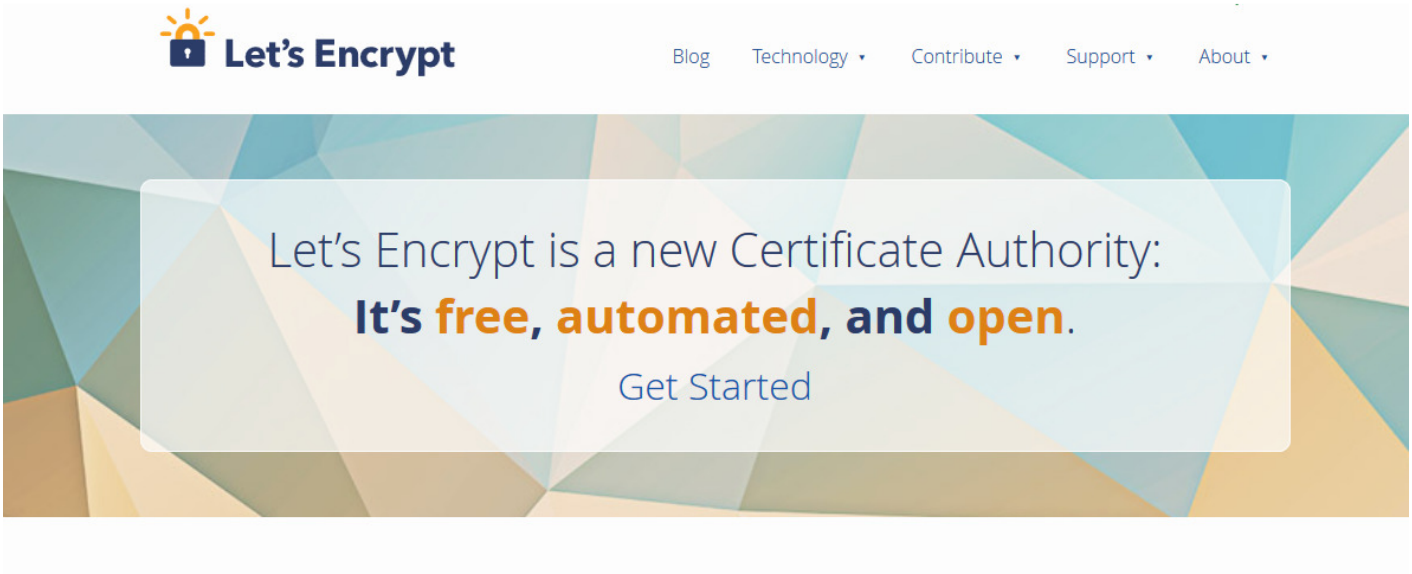
Lasst uns verschlüsseln: Kostenlose TLS Zertifikate für alle

Kategorien : Open Source

Schlagwörter : r23.de intern, WordPress

Datum : 17. Mai 2016



Sicherheit wird bei uns großgeschrieben. Wir haben für unseren Blog nun die SSL Verschlüsselung eingerichtet und erklären euch wie es funktioniert.

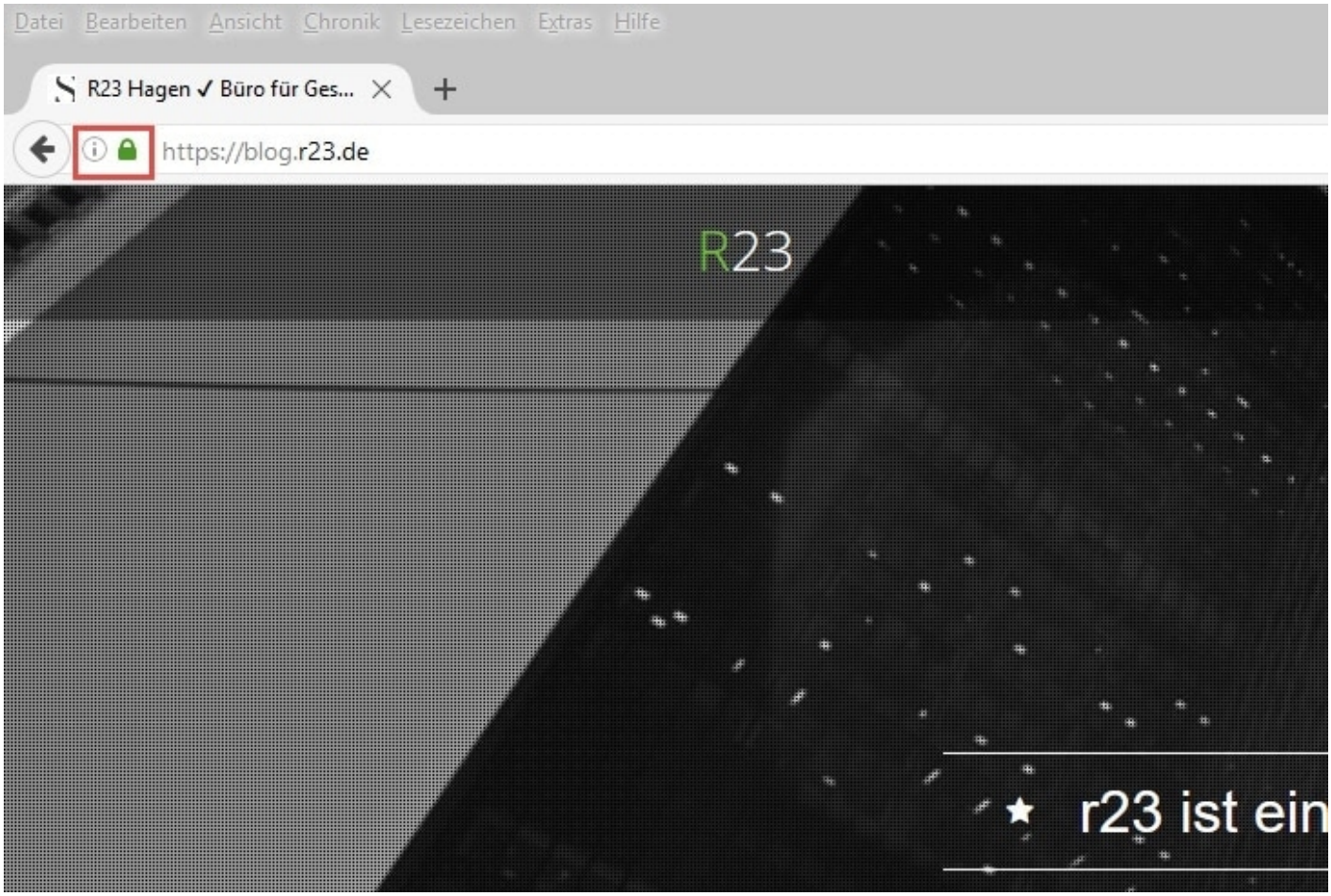
Was bedeutet SSL Verschlüsselung?

Secure Sockets Layer, die alte Bezeichnung für **Transport Layer Security**, ein Netzwerkprotokoll zur sicheren Übertragung von Daten.

Transport Layer Security (TLS), weitläufiger bekannt unter der Vorgängerbezeichnung **Secure Sockets Layer** (SSL), ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert.

Wie kann ich feststellen, ob meine Verbindung zum Blog verschlüsselt erfolgt?

Beim Besuch einer sicheren Webseite wird in der Adressleiste die Schaltfläche zur Webseitenidentität (ein Sperrschloss) angezeigt. Damit könnt ihr schnell feststellen, ob die Verbindung zur gerade angezeigten Website verschlüsselt ist. Das soll dir dabei helfen, bösartige Seiten zu erkennen und zu vermeiden, dass diese an deine persönlichen Daten gelangen.



Die Schaltfläche zur Webseitenidentität befindet sich in der Adressleiste links neben der Adresse. Meistens zeigt diese Schaltfläche beim Betrachten einer sicheren Webseite ein grünes Sperrschloss.

In seltenen Fällen kann aber auch ein grünes Sperrschloss mit grauem Warndreieck, ein graues

Sperrschloss mit gelbem Warndreieck oder ein rot durchgestrichenes graues Sperrschloss angezeigt werden.

Achtung: Gebe niemals sensible Informationen (Bankdaten, Kreditkarteninformationen, Versicherungsnummern usw.) an Webseiten ohne das Sperrschloss-Symbol in der Adressleiste - in diesem Fall ist weder sichergestellt, dass du auch wirklich mit der beabsichtigten Webseite kommunizierst, noch ist die Verbindung abhörsicher!

Grünes Sperrschloss

Ein grünes Sperrschloss bedeutet:

- Du bist mit Sicherheit mit jener Website verbunden, deren Adresse in der Adressleiste angezeigt wird, und die Verbindung wurde nicht abgefangen.
- Die Verbindung zwischen Webbrowser und der Website erfolgt verschlüsselt, um deren Abhören zu verhindern.

Anleitung für Let’s Encrypt: Kostenlose TLS Zertifikate für alle

Let’s Encrypt ist eine Zertifizierungsstelle, die Ende 2015 in Betrieb gegangen ist und kostenlose X.509-Zertifikate für Transport Layer Security (TLS) anbietet. Dabei ersetzt ein automatisierter Prozess die bisher gängigen komplexen händischen Vorgänge bei der Erstellung, Validierung, Signierung, Einrichtung und Erneuerung von Zertifikaten für verschlüsselte Websites.

Let’s Encrypt ist ein von der gemeinnützigen Internet Security Research Group (ISRG) angebotener Dienst. Hauptsponsoren sind die Electronic Frontier Foundation (EFF), die Mozilla Foundation, Akamai und Cisco Systems. Weitere Beteiligte sind die Zertifizierungsstelle IdenTrust, die University of Michigan (U-M), die Stanford Law School, die Linux Foundation sowie Stephen Kent von Raytheon/BBN Technologies und Alex Polvi von CoreOS.

Für den Erhalt eines Zertifikats sind nur wenige, einfache Schritte erforderlich, die ich im Folgenden erkläre:

Let’s Encrypt nutzt ein Protokoll namens „ACME“ zur Kommunikation mit den CA-Servern. Ich

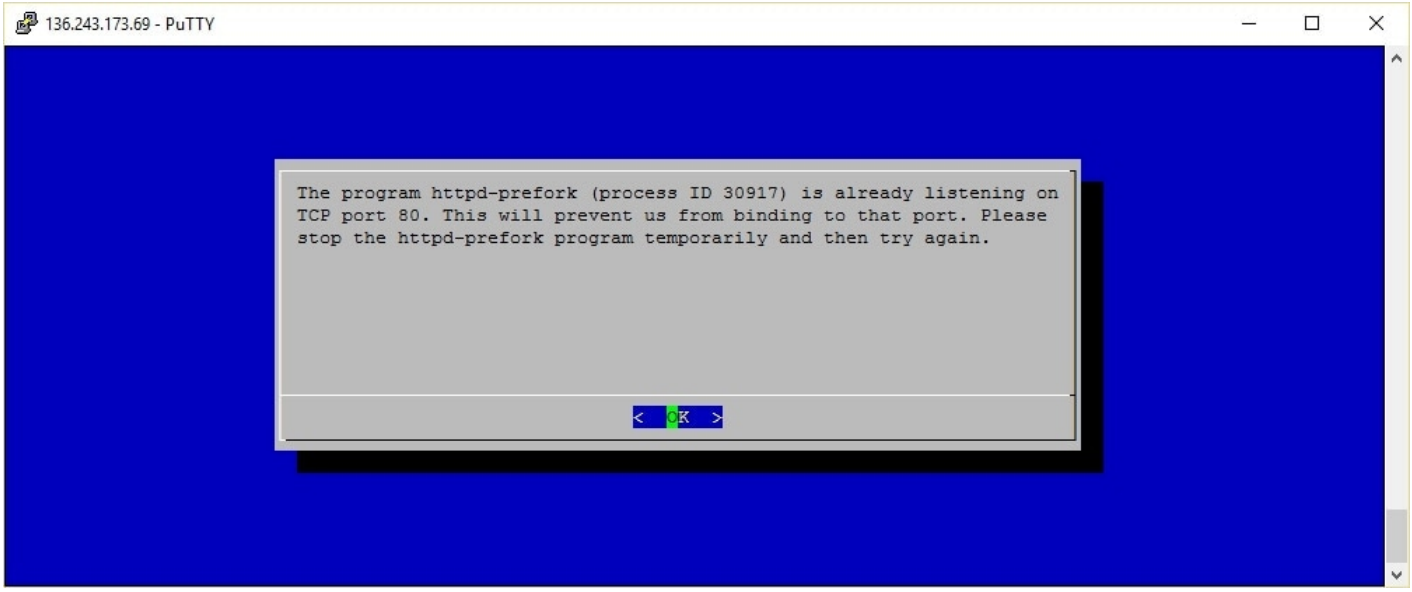
habe den Referenz-ACME-Client „Certbot“ von LE genutzt – um den soll es hier gehen. Außerdem wird der Client in dieser Anleitung direkt auf dem Zielserver ausgeführt – das ist die einfachere Methode.

Certbot ACME-Client installieren

Schaltet euch (als root!) via SSH auf euren Server auf und installiert zuerst Certbot:

cd opt
git clone https://github.com/certbot/certbot
cd certbot

Let’s Encrypt Zertifikate abholen



Bevor der Client gestartet werden kann, muss der Webserver auf dem Host kurz abgeschaltet

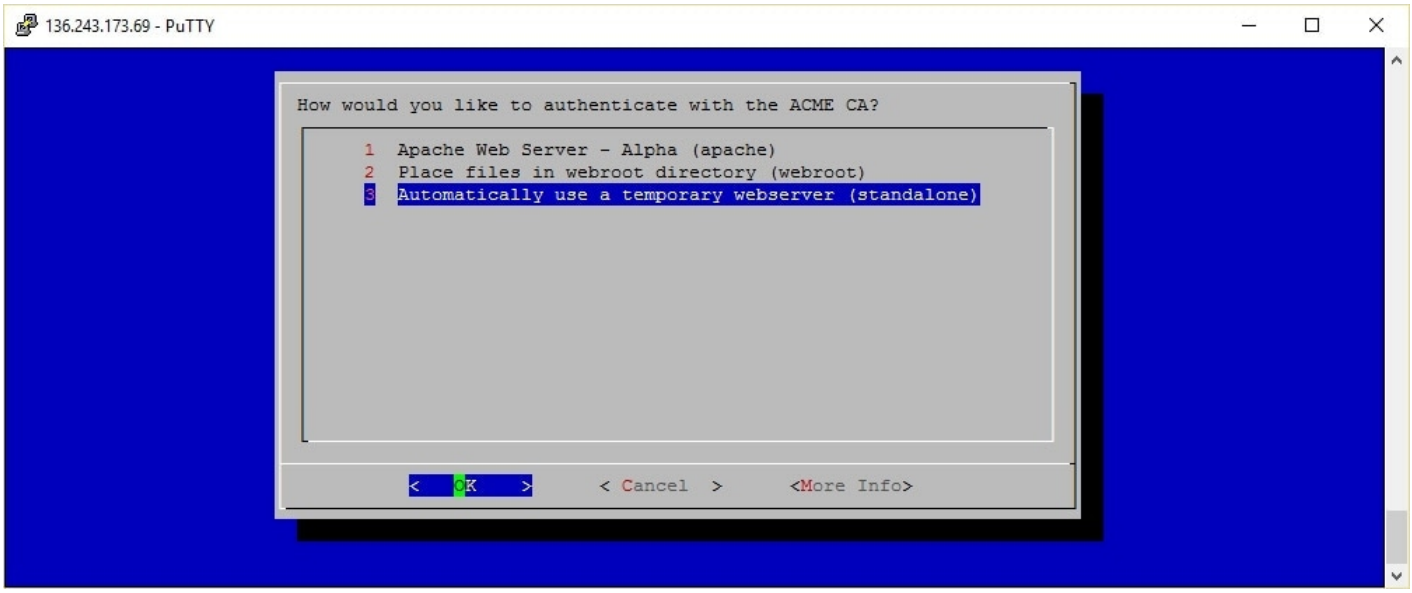
werden, damit Port 80 für den Certbot zur Verfügung steht. Danach kann es mit der Zertifikatsanfrage weitergehen:

./certbot-auto certonly --standalone --rsa-key-size 4096 -d blog.r23.de

Die „certonly“ Option sorgt dafür, dass die Zertifikate nur abgeholt und gespeichert werden.

Mit dem –rsa-key-size Parameter wird die Länge für den zu generierenden RSA Private Key auf 4096 Bits gesetzt (statt der standardmäßig gesetzten 2048 Bit).

Danach folgt mit „-d“ die Domains, für die das Zertifikat gelten soll.



IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at /etc/letsencrypt/live/[domain]/fullchain.pem. Your cert will expire on [Datum]. To obtain a new version of the certificate in the future, simply run Certbot again.

- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
Donating to EFF: https://eff.org/donate-le

Nach Eingabe der E-Mail Adresse und der Zustimmung zu den Nutzungsbedingungen wird das gewünschte Zertifikat vom ACME-Server abgeholt und in /etc/letsencrypt/live/[domain] gespeichert. Dort liegen vier verschiedene Dateien:

- cert.pem (Das öffentliche Zertifikat in Reinform)
- chain.pem (Öffentliches Zertifikat aus der sog. Keychain)
- fullchain.pem (entspricht cert.pem + chain.pem)
- privkey.pem (Der private Schlüssel)

Welches Zertifikat nun wofür? Das hängt vom Webserver ab. Mein Webserver benötigt nur zwei Zertifikatsdateien: Das öffentliche Zertifikat inkl. Keychain (fullchain.pem) und das den privaten Schlüssel (privkey.pem). Die Apache-Konfiguration sieht also so aus:

```
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/letsencrypt/live/[domain]/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/[domain]/privkey.pem
```

Eine vollständige Dokumentation findet ihr hier: https://certbot.eff.org/docs/

Nachdem die Webserver-Konfiguration angepasst wurde, könnt ihr den Webserver wieder starten und prüfen, ob die TLS-Zertifikate funktionieren.

Bei WordPress die Domain ändern

Durch die TLS-Zertifikate ändert sich die Adresse einer WordPress-Webseite von https://blog.r23.de nach https://blog.r23.de

Es gibt verschiedene Wege eine Domain-Änderung mit einer WordPress-Webseite zu lösen und einige Dinge sind dabei zu beachten.

Probleme bereiten manche Widgets, die nicht nur URLs speichern, sondern auch deren Länge. Ändert sich die URL, die Länge passt aber nicht mehr dazu, ist das Widget unbrauchbar. Um dieses Problem zu umgehen, kann man zum Beispiel das Plugin *UpdraftPlus - Backup/Restore* mit der kostenpflichtigen Erweiterung *Migrate a WordPress site to a different location* verwenden.

Von diesem WordPress Plug-in erhält man eine Log über die Änderungen:

> 0000.009 () Opened log file at time: Sun, 15 May 2016 04:41:05 +0000 on https://blog.r23.de
> 0000.009 () UpdraftPlus WordPress backup plugin (https://updraftplus.com): 2.12.9.1 WP: 4.x.x PHP: 7.x.x ....
> 0000.009 () Free space on disk containing Updraft's temporary directory: ....
> 0000.014 () Restore job started. Entities to restore: db. Restore options: {"updraft_restorer_replacesiteurl":true,"updraft_encryptionphrase":"","updraft_restorer_wpcore_includewpconfig":false}
> 0000.420 () Entity: db
> 0000.420 () restore_backup(backup_file=backup_2016-05-15-0536_PopArt_Portraits_und_mehr_von_r_cc98a140c4b6-db.gz, type=db, info=a:0:{}, last_one=1)
> 0000.421 () Entpacke Sicherung...
> 0000.511 () Database successfully unpacked
> 0000.511 () Stelle Datenbank wieder her (bei großen Seiten kann das dauern - wenn der Vorgang in einen Timeout läuft (was passieren kann wenn dein Webhoster die Ressourcen limitiert) solltest du andere Methoden, wie z.B. phpMyAdmin, nutzen) ...
> 0000.511 () Using direct MySQL access; value of use_mysqli is: 1
> 0000.512 () Max packet size: ...
> 0000.512 () Entering maintenance mode
> 0000.512 () Anschalten des Wartungsmodus…
> 0000.513 () **Backup of:** https://blog.r23.de
> 0000.513 () Site home: https://blog.r23.de
> 0000.513 () Content URL: https://blog.r23.de/wp-content
> 0000.513 () Uploads URL: https://blog.r23.de/wp-content/uploads
> 0000.513 () Old table prefix: ....
> ...
> 004.021 () Search and replacing table: ..._postmeta: rows: 389
> 0005.924 () Restoring table (InnoDB): ..._posts
> 0013.987 () Skipping search/replace on GUID column in posts table
> ...
> 0049.830 () Finished: lines processed: 204 in 49.32 seconds
> 0049.830 () Räume auf ...

0049.831 () Begin search and replace (updraftplus_restored_db)
0049.832 () Restored pre-migration site ID for this installation
0049.853 () Database search and replace: replace https://blog.r23.de in backup dump with https://blog.r23.de
0049.853 () Database search and replace: replace https://blog.r23.de in backup dump with https://blog.r23.de
...
0049.854 () Search and replacing table: ..._options: already done
...
0049.886 () Restore successful!
0049.886 () Restore successful

https://codex.wordpress.org/Changing_The_Site_URL

Jetzt bist du gefragt!

Falls Ihr noch Fragen zum Ablauf habt oder auf Probleme stoßt, die nicht erwähnt werden, hinterlasst einen Kommentar zum Artikel.

Du kannst diesen Beitrag natürlich auch weiterempfehlen. Wir sind dir für jede Unterstützung dankbar!

Verwandeln Sie Ihren Commerce mit AR und 3D-Produktvisualisierung!

Bei uns geht es um Techniken, die es schaffen, das Produkt zum Erlebnis zu machen. Virtual & Augmented Reality, 360 Grad-Videos, Darstellungen in 3D, virtuelle Showrooms. Die Besucher:innen sollen eintauchen in die Welt des Unternehmens mit immersiven Technologien.

Sie können uns mit der Erstellung von individuellen 3D-Visualisierungen beauftragen. Jeder kann 3D-Visualisierungen bei unserem Kreativservice bestellen - unabhängig davon, ob Sie nur ein einzelnes 3D-Modell benötigen oder viele.

Wir unterstützen Sie bei der Umsetzung Ihres Augmented Reality (AR) oder Virtual Reality (VR) Projektes! Egal ob Produktfotografie, 3D-Scan-Service, 3D-Visualisierung oder fertige 3D-Modelle für AR/VR – wir beraten Sie persönlich und unverbindlich.

Wo kann ich Anregungen, Lob oder Kritik äußern?

Ihre Meinung ist uns wichtig! Schreiben Sie uns, was Ihnen in Bezug auf unser Angebot bewegt.
info@r23.de

R23 — Ihr Atelier für Virtual Reality und interaktive Markenerlebnisse

Wünschen Sie ein individuelles Angebot auf Basis Ihrer aktuellen Vorlagen, nutzen Sie einfach unser **Anfrageformular**.

Lasst uns verschlüsseln: Kostenlose TLS Zertifikate für alle

https://blog.r23.de/software/open-source/lasst-uns-verschluesseln/

Besuchen Sie uns auch auf Facebook und Twitter.

r23
Thüringenstr. 20
58135 Hagen
Deutschland
Telefon: 02331 / 9 23 21 29

E-Mail: info@r23.de

Ust-IdNr.:DE250502477