Kommunikation schützen mit Verschlüsselung

Warnungen

technisch

beängstigend

praktisch

interaktiv

interaktiv

interaktiv

Kommunikation

Kommunikation

Internet

Internet

Alice - Bob

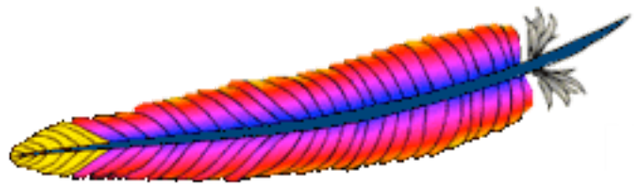
Programm - Server

Software - Software

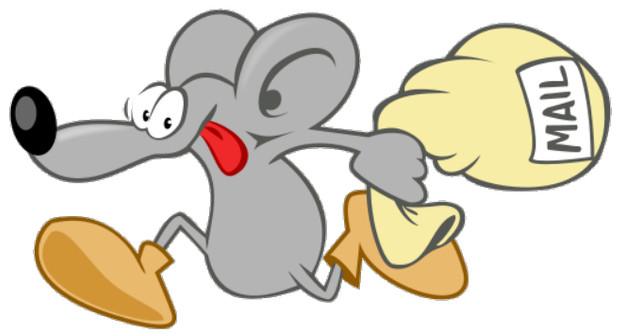

Safari File Edit View History Bookmarks Window Help
Sat 9:26 PM
DNP 14 | Brandung 2.0
https://dnp.unwatched.org/
DNP14
DATEN.NETZ.POLITIK
BRANDUNG 2.0
20. - 21. SEPTEMBER 2014 IM GARTENPALAIS SCHÖNBORN, WIEN
DER KONGRESS
PROGRAMM
LOCATION
TICKETS
SPONSOREN
PRESSE
KONTAKT
Der Daten, Netz & Politik Kongress 2014 hat begonnen!
Willkommen
bei
Daten, Netz & Politik 2014
DNP
INFORMIERT BLEIBEN
Jetzt Newsletter abonnieren!
E-Mail Adresse
Abonnieren
ANMELDUNG
Benutzername:
Passwort:
ANMELDEN
Neues Passwort anfordern
SUCHE
Diese Website durchsuchen:
SUCHEN
PowerBook G4


01:26
38 %
DNP 14 | Brandung 2.0
dnp.unwatched.org/
Google
DNP14
DATEN.NETZ.POLITIK
BRANDUNG 2.0
20. - 21. SEPTEMBER 2014 IM GARTENPALAIS SCHÖNBORN, WIEN
DER KONGRESS
PROGRAMM
LOCATION
TICKETS
SPONSOREN
PRESSE
KONTAKT
Der Daten, Netz & Politik Kongress 2014 hat begonnen!
Willkommen bei Daten, Netz & Politik 2014
Wir freuen uns auf zwei Tage voller interessanter Vorträge, spannender Diskussionen und anregender Gespräche mit unseren TeilnehmerInnen.
INFORMIERT BLEIBEN
ANMELDUNG
SUCHE
SPONSOREN
ispa
Barracuda


NOKIA
SIM
einsetzen
STOP
1
2 abc
3 def
4 ghi
5 jkl
6 mno
7 pqrs
8 tuv
9 wxyz
*
0
#



NGINX™



DOVECOT

ejabberd

Technik

Protokolle

http

xmpp

smtp

submission

:

imap

pop

Gemeinsamkeiten?

Alt

Klartext

Angst

WLAN

Internet Provider

＼(=^‥^)

Und nun?

Irefpuyüffryhat

Verschlüsselung

Vertraulichkeit

2 Integrität

3 Authentizität

4 Nichtabstreitbarkeit

Transportverschlüsselung

TLS 1.2

TLS 1.1

TLS 1.0

~~*SSLv3*~~

~~*SSLv2*~~

Testen

Webserver testen

https://ssllabs.com/ssltest

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Domain name: Submit

Do not show the results on the boards

Recently Seen

metronets.com	Err
slack.com	
owncloud.jonaskim.de	
wasserwacht-magdeburg.de	A-
pescaboutique.com	C
openmailbox.org	A
d2p-dev.novartis.com	Err
pop.openmailbox.org	A
client.investia.ca	F
smtp.openmailbox.org	A

Recent Best-Rated

londoners.ro	A+
openmailbox.org	A
pop.openmailbox.org	A
smtp.openmailbox.org	A
scottlinux.com	A-
sal.investpoint.automatedfin ...	A-
vlietlandziekenhuis.nl	B
votesmart.org	B
pescaboutique.com	C
office.com	C

Recent Worst-Rated

client.investia.ca	F
outlook.com	F
webmin.studiotwo.com	Trust
myhr.ahg.com.au	F
portal.lrgh.org	F
questful.com	F
poulp.net	Trust
mysql.triedtoswiminlava.net	Trust
my.sph.harvard.edu	F
api.2dehands.com	F

SSL Report: nsa.gov (23.39.50.161)

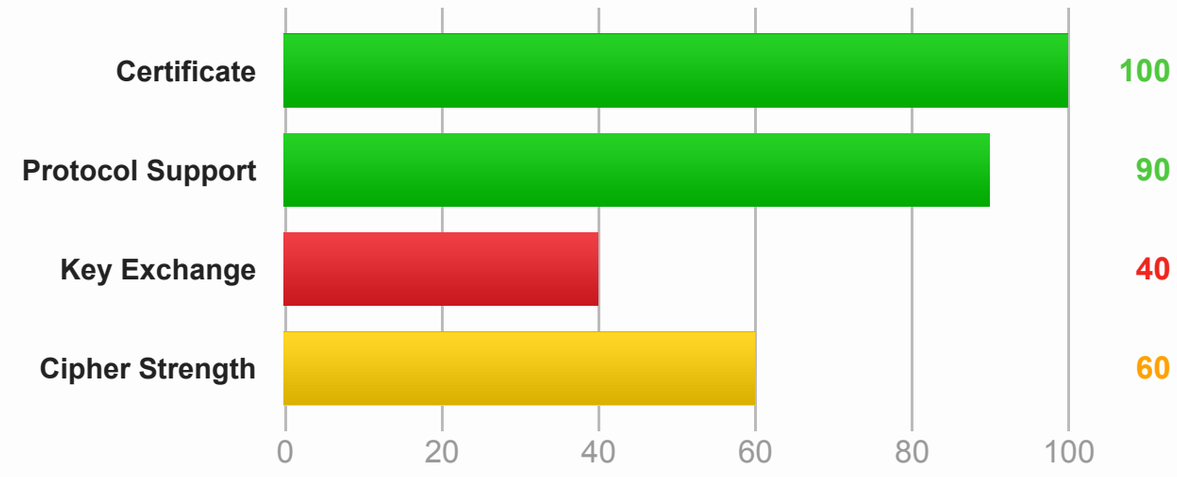
Assessed on: Sat Sep 20 20:37:28 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

C



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

🎄 https://isitchristmas.com

SSL Report: isitchristmas.com (54.235.64.112)

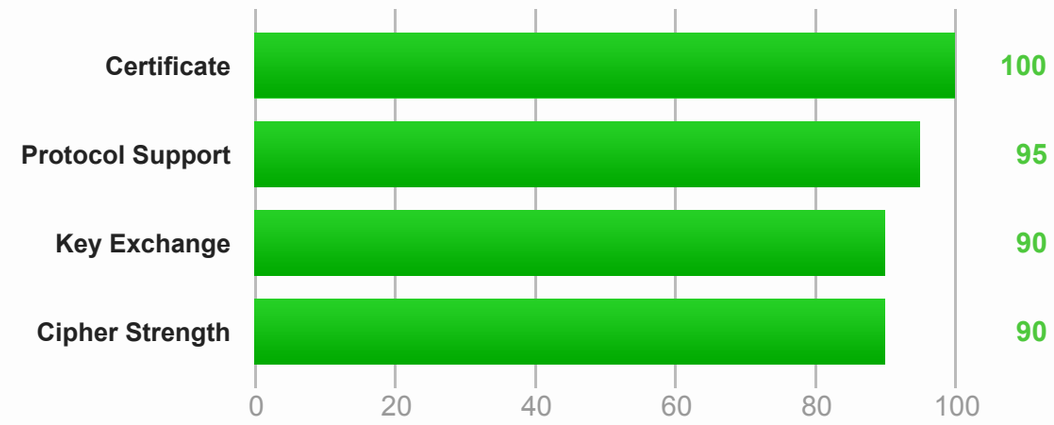
Assessed on: Mon Jul 28 06:42:17 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

A+



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication

Server Key and Certificate #1

SSL Report: ecb.europa.eu (184.25.151.166)

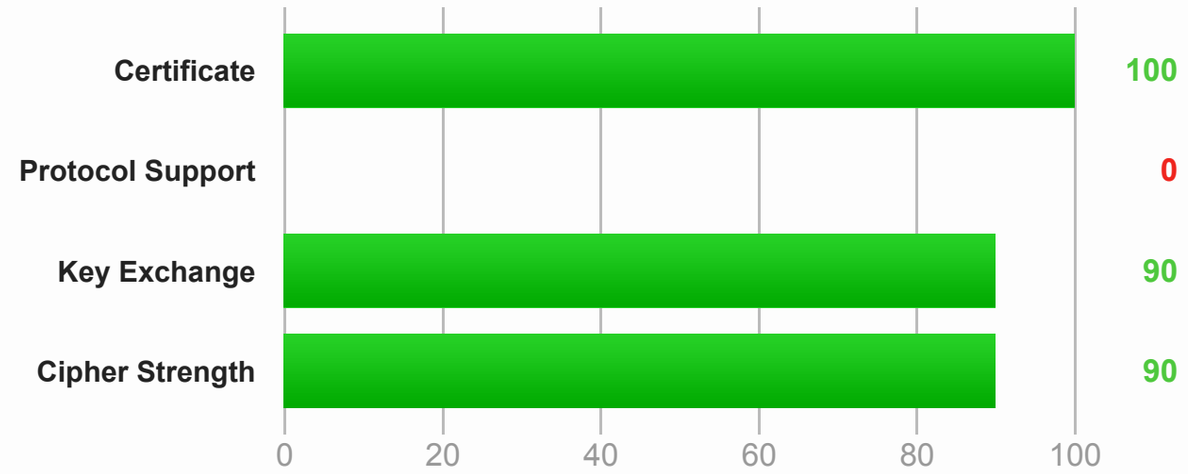
Assessed on: Sat Sep 20 20:51:40 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

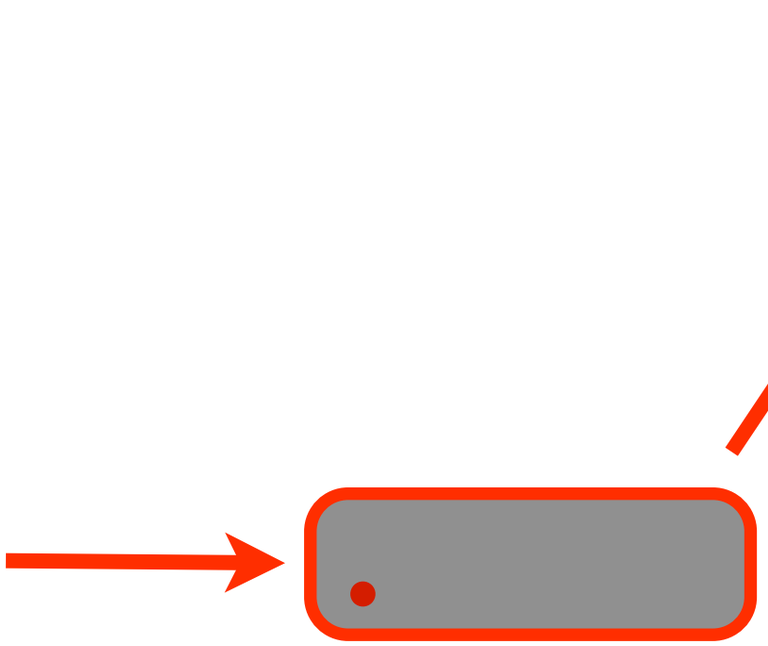
This server supports SSL 2, which is obsolete and insecure. Grade set to F.

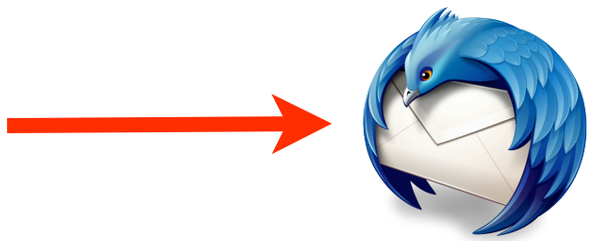
Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Email

https://starttls.info/





Does your mail server support STARTTLS?

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

Results for: digitalcity.wien

Mail server	Result
us2.mx1.mailhostbox.com	STARTTLS not supported!
us2.mx2.mailhostbox.com	STARTTLS not supported!
us2.mx3.mailhostbox.com	STARTTLS not supported!

Click the score for details.

Test another!

This site is a beta. | Read about this. | 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: parlament.gv.at

Mail server	Result
mta3.parlament.gv.at	STARTTLS not supported!
mta2.parlament.gv.at	STARTTLS not supported!

Click the score for details.

Test another!

This site is a beta. | Read about this. | 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: wko.at

Mail server	Result
mail1.wk.or.at	Grade: C (58.0%)

Certificate

- The certificate is not valid for the server's hostname.
- There is a self-signed certificate in the trust chain. It may be a configuration problem.
- There are one or more fatal problems which causes the certificate not to be trusted.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Protocol

- Supports TLSV1.

Key exchange

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

Cipher

- Weakest accepted cipher: 40.
- Strongest accepted cipher: 56.

Does your mail server support STARTTLS?

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

Results for: ubermorgen.com

Mail server	Result
ubermorgen.com	Grade: A (93.4%)

Certificate

- No remarks.

Protocol

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

Key exchange

- Key size is 4096 bits; that's very good.

Cipher

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

Results for: nsa.gov

Mail server	Result
emvm-gh1-uea09.nsa.gov	Grade: D (42.8%)

Certificate

- The certificate is not valid for the server's hostname.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Protocol

- Supports SSLV3.
- Supports TLSV1.

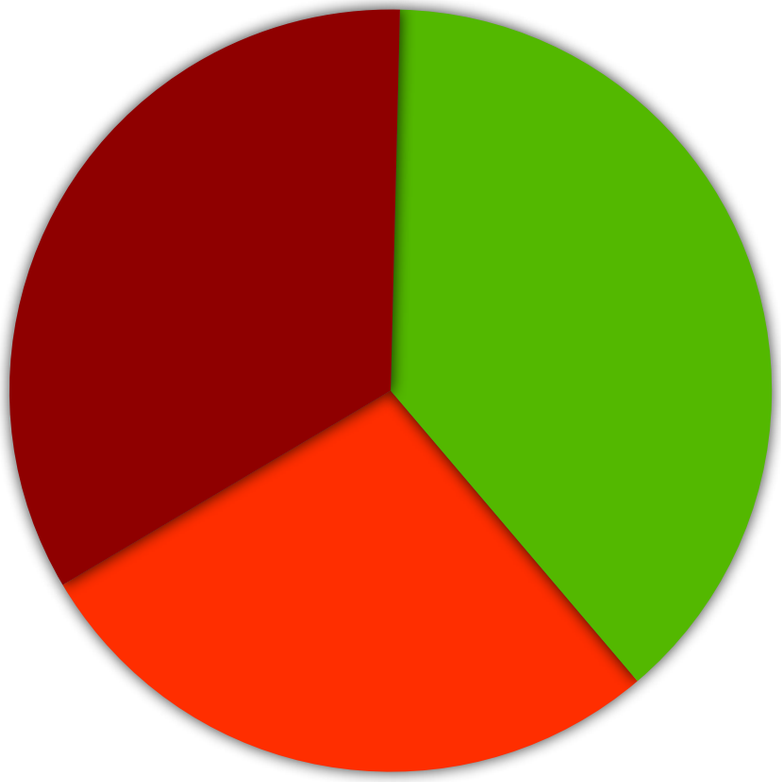
Key exchange

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

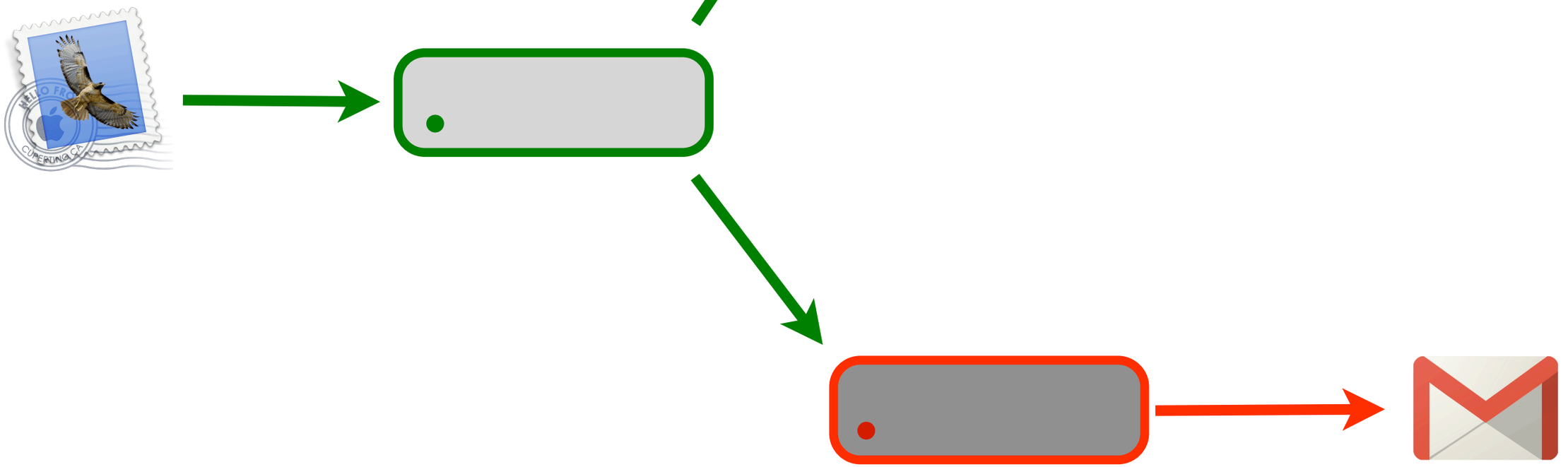
Cipher

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

emvm-gh1-uea08.nsa.gov	Grade: D (44.3%)



https://starttls.info/stats



Chat

https://xmpp.net/

IM Observatory client report for jabber.maclemon.at

Test started 2014-09-20 20:38:05 UTC 28 minutes ago.

Show server to server result | Permalink to this report

Score

jabber.maclemon.at:5222

Certificate score:	100	Grade:
Key exchange score:	100	A
Protocol score:	95	
Cipher score:	90	

General

jabber.maclemon.at:5222

Version	unknown unknown
StartTLS	REQUIRED

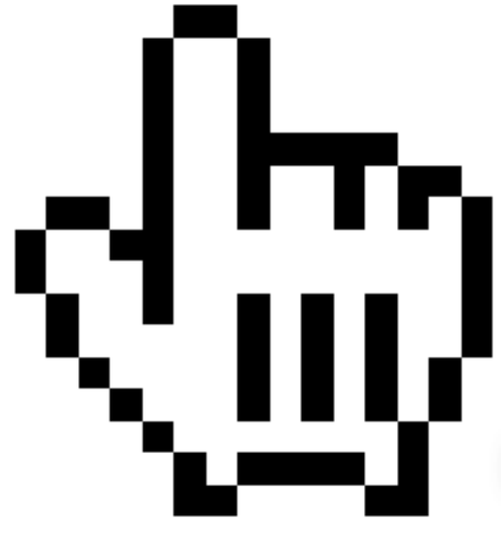

A

Handlungsbedarf

Verschlüsselung muß Standard sein

CRYPTO PARTY


bettercrypto·org



Fragen?

Hausübung:

https://SSLLabs.com Web

https://StartTLS.info Mail

https://xmpp.net Chat

Weitere Information

https://CryptoParty.at

https://BetterCrypto.org

https://MacLemon.at

Pepi Zawodsky

@MacLemon

https://MacLemon.at/

Bilder und Logos


Slide 16: PowerBook G4


Slide 17: iPhone


Slide 18: Nokia 7110



https://www.mozilla.org/en-US/foundation/licensing/


http://creativecommons.org/licenses/by/2.5/


https://www.torproject.org/docs/trademark-faq.html.en


https://www.apple.com/pr/products/


https://www.apache.org/licenses/

http://wiki.nginx.org/Propaganda

http://wiki2.dovecot.org/MitLicense


http://www.postfix.org/documentation.html


https://adium.im/about/


https://pidgin.im/about/

https://www.process-one.net/en/company/