

## [de] Zertifikate - Handling - OpenSSL - Prüfe CA Zertifikate unter Linux

09/10/2024 18:24:48

[FAQ Article Print](#)

<b>Category:</b>	IT-Sicherheit & Anmeldung an Diensten::PKI-Zertifikate	<b>Votes:</b>	1
<b>State:</b>	public (all)	<b>Result:</b>	100.00 %
<b>Language:</b>	de	<b>Last update:</b>	11:41:25 - 09/01/2023

### Keywords

OpenSSL OpenLDAP CA Certificate

### Solution (public)

CA Zertifikate unter Linux werden mit dem Paket `ca-certificates` installiert. In der Regel liegen die Root-Zertifikate unter `/etc/ssl/certs` und als Zusammenfassung in der Datei `/etc/ssl/certs/ca-certificates.crt`. Neue CA Zertifikate werden in der Regel unter `/etc/ssl/certs` abgelegt und mit dem Befehl `update-ca-certificates` in der Datei `ca-certificates.crt` ergänzt oder entfernt.

Weitere Informationen können sie speziell aus Ihrer Distributionsdokumentation entnehmen z.B.

[1]<https://wiki.ubuntuusers.de/CA/>

Das Skript `check_cert_chain.sh` aus dem Anhang dieses FAQ kann für die Prüfung des Root Zertifikates auf einem Client verwendet werden. Hinweis: Dies ist keine Sicherheit, dass die Clientanwendung auch diesen Zertifikatsspeicher verwendet! Bei dieser Prüfung handelt es sich um eine globale Voraussetzung, welche lokal in jeder Anwendung auch anders konfiguriert sein kann.

Der Dienst z.B. `ldap-lzr.zih.tu-dresden.de` besitzt ein Serverzertifikat, das mit weiteren Zwischenzertifikaten der Sectigo CA signiert wurde. Die Zwischenzertifikate werden vom Dienst mit ausgeliefert, sodass sich am Ende eine vollständige Zertifikatskette ergibt, so wie die Datei `ldap-lzr-sectigo-fullchain.pem` im Anhang.

Der Client sollte bzw. muss mindestens das Wurzelzertifikat besitzen! Dies wäre bei Sectigo das USERTrust RSA Certification Authority. Das Besitzen der Zwischenzertifikate ist nur optional erforderlich, da die vollständige Zertifikatskette mit ausgeliefert wird.

Folgende Ausführung sollte auf dem Client erscheinen:

```
service@my_client:~# ./check_cert_chain.sh ldap-lzr-sectigo-fullchain.pem
stdin: OK - CN subject=C = US, ST = New Jersey, L = Jersey City, O = The
USERTRUST Network, CN = USERTrust RSA Certification Authority
stdin: OK - CN subject=C = GB, ST = Greater Manchester, L = Salford, O =
Sectigo Limited, CN = Sectigo RSA Organization Validation Secure Server CA
stdin: OK - CN subject=C = DE, ST = Sachsen, O = Technische Universitaet
Dresden, CN = ldap-lzr.zih.tu-dresden.de
```

[1] <https://wiki.ubuntuusers.de/CA/>