TLS, Zertifikate und Let’s Encrypt

Installation der Prüfwerkzeuge (Debian)

```
sudo apt update
```

```
sudo apt install openssl
```

```
openssl version
```

Für die Zertifikatsverwaltung mit Certbot, sofern diese Methode eingesetzt wird:

```
sudo apt install certbot
```

```
certbot --version
```

Verbindung und Zertifikat prüfen

```
openssl s_client -connect wiki.bluegnu.de:443 -servername wiki.bluegnu.de -
verify_return_error </dev/null
```

Bei HTTPS erfolgt die Entschlüsselung der übertragenen Daten automatisch durch Browser oder HTTP-Client. Ein gesonderter Entschlüsselungsbefehl ist nicht nötig. `openssl s_client` ist ein Diagnosewerkzeug und kein vollständiger Ersatz für die Zertifikatsprüfung eines Browsers.

Zweck

TLS schützt Netzwerkverbindungen, beispielsweise HTTPS. Bei einer typischen Website weist sich der Server mit einem X.509-Zertifikat aus. Die Datenübertragung erfolgt anschließend mit symmetrischer Verschlüsselung.

Bestandteile

- **Privater Server-Schlüssel:** Muss geheim bleiben.
- **Zertifikat:** Enthält unter anderem öffentlichen Schlüssel, Domainnamen und Gültigkeitszeitraum.
- **Zertifikatskette:** Verbindet das Serverzertifikat mit einer vertrauenswürdigen Zertifizierungsstelle (CA).

Let's Encrypt ist eine öffentliche CA, die Zertifikate automatisiert ausstellt. Das Zertifikat ersetzt nicht

den privaten Schlüssel.

Zertifikat einer Website ansehen

```
openssl s_client -connect wiki.bluegnu.de:443 -servername wiki.bluegnu.de
</dev/null
```

Die Ausgabe enthält Zertifikats- und Verbindungsinformationen. Für eine übersichtliche Darstellung des lokal gespeicherten Zertifikats:

```
openssl x509 -in zertifikat.pem -noout -subject -issuer -dates
```

```
openssl x509 -in zertifikat.pem -noout -fingerprint -sha256
```

Zertifikatserneuerung

Bei Certbot kann der Status der Zertifikate angezeigt werden:

```
sudo certbot certificates
```

Ein Test der automatischen Erneuerung ist möglich mit:

```
sudo certbot renew --dry-run
```

Diese Befehle setzen eine vorhandene Certbot-Installation und passende Berechtigungen voraus.

Was Browser prüfen

Zu den Prüfungen gehören Zertifikatskette, Domainname und Gültigkeitszeitraum. Ein korrektes Zertifikat belegt nicht, dass die Inhalte einer Website vertrauenswürdig oder frei von Schadsoftware sind.

Schlüsselwechsel und Vorfälle

Bei Verlust des privaten TLS-Schlüssels ist ein neues Schlüsselpaar mit neuem Zertifikat auszustellen. Bei vermuteter Kompromittierung sollte das betroffene Zertifikat zusätzlich widerrufen werden. Automatische Erneuerung und die Erreichbarkeit der Website regelmäßig kontrollieren.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:tls

Last update: **2026/11/15 16:36**