Let's Encrypt with Best Practices

Till Maas
till.maas@redteam-pentesting.de
https://www.redteam-pentesting.de/

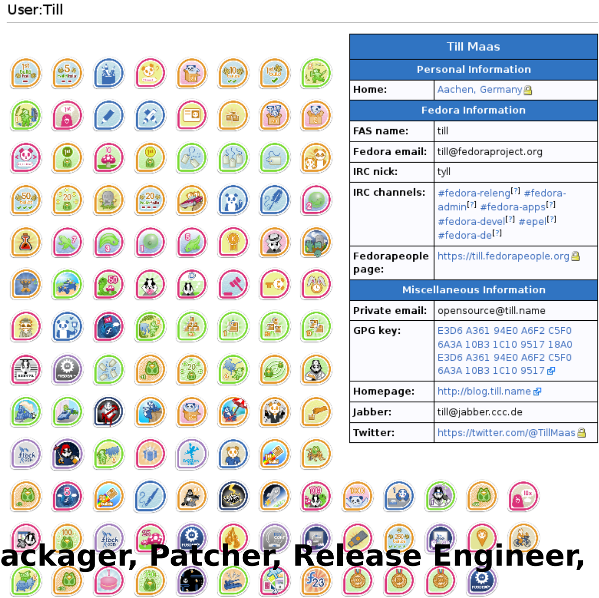
6 February 2016

Queen
Elizabeth
Islands
Greenland
Barents
Sea
Siberia
ASIA
NORTH
AMERICA
North
Atlantic
Ocean
EUROPE
Gobi
North
Pacific
Ocean
Sahara
Arabian
Peninsula
AFRICA
Amazon
Basin
Congo
Basin
Indian
Ocean
Indonesia
SOUTH
AMERICA
South
Atlantic
Ocean
AUSTRALIA

© OpenStreetMap contributors. Tiles courtesy of MapQuest

Aachen, Germany

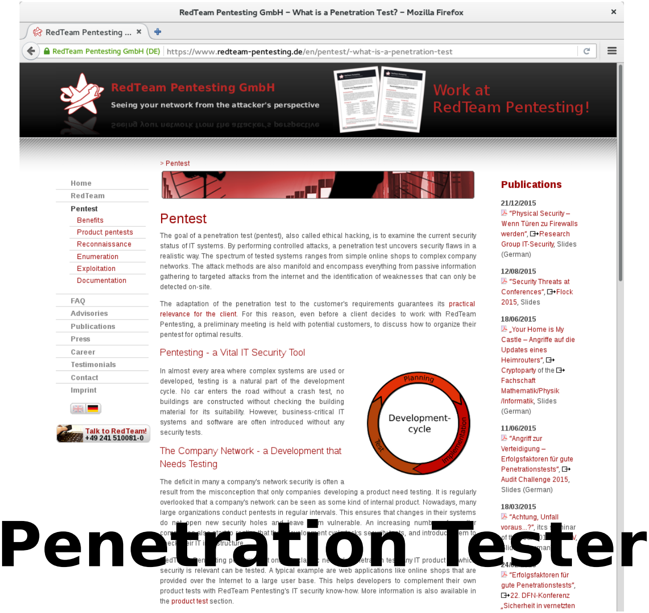
Original
Nobis-Printen
aus
Aachen
Schokolade-Nuss Printen-Bruch
Kräuter-Mandel Bruch-Printen
Prinzess Printen
Schokolade-Nuss-Printen
Kräuter-Printen-Bruch



User:Till

Till Maas	
Personal Information	
Home:	Aachen, Germany
Fedora Information	
FAS name:	till
Fedora email:	till@fedoraproject.org
IRC nick:	tyll
IRC channels:	#fedora-releng[?] #fedora-admin[?] #fedora-apps[?] #fedora-devel[?] #epel[?] #fedora-de[?]
Fedorapeople page:	https://till.fedorapeople.org
Miscellaneous Information	
Private email:	opensource@till.name
GPG key:	E3D6 A361 94E0 A6F2 C5F0 6A3A 10B3 1C10 9517 18A0 E3D6 A361 94E0 A6F2 C5F0 6A3A 10B3 1C10 9517
Homepage:	http://blog.till.name
Jabber:	till@jabber.ccc.de
Twitter:	https://twitter.com/@TillMaas

Packager, Patcher, Release Engineer, ...



Pentest

The goal of a penetration test (pentest), also called ethical hacking, is to examine the current security status of IT systems. By performing controlled attacks, a penetration test uncovers security flaws in a realistic way. The spectrum of tested systems ranges from simple online shops to complex company networks. The attack methods are also manifold and encompass everything from passive information gathering to targeted attacks from the internet and the identification of weaknesses that can only be detected on-site.

The adaptation of the penetration test to the customer's requirements guarantees its practical relevance for the client. For this reason, even before a client decides to work with RedTeam Pentesting, a preliminary meeting is held with potential customers, to discuss how to organize their pentest for optimal results.

Pentesting - a Vital IT Security Tool

In almost every area where complex systems are used or developed, testing is a natural part of the development cycle. No car enters the road without a crash test, no buildings are constructed without checking the building material for its suitability. However, business-critical IT systems and software are often introduced without any security tests.

The Company Network - a Development that Needs Testing

The deficit in many a company's network security is often a result from the misconception that only companies developing a product need testing. It is regularly overlooked that a company's network can be seen as some kind of internal product. Nowadays, many large organizations conduct pentests in regular intervals. This ensures that changes in their systems do not open new security holes and leave them vulnerable. An increasing number of smaller companies also start to realize that their development cycle lacks security tests, and introduce them to check their IT infrastructure.

RedTeam Pentesting performs not only classic network penetration tests: any IT product for which security is relevant can be tested. A typical example are web applications like online shops that are provided over the Internet to a large user base. This helps developers to complement their own product tests with RedTeam Pentesting's IT security know-how. More information is also available in the product test section.

Publications

21/12/2015
"Physical Security – Wenn Türen zu Firewalls werden", Research Group IT-Security, Slides (German)

12/08/2015
"Security Threats at Conferences", Flock 2015, Slides

18/06/2015
„Your Home is My Castle – Angriffe auf die Updates eines Heimrouters", Cryptoparty of the Fachschaft Mathematik/Physik /Informatik, Slides (German)

11/06/2015
"Angriff zur Verteidigung – Erfolgsfaktoren für gute Penetrationstests", Audit Challenge 2015, Slides (German)

18/03/2015
"Achtung, Unfall voraus...?", itcs seminar of the [illegible] V, Slides (German)

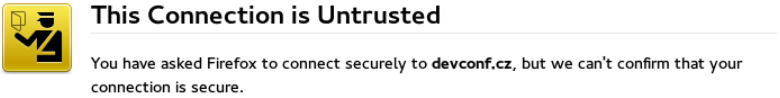
24/02/2015
"Erfolgsfaktoren für gute Penetrationstests", 22. DFN-Konferenz „Sicherheit in vernetzten

Penetration Tester

Transport Layer Security

HTTPS
IMAPS
SMTPS
FTPS

TLS Certificates

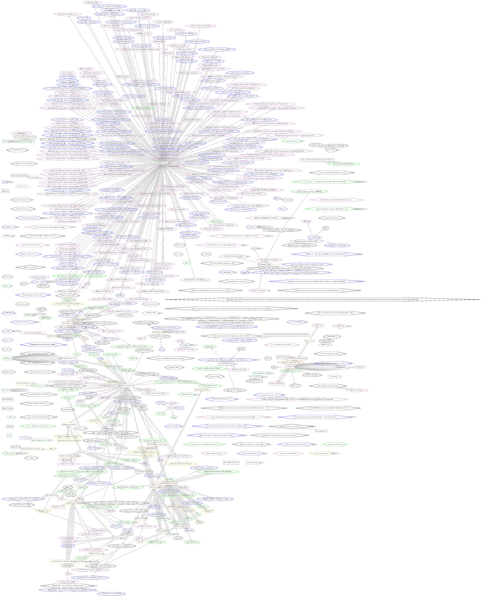


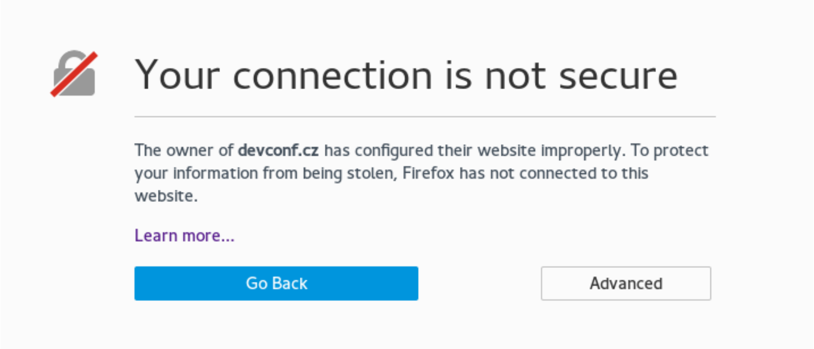
This Connection is Untrusted

You have asked Firefox to connect securely to **devconf.cz**, but we can't confirm that your connection is secure.

Certificate Authority (CA)

202

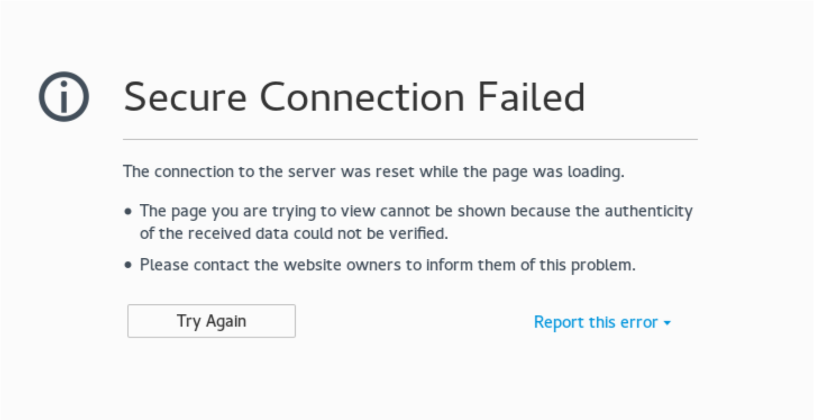




Your connection is not secure

The owner of **devconf.cz** has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

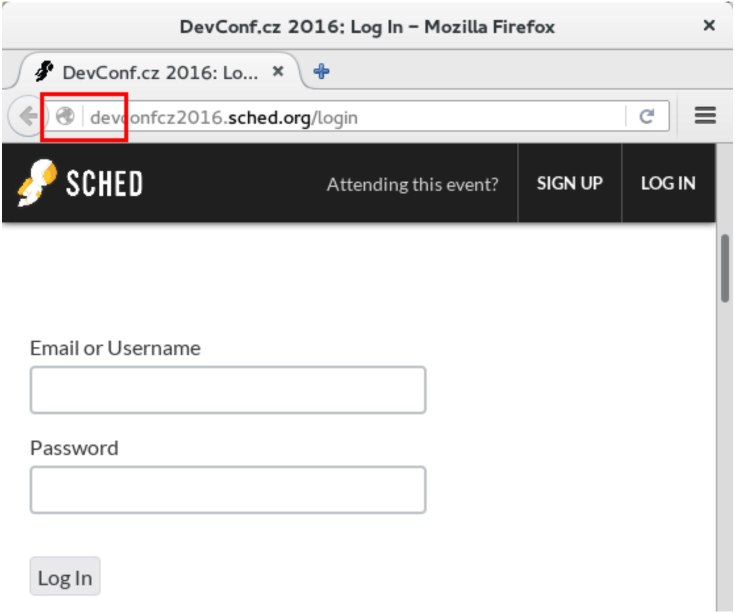
Learn more…



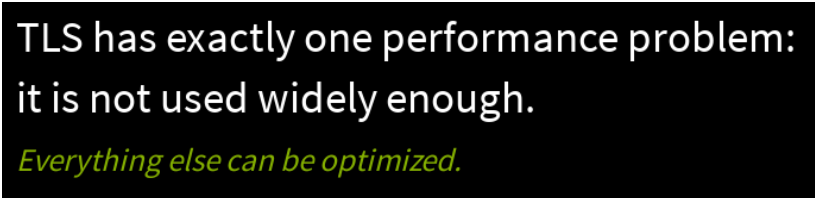
Secure Connection Failed

The connection to the server was reset while the page was loading.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.



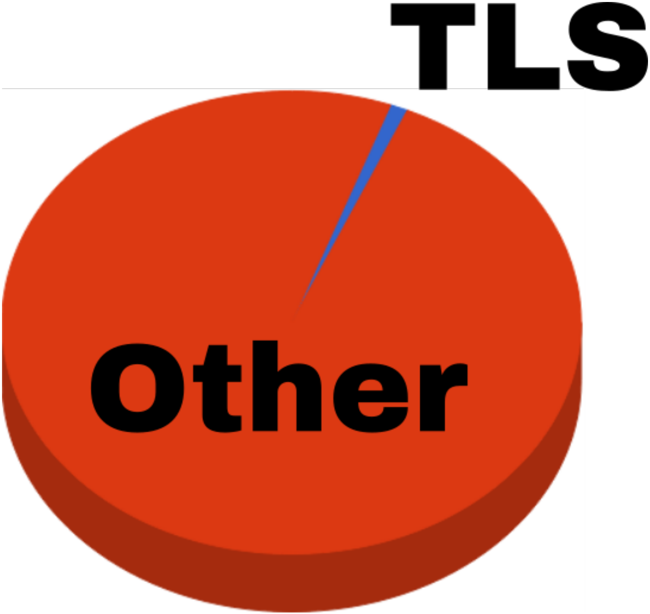
DevConf.cz 2016: Log In – Mozilla Firefox
DevConf.cz 2016: Lo...
devconfcz2016.sched.org/login
SCHED
Attending this event?
SIGN UP
LOG IN
Email or Username
Password
Log In

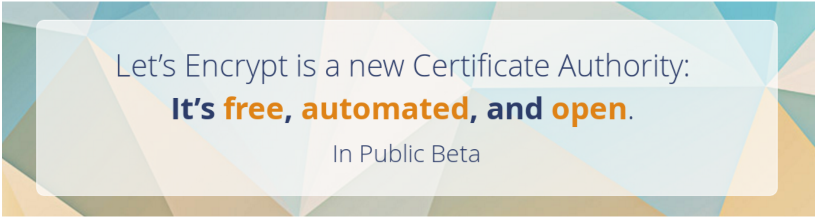


TLS has exactly one performance problem: it is not used widely enough.

Everything else can be optimized.

istlsfastyet.com

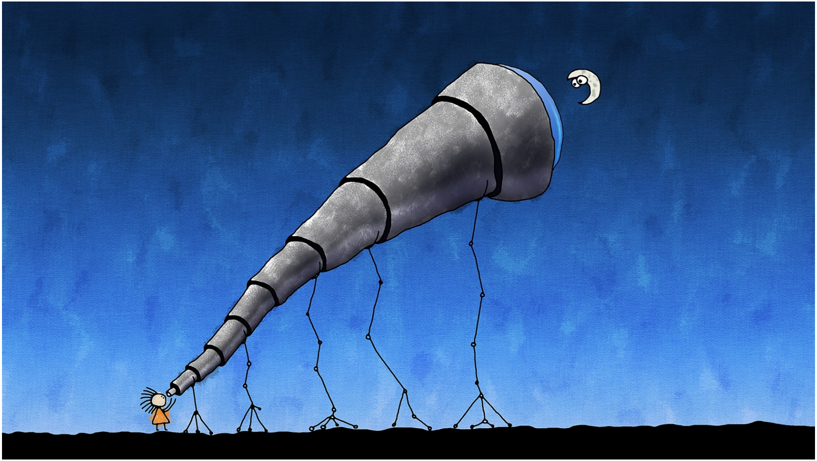

TLS
Other

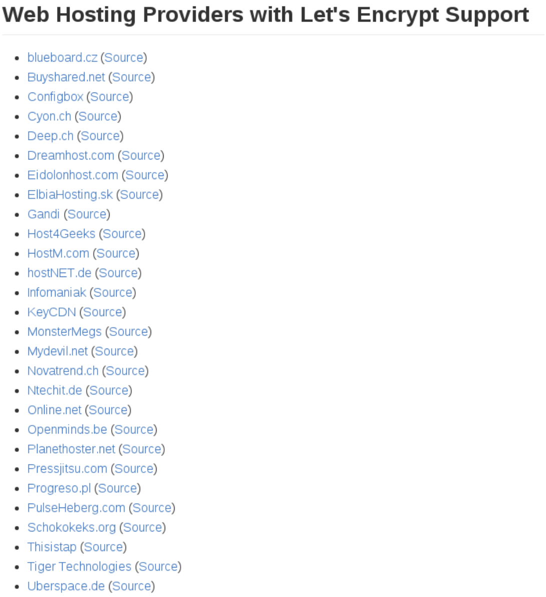


Let's Encrypt is a new Certificate Authority:

It's free, automated, and open.

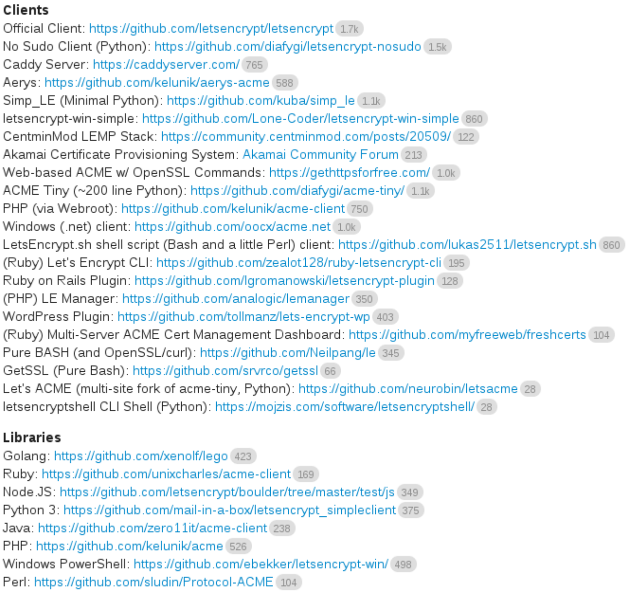
In Public Beta





Web Hosting Providers with Let's Encrypt Support

- blueboard.cz (Source)
- Buyshared.net (Source)
- Configbox (Source)
- Cyon.ch (Source)
- Deep.ch (Source)
- Dreamhost.com (Source)
- Eidolonhost.com (Source)
- ElbiaHosting.sk (Source)
- Gandi (Source)
- Host4Geeks (Source)
- HostM.com (Source)
- hostNET.de (Source)
- Infomaniak (Source)
- KeyCDN (Source)
- MonsterMegs (Source)
- Mydevil.net (Source)
- Novatrend.ch (Source)
- Ntechit.de (Source)
- Online.net (Source)
- Openminds.be (Source)
- Planethoster.net (Source)
- Pressjitsu.com (Source)
- Progreso.pl (Source)
- PulseHeberg.com (Source)
- Schokokeks.org (Source)
- Thisistap (Source)
- Tiger Technologies (Source)
- Uberspace.de (Source)

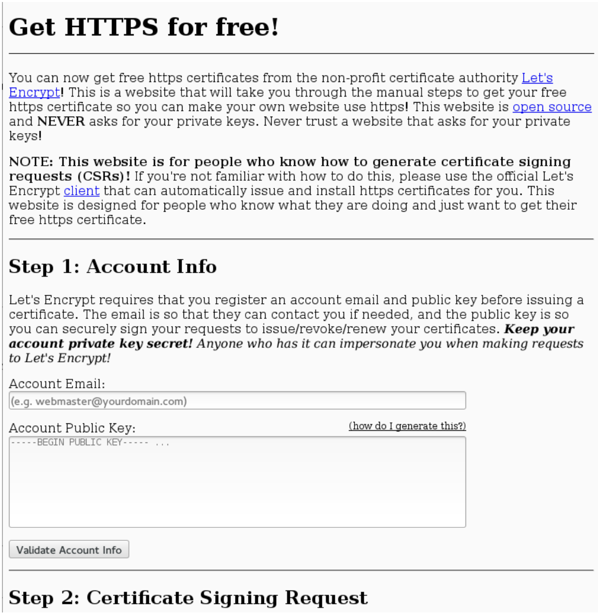


Clients

Official Client: https://github.com/letsencrypt/letsencrypt 1.7k
No Sudo Client (Python): https://github.com/diafygi/letsencrypt-nosudo 1.5k
Caddy Server: https://caddyserver.com/ 765
Aerys: https://github.com/kelunik/aerys-acme 588
Simp_LE (Minimal Python): https://github.com/kuba/simp_le 1.1k
letsencrypt-win-simple: https://github.com/Lone-Coder/letsencrypt-win-simple 860
CentminMod LEMP Stack: https://community.centminmod.com/posts/20509/ 122
Akamai Certificate Provisioning System: Akamai Community Forum 213
Web-based ACME w/ OpenSSL Commands: https://gethttpsforfree.com/ 1.0k
ACME Tiny (~200 line Python): https://github.com/diafygi/acme-tiny/ 1.1k
PHP (via Webroot): https://github.com/kelunik/acme-client 750
Windows (.net) client: https://github.com/oocx/acme.net 1.0k
LetsEncrypt.sh shell script (Bash and a little Perl) client: https://github.com/lukas2511/letsencrypt.sh 860
(Ruby) Let's Encrypt CLI: https://github.com/zealot128/ruby-letsencrypt-cli 195
Ruby on Rails Plugin: https://github.com/lgromanowski/letsencrypt-plugin 128
(PHP) LE Manager: https://github.com/analogic/lemanager 350
WordPress Plugin: https://github.com/tollmanz/lets-encrypt-wp 403
(Ruby) Multi-Server ACME Cert Management Dashboard: https://github.com/myfreeweb/freshcerts 104
Pure BASH (and OpenSSL/curl): https://github.com/Neilpang/le 345
GetSSL (Pure Bash): https://github.com/srvrco/getssl 66
Let's ACME (multi-site fork of acme-tiny, Python): https://github.com/neurobin/letsacme 28
letsencryptshell CLI Shell (Python): https://mojzis.com/software/letsencryptshell/ 28

Libraries

Golang: https://github.com/xenolf/lego 423
Ruby: https://github.com/unixcharles/acme-client 169
Node.JS: https://github.com/letsencrypt/boulder/tree/master/test/js 349
Python 3: https://github.com/mail-in-a-box/letsencrypt_simpleclient 375
Java: https://github.com/zero11it/acme-client 238
PHP: https://github.com/kelunik/acme 526
Windows PowerShell: https://github.com/ebekker/letsencrypt-win/ 498
Perl: https://github.com/sludin/Protocol-ACME 104



Get HTTPS for free!

You can now get free https certificates from the non-profit certificate authority Let's Encrypt! This is a website that will take you through the manual steps to get your free https certificate so you can make your own website use https! This website is open source and **NEVER** asks for your private keys. Never trust a website that asks for your private keys!

NOTE: This website is for people who know how to generate certificate signing requests (CSRs)! If you're not familiar with how to do this, please use the official Let's Encrypt client that can automatically issue and install https certificates for you. This website is designed for people who know what they are doing and just want to get their free https certificate.

Step 1: Account Info

Let's Encrypt requires that you register an account email and public key before issuing a certificate. The email is so that they can contact you if needed, and the public key is so you can securely sign your requests to issue/revoke/renew your certificates. ***Keep your account private key secret!** Anyone who has it can impersonate you when making requests to Let's Encrypt!*

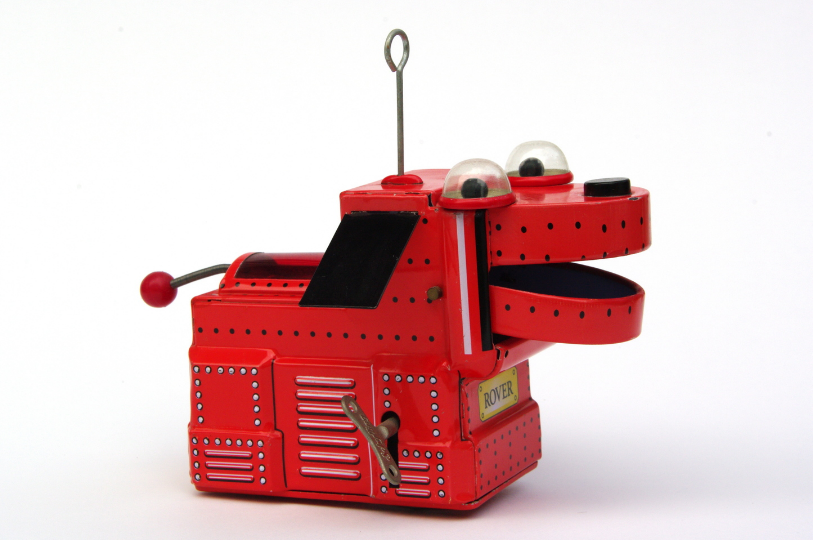
Account Email:

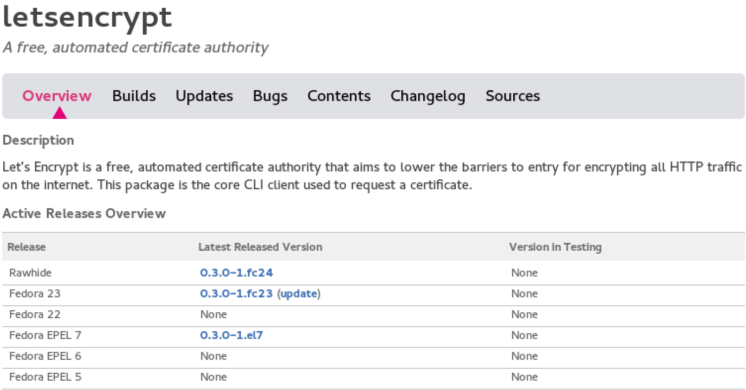
(e.g. webmaster@yourdomain.com)

Account Public Key:

```
-----BEGIN PUBLIC KEY----- ...
```

Step 2: Certificate Signing Request


ROVER



letsencrypt

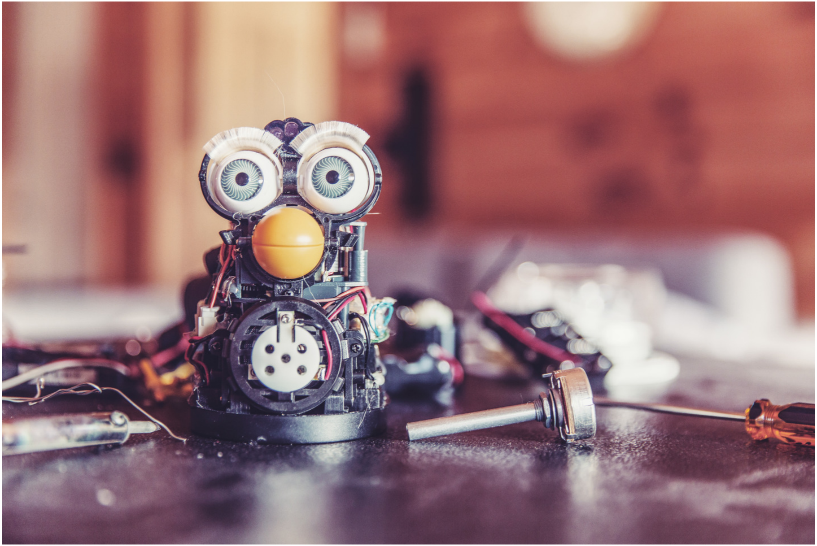
A free, automated certificate authority

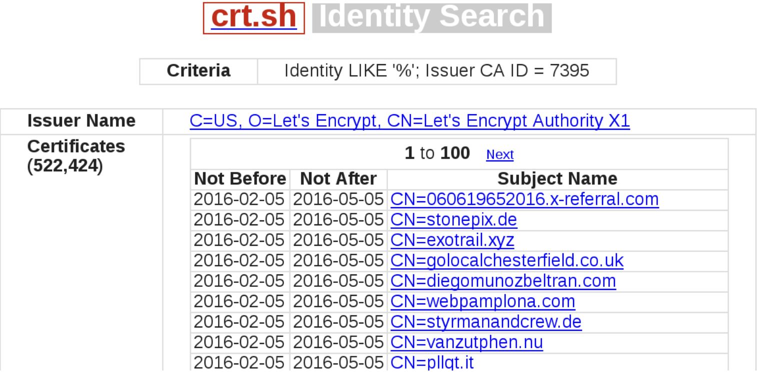
Description

Let's Encrypt is a free, automated certificate authority that aims to lower the barriers to entry for encrypting all HTTP traffic on the internet. This package is the core CLI client used to request a certificate.

Active Releases Overview

Release	Latest Released Version	Version in Testing
Rawhide	0.3.0-1.fc24	None
Fedora 23	0.3.0-1.fc23 (update)	None
Fedora 22	None	None
Fedora EPEL 7	0.3.0-1.el7	None
Fedora EPEL 6	None	None
Fedora EPEL 5	None	None





crt.sh Identity Search

Criteria	Identity LIKE '%'; Issuer CA ID = 7395

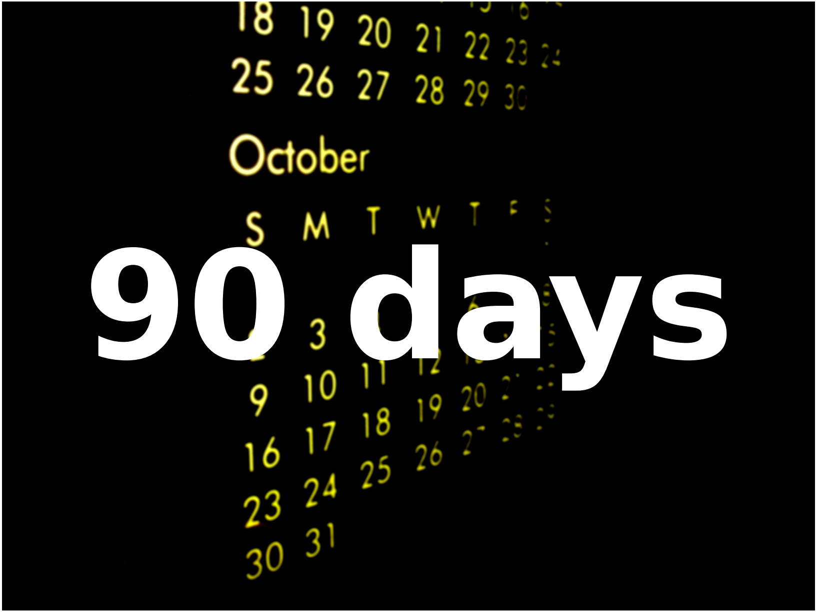
Issuer Name C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1

Certificates (522,424)

1 to **100** Next

Not Before	Not After	Subject Name
2016-02-05	2016-05-05	CN=060619652016.x-referral.com
2016-02-05	2016-05-05	CN=stonepix.de
2016-02-05	2016-05-05	CN=exotrail.xyz
2016-02-05	2016-05-05	CN=golocalchesterfield.co.uk
2016-02-05	2016-05-05	CN=diegomunozbeltran.com
2016-02-05	2016-05-05	CN=webpamplona.com
2016-02-05	2016-05-05	CN=styrmanandcrew.de
2016-02-05	2016-05-05	CN=vanzutphen.nu
2016-02-05	2016-05-05	CN=pllqt.it

5 certificates in 7 days per domain
100 hostnames per certificate



90 days

```
// DynDNS.com : http://www.dyndns.com/services/dns/dyndns/
dyndns-at-home.com
dyndns-at-work.com
dyndns-blog.com
dyndns-free.com
dyndns-home.com
dyndns-ip.com
dyndns-mail.com
dyndns-office.com
dyndns-pics.com
dyndns-remote.com
dyndns-server.com
dyndns-web.com
dyndns-wiki.com
dyndns-work.com
dyndns.biz
dyndns.info
dyndns.org
dyndns.tv
```

publicsuffix.org

No:

organization validated (OV)

extended validated (EV)

Code signing

.mil

IP addresses

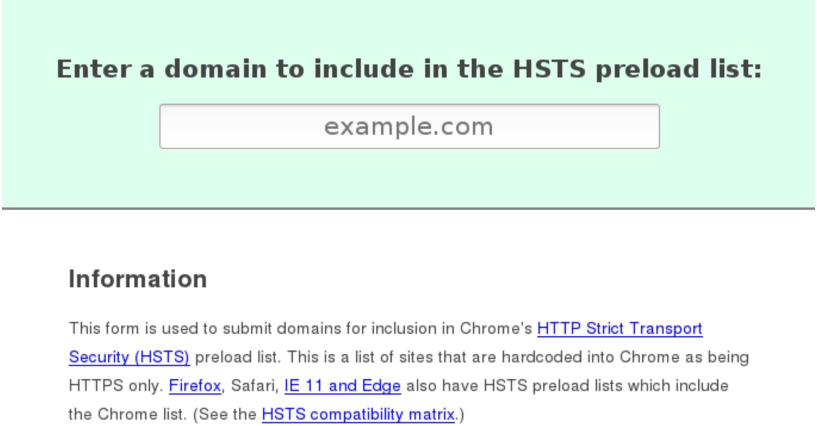
wildcard (*.example.com)
International Domain Names
ECC
S/MIME

Java
Android 2.3.5
Windows XP
Blackberry

https://

Upgrade Insecure Requests

Strict Transport Security



Enter a domain to include in the HSTS preload list:

example.com

Information

This form is used to submit domains for inclusion in Chrome's HTTP Strict Transport Security (HSTS) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only. Firefox, Safari, IE 11 and Edge also have HSTS preload lists which include the Chrome list. (See the HSTS compatibility matrix.)

hstspreload.appspot.com

ONE WAY

ANSSI

CNNIC/MCS Holdings

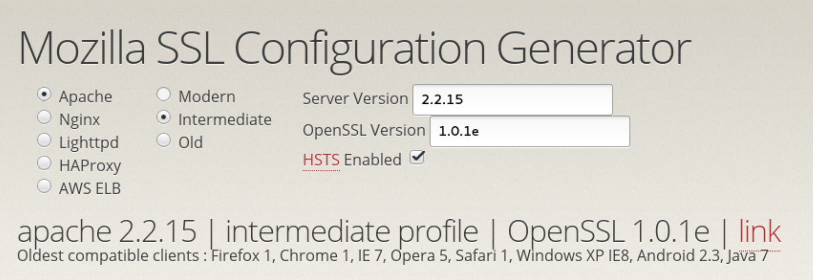
DigiNotar

eDellRoot

SuperFish

Symantec

Public Key Pinning



Mozilla SSL Configuration Generator

- ● Apache
- ○ Nginx
- ○ Lighttpd
- ○ HAProxy
- ○ AWS ELB

- ○ Modern
- ● Intermediate
- ○ Old

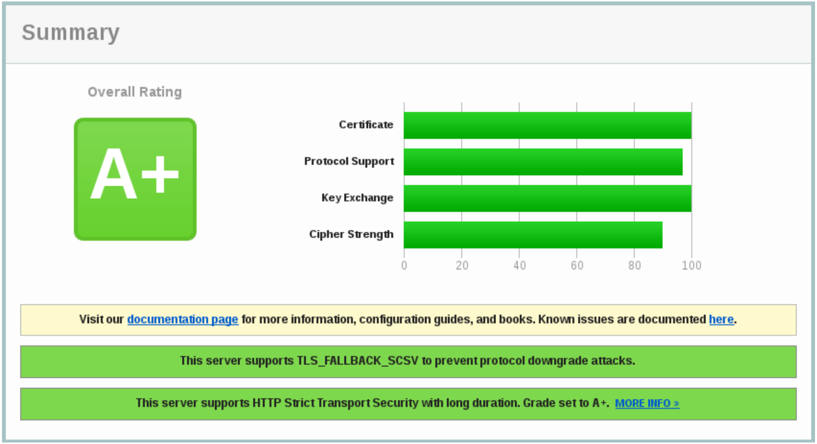
Server Version: 2.2.15

OpenSSL Version: 1.0.1e

HSTS Enabled ☑

apache 2.2.15 | intermediate profile | OpenSSL 1.0.1e | link

Oldest compatible clients : Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7



Summary

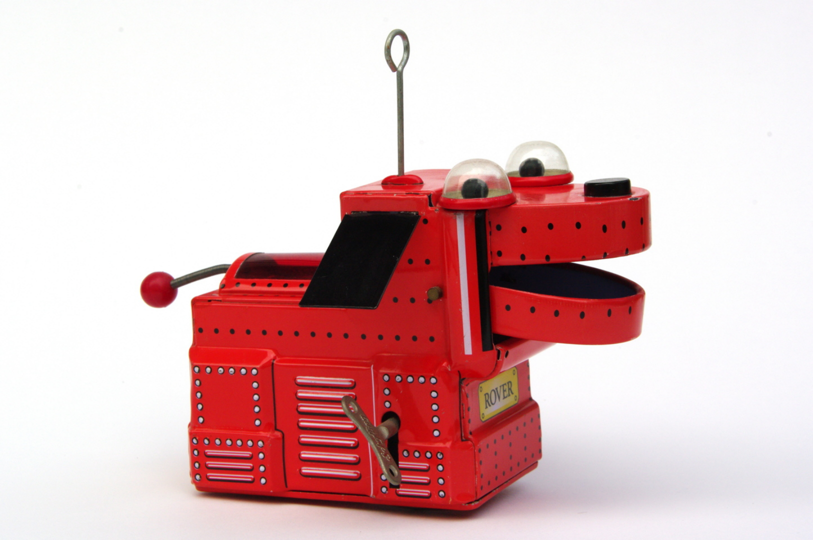
Overall Rating

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

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

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

www.ssllabs.com/ssltest


ROVER

Thank you OpenStreetMap:
World map - Data, imagery and map information provided by MapQuest,
OpenStreetMap
<http://www.openstreetmap.org/copyrigh>
and contributors, ODbL
<http://wiki.openstreetmap.org/wiki/Legal_FAQ#3a._I_would_like_to_use_OpenStreetMap_maps._How_should_I_credit_you.3F>.

Thank you image providers:
https://www.flickr.com/photos/
compujeramey/168102810 - railroad track - Jeramey Jannene - Railroad Track - by/2.0
tiffini/4129317099 - passport stamps - tiffini - Passport - by/2.0
diekatrin/4199009279/ - printen - Katrin Gilger - Printenbäckerei I - by-sa/2.0

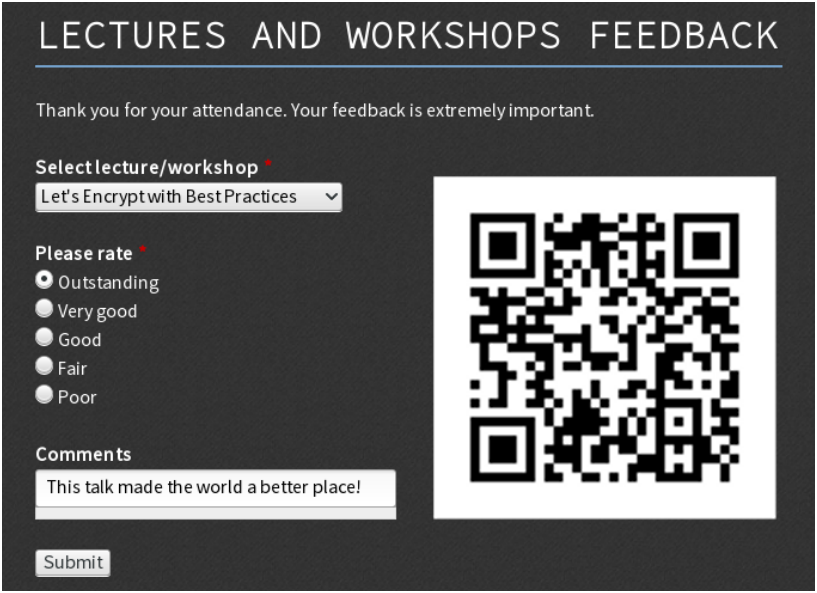
https://www.eff.org/files/colour_map_of_cas.pdf - EFF - - by/3.0/us

http://pixabay.com/
http://morguefile.com/
http://gratisography.com/

Thank you creative commons:
https://creativecommons.org/licenses/
by/2.0/
by/3.0/us
by-sa/2.0/
zero/1.0

Made with pinpoint and TexLive:
https://github.com/GNOME/pinpoint
https://www.tug.org/texlive/

Thank you!



LECTURES AND WORKSHOPS FEEDBACK

Thank you for your attendance. Your feedback is extremely important.

Select lecture/workshop *

Let's Encrypt with Best Practices

Please rate *

- ● Outstanding
- ○ Very good
- ○ Good
- ○ Fair
- ○ Poor

Comments

This talk made the world a better place!

```
Feedback: http://www.devconf.cz/feedback/318 or @TillMaas

pub   4096R/6A3A10B31C109517 2007-06-22 [expires: 2021-05-23]
      Key fingerprint = 18A0 E3D6 A361 94E0 A6F2  C5F0 6A3A 10B3 1C10 9517
uid                          Till Maas <till.maas@till.name>
uid                          Till Maas <opensource@till.name>
uid                          Till Maas <till@fedoraproject.org>
sub   4096R/F4AA50CBB5098148 2007-06-22 [expires: 2021-05-23]
```

Let's Encrypt Client Implementations: https://goo.gl/hSmZf2
Web Hosting Providers using Let's Encrypt: https://goo.gl/J1okbA
JavaScript Client: https://gethttpsforfree.com

https://github.com/letsencrypt
Automated Certificate Management Environment (acme)
https://datatracker.ietf.org/wg/acme/documents/
Mozilla SSL Configuration Editor: https://goo.gl/SYriUV