Versionsüberprüfung und Update-Anleitung des nginx.truststore im DEMIS-Adapter

Mit der kommenden Zertifikatsaktualisierung kann es in Verbindung mit älteren Versionen des nginx.truststore zu den unten stehenden Fehlermeldungen kommen.

- **WARN** de.rki.demis.adapter.api.mtls.TLSTokenFetcher:getAccessToken:201 - TLSTokenFetcher.getAccessToken() failed: *javax.net.ssl.SSLHandshakeException*: PKIX path building failed: *sun.security.provider.certpath.SunCertPathBuilderException*: unable to find valid certification path to requested target

- **ERROR** de.rki.demis.adapter.api.LaborConfig:refreshToken:
  372 - could not refresh Token, check connection to Identity Provider server, exception message: PKIX path building failed: *sun.security.provider.certpath.SunCertPathBuilderException*: unable to find valid certification path to requested target

Bitte prüfen Sie die Version Ihres nginx.trustores und aktualisieren Sie - sofern notwendig - nach unten stehenden Anleitungen.

Wenn Sie den Truststore des **Importer V1.6.1** oder des **Adapter V1.1.0** oder höhere Versionen benutzen, müssen Sie den Truststore nicht austauschen. Ab diesen Versionen wird ein Truststore mitgeliefert, der für die Produktiv- und die Testumgebung auch nach der Zertifikatsaktualisierung weiterhin gültig ist.

Wie überprüfe ich die installierte Version des nginx.truststore?

Zur Überprüfung Ihres nginx.trustores führen Sie bitte das unten stehende Kommando im /config/ Verzeichnis Ihres DEMIS-Adapters aus:

```
keytool -list -v -keystore nginx.truststore
Das dazugehörige Keystore-Kennwort lautet: secret
```

Wenn das ausgegeben Ergebnis die beiden gelben Zeilen enthält, benötigt Ihr ngnix.truststore keine Aktualisierung.

Wenn das ausgegeben Ergebnis die beiden gelben Zeilen nicht enthält, folgen Sie bitte der unten stehenden Anleitung zur Aktualisierung des nginx.trustores.

```
D:\tools\Demis-Adapter-1.7.1\config>keytool -list -keystore nginx.truststore
Keystore-Kennwort eingeben:
Keystore-Typ: PKCS12
Keystore-Provider: SUN

Keystore enthält 8 Einträge

demis-test.rki.de, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): 85:13:25:CA:01:F5:0F:91:90:C7:FE:D3:02:A6:E8:FD:89:A0:79:88:F2:6F:20:E0:64:F1:D1:2C:0D:DC:76:FC
demis.rki.de, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): 8B:E9:68:F7:8A:5D:E3:6E:34:D0:D1:53:11:F0:C1:F0:9D:B2:DE:93:BD:6A:F4:45:0E:8E:DF:26:88:07:06:DE
demis.rki.de_d-trust, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): 28:B8:CC:12:03:3C:F3:61:B6:09:D4:31:B9:80:52:2F:B2:C4:6D:02:D6:93:73:B1:C9:40:59:D4:87:73:72:88
localhost, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): 87:82:75:70:08:E6:C9:74:9B:5C:B3:30:07:38:5F:EC:DE:49:BB:C0:B0:4C:59:96:5F:A6:88:EA:FA:88:6B:73
root_d-trust, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): EE:C5:49:6B:98:8C:E9:86:25:B9:34:09:2E:EC:29:08:BE:D0:B0:F3:16:C2:D4:73:0C:84:EA:F1:F3:D3:48:81
root_digicert, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): CB:3C:CB:B7:60:31:E5:E0:13:8F:8D:D3:9A:23:F9:DE:47:FF:C3:5E:43:C1:14:4C:EA:27:D4:6A:5A:B1:CB:5F
sub_d-trust, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): B0:93:5D:C0:4B:4E:60:C0:C4:2D:EF:7E:C5:7A:1B:1D:8F:95:8D:17:98:8E:71:CC:80:A8:CF:5E:63:5B:A5:B4
sub_digicert, 26.08.2021, trustedCertEntry,
Zertifikat-Fingerprint (SHA-256): 44:22:E9:63:EE:53:CD:58:CC:9F:85:CD:40:BF:5F:FE:C0:09:5F:DF:1A:15:45:35:66:1C:1C:06:BC:AD:C6:9B
```

Wie aktualisiere ich meine Version des nginx.truststore?

Zur manuelle Aktualisierung des nginx.truststore, laden Sie bitte die unten stehende Version herunter und speichern Sie die Datei in den Ordner /config/ in Ihrem DEMIS-Adapter-Verzeichnis.

Truststore

nginx.truststore