letsencrypt & JAVA

Seit 3.12 befindet sich letsencrypt.org in der offenen Beta Phase, das heißt, es gibt Zertifikate für alle. Leider fehlt das Root Zertifikat, mit dem das CA Zertifikat der Intermediate CAs, die die Zertifikate dann letztendlich ausstellen im Default JAVA Truststore. Das kann aber geändert werden:

1. Exportieren des "DSTRootCAX3", der Einfachheit halber mit Firefox aus der Zertifikatskette einer schon per letsencrypt "verschönerten" Website
2. Import mittels Java Keytool (Teil des JDK) in den Truststore der JRE:

```
C:\>set PATH=%PATH%;"D:\Program Files (x86)\Java\jdk1.8.0_66\bin"
C:\>cd /d "D:\Program Files (x86)\Java\jre1.8.0_66\lib\security"
D:\Program Files (x86)\Java\jre1.8.0_66\lib\security>copy cacerts
cacerts.bak
D:\Program Files (x86)\Java\jre1.8.0_66\lib\security>keytool -import -
trustcacerts -alias DSTRootCAX3 -file DSTRootCAX3.crt -keystore cacerts
Keystore-Kennwort eingeben: changeit
Eigentümer: CN=DST Root CA X3, O=Digital Signature Trust Co.
Aussteller: CN=DST Root CA X3, O=Digital Signature Trust Co.
Seriennummer: 44afb080d6a327ba893039862ef8406b
Gültig von: Sat Sep 30 23:12:19 CEST 2000 bis: Thu Sep 30 16:01:15 CEST
2021
Zertifikat-Fingerprints:
         MD5:  41:03:52:DC:0F:F7:50:1B:16:F0:02:8E:BA:6F:45:C5
         SHA1:
DA:C9:02:4F:54:D8:F6:DF:94:93:5F:B1:73:26:38:CA:6A:D7:7C:13
         SHA256:
06:87:26:03:31:A7:24:03:D9:09:F1:05:E6:9B:CF:0D:32:E1:BD:24:93:FF:C6:D9
:20:6D:11:BC:D6:77:07:39
         Signaturalgorithmusname: SHA1withRSA
         Version: 3

Erweiterungen:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
```

```
KeyIdentifier [
0000: C4 A7 B1 A4 7B 2C 71 FA   DB E1 4B 90 75 FF C4 15
.....,q...K.u...
0010: 60 85 89 10                                        `...
]
]

Diesem Zertifikat vertrauen? [Nein]:  j
Zertifikat wurde Keystore hinzugefügt
```

Damit funktioniert beispielsweise auf eGit in der Eclipse ohne “http.sslVerify = false”.

kb, java, ssl