Installation des Root-CA-Zertifikats der Deutschen Telekom in Linux-Serversystemen

Debian (und ähnliche, z.B. Ubuntu)

- Herunterladen des Zertifikats
```
cd /tmp
wget –no-check-certificate \
'https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-
TeleSec_GlobalRoot_Class_2.crt'
```
- Konvertieren des Zertifikats in das PEM Format
```
openssl x509 -inform der -in deutsche-telekom-root-ca-2.crt \
-outform pem -addtrust serverAuth -out deutsche-telekom.pem
```
- Kopieren der PEM-Datei in das Verzeichnis für CA-Zertifikate
```
cp deutsche-telekom.pem /etc/ssl/certs/
```
- Reindizieren der CA-Zertifikate
```
c_rehash
```

Das CA-Zertifikat ist nun für die Verwendung mit Applikationen, die openSSL nutzen, installiert.

Überprüfen z.B. mit:
```
openssl s_client -host webmail.uni-weimar.de -port 443 -CApath /etc/ssl/certs
```
in der letzten Zeile muss erscheinen:
```
Verify return code: 0 (ok)
```

Konfigurieren der LDAP-Client-Anwendungen

- Datei `/etc/ldap/ldap.conf` bearbeiten oder erstellen, mit folgendem Inhalt
```
TLS_CACERT /etc/ssl/certs/deutsche-telekom.pem
TLS_REQCERT hard
TLS_CRLCHECK none
```

Sollte LDAP im Apache mit PHP genutzt werden, so ist Apache komplett neuzustarten (graceful reicht nicht aus), damit die Änderungen übernommen werden.

Es ist wichtig, darauf zu achten, dass die korrekten Hostnamen verwendet werden, da der Zertifikatsabgleich sonst fehlschlägt, also z.B.

ldap://nisslave.nisad.uni-weimar.de

statt

ldap://141.54.1.21

Weiterhin muss in PHP ein expliziter Aufruf von `ldap_start_tls()` erfolgen. Alternativ kann mit der Angabe von ldaps://... SSL verwendet werden.