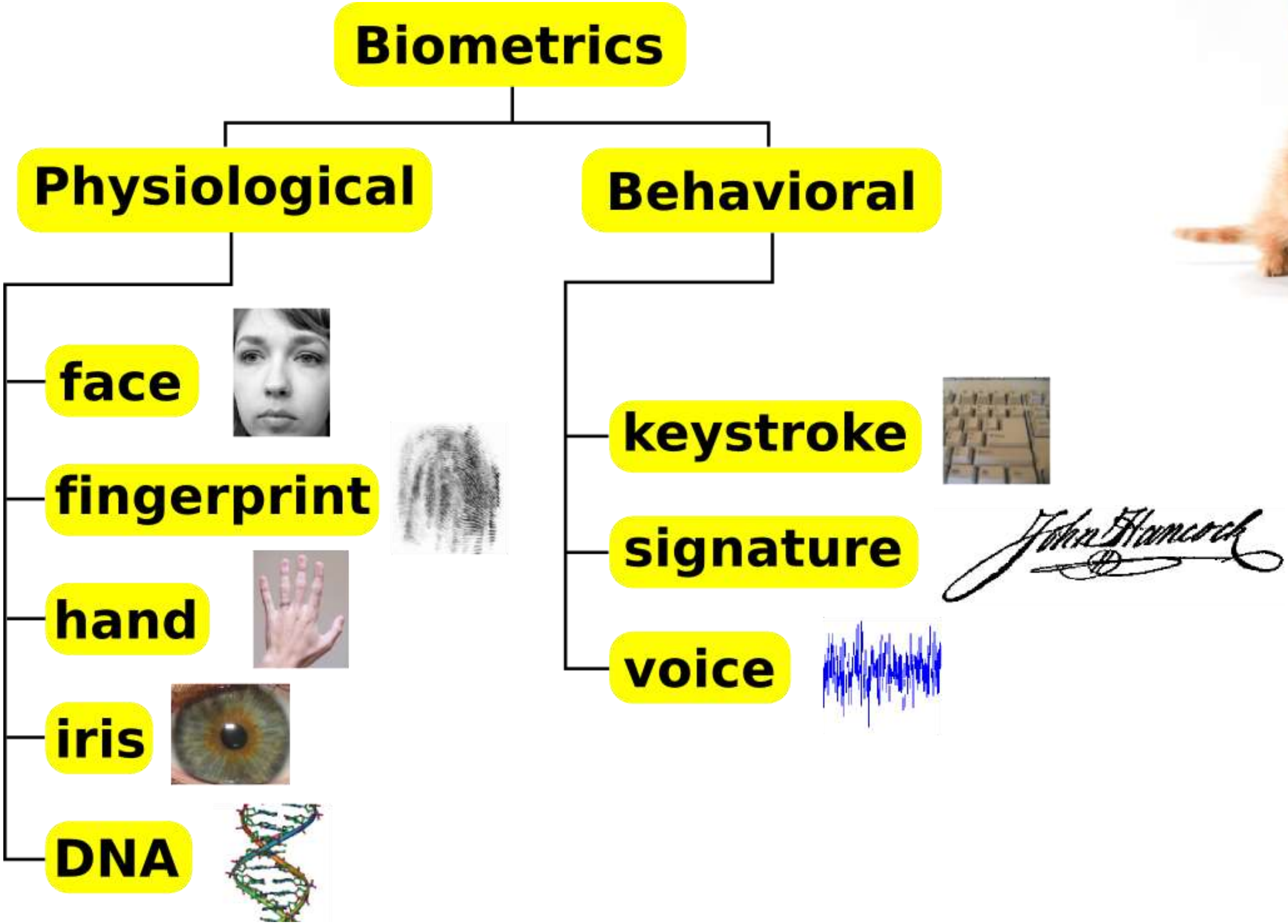
2001:1578:400:111:0:0:0:7

Usable TLSA Records

```
3, 0, 1 9273b4e9040c1b9e[...]c41655e32b15cbe0
```

Keystroke Dynamics

Tracking the human, not the browser, computer or network.



Biometrics

- Physiological
  - face
  - fingerprint
  - hand
  - iris
  - DNA
- Behavioral
  - keystroke
  - signature
  - voice

Behavioral Biometrics – For Good & Bad

Good

- «Invisible» 2FA
- Identifies humans, not tech
- Does not require login
- Keystroke, mouse & touch
- Biometric profile generation by enrollment or through «normal use»
- Continous authentication

Bad

See left column.

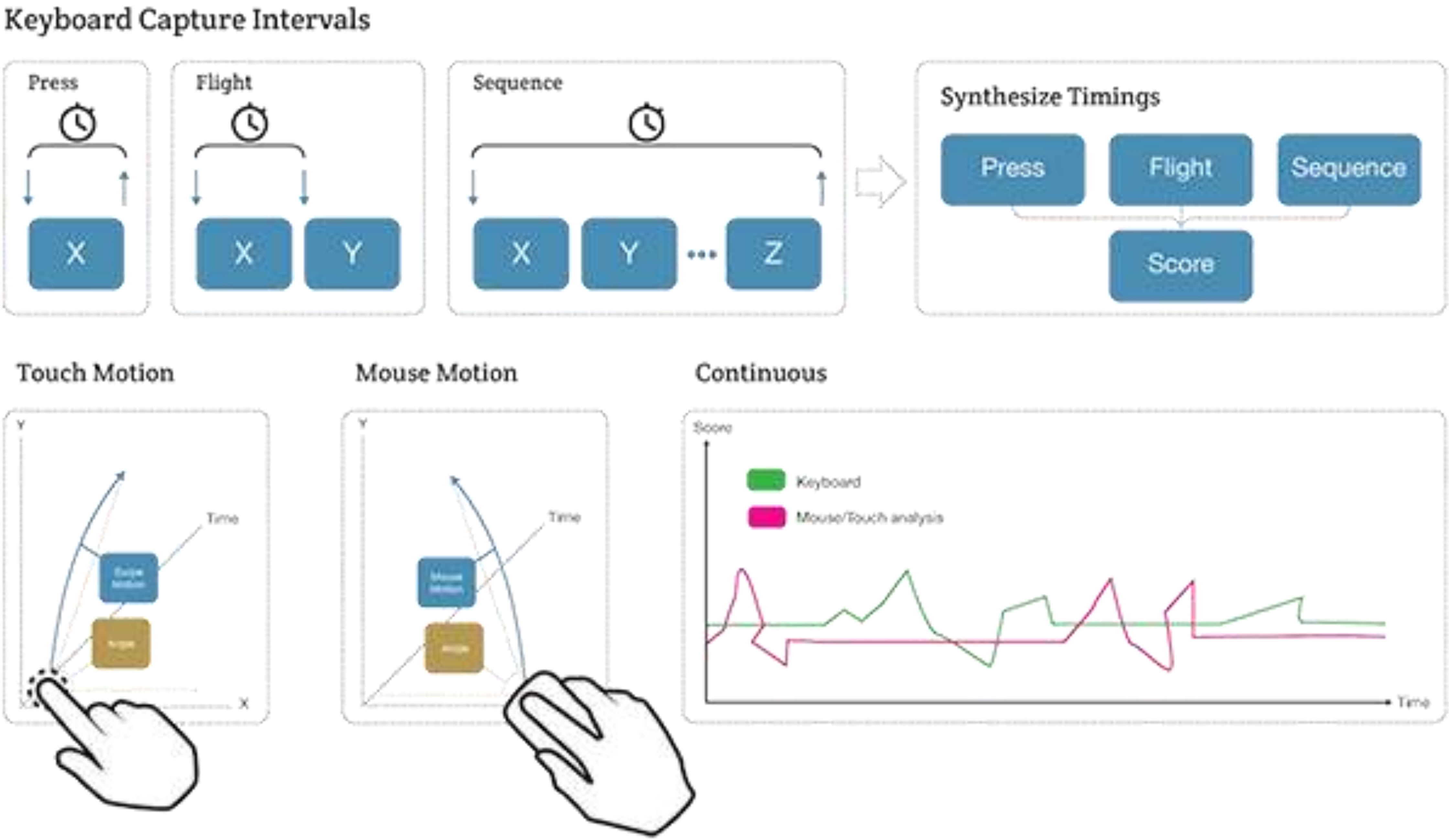
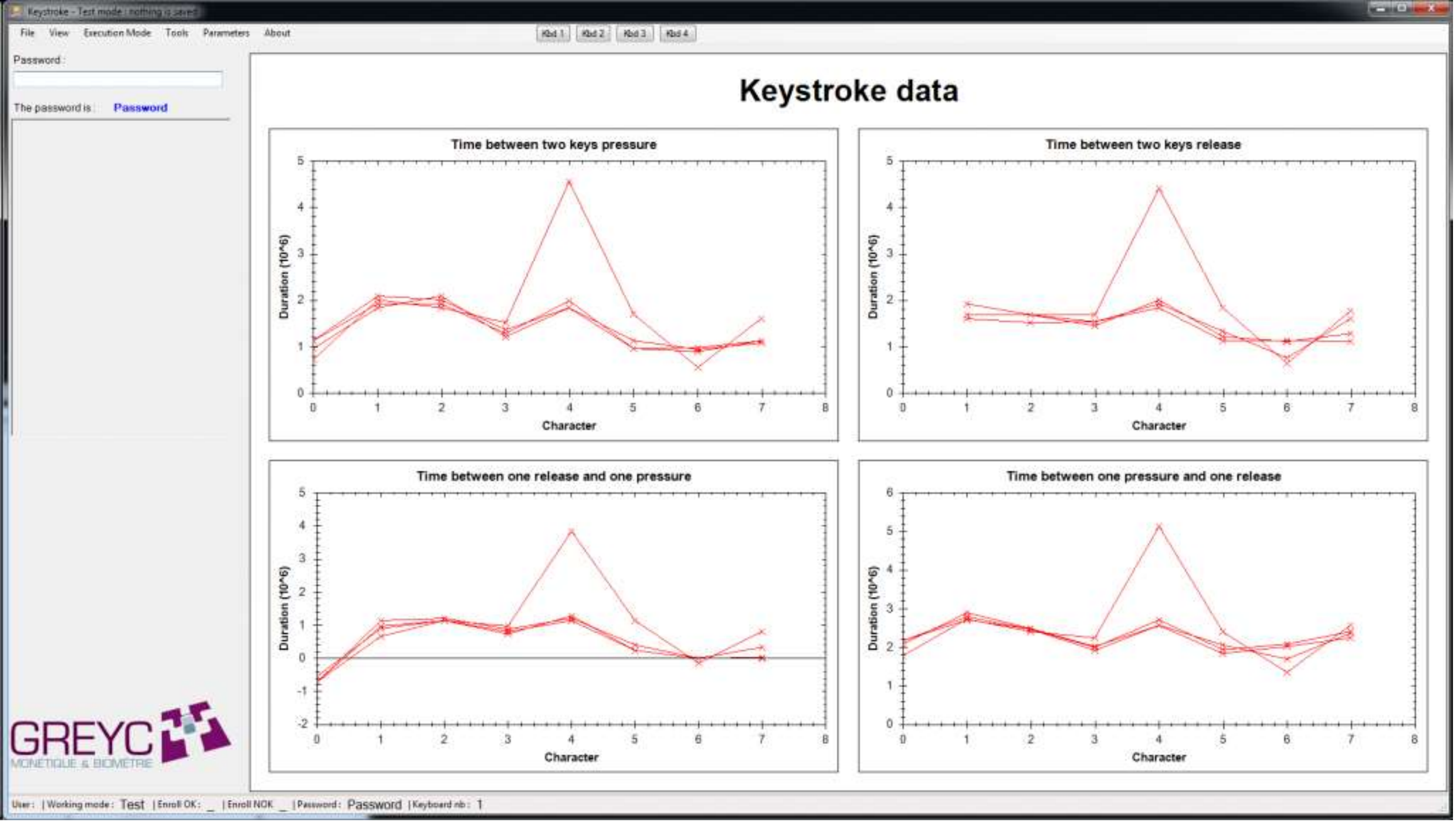


Image source: Behaviosec.com


Keystroke - Test mode : nothing is saved
File
View
Execution Mode
Tools
Parameters
About
Kbd 1
Kbd 2
Kbd 3
Kbd 4
GREYC
MONETIQUE & BIOMETRIE
Time between two keys pressure
Time between two keys release
Time between one release and one pressure
Time between one pressure and one release
Duration (10^6)
Character
0
1
2
3
4
5
6
7
8
-1
-2

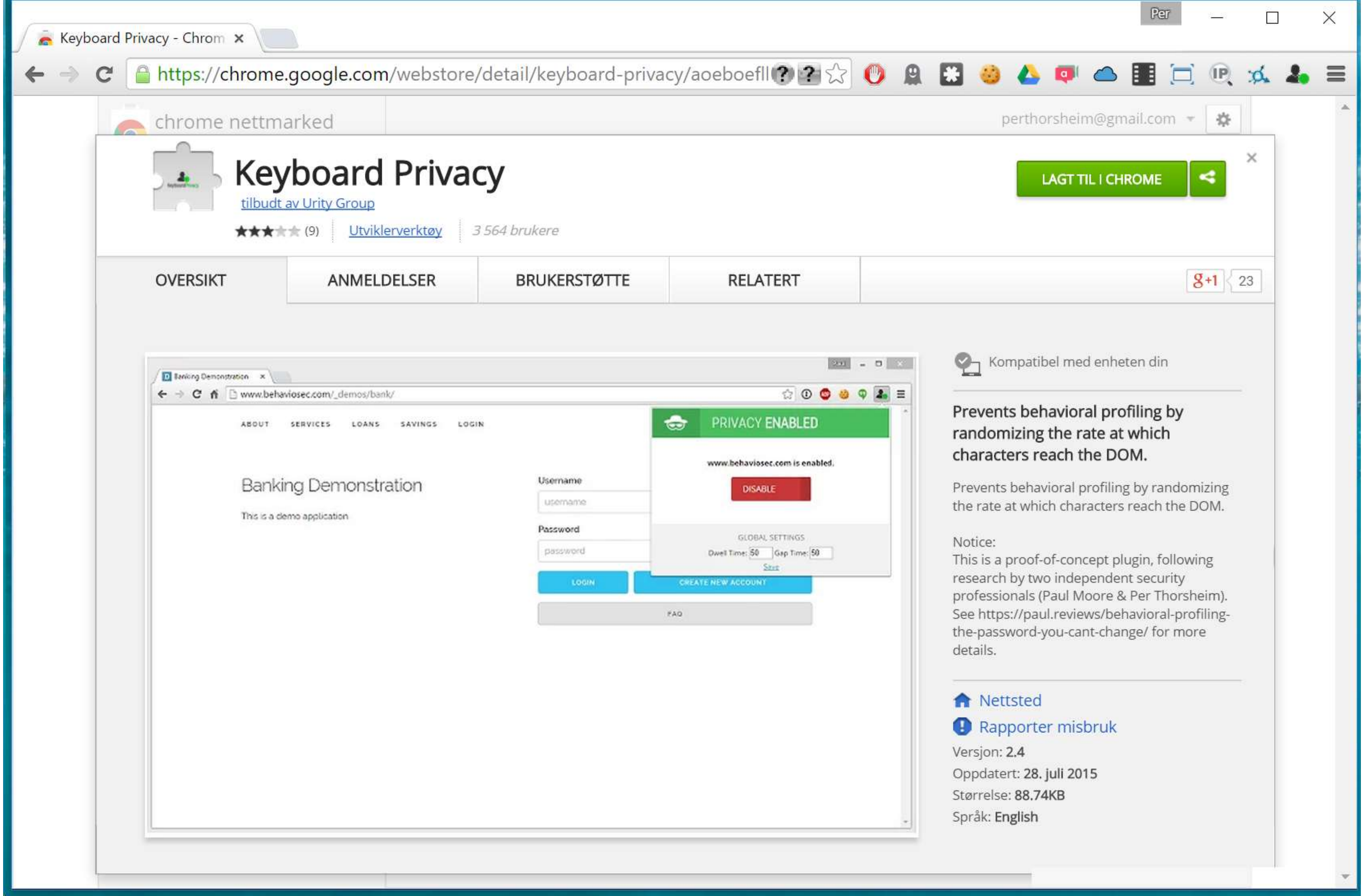
Password :

The password is : Password

Keystroke data

User : | Working mode : Test | Enroll OK : _ | Enroll NOK _ | Password : Password | Keyboard nb : 1

Free download: http://www.epaymentbiometrics.ensicaen.fr/publications/resources



Keyboard Privacy - Chrom ×
Per
https://chrome.google.com/webstore/detail/keyboard-privacy/aoeboefll
chrome nettmarked
perthorsheim@gmail.com

Keyboard Privacy

tilbudt av Urity Group

★★★☆☆ (9) | Utviklerverktøy | 3 564 brukere

Banking Demonstration

This is a demo application

Username

username

Password

password

www.behaviosec.com is enabled.

Dwell Time: 50 Gap Time: 50

Kompatibel med enheten din

Prevents behavioral profiling by randomizing the rate at which characters reach the DOM.

Prevents behavioral profiling by randomizing the rate at which characters reach the DOM.

Notice:
This is a proof-of-concept plugin, following research by two independent security professionals (Paul Moore & Per Thorsheim). See https://paul.reviews/behavioral-profiling-the-password-you-cant-change/ for more details.

Nettsted

Rapporter misbruk

Versjon: 2.4

Oppdatert: 28. juli 2015

Størrelse: 88.74KB

Språk: English

GodPraksis

✉ per@godpraksis.no

🌐 godpraksis.no

☎ +47 90 99 92 59

@thorsheim