

SSL

Bei einer Umstellung auf https müssen alle Programme über dasselbe Protokoll miteinander kommunizieren! In der Regel sind folgende Programme betroffen und es werden folgende Zertifikate benötigt:

- **Tomcat8**

PFX / P12 Datei mit Kennwort. Eine PFX-Datei kann einfach in .p12 umbenannt werden!

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
  [maxThreads="200"
    SSLEnabled="true"
    scheme="https"
    secure="true"
  [keystoreFile="D:\Applikationen\Documents5\tomcat8\conf\zertifikatsdatei.p12"
    keystorePass="ZertifikatPasswort"
  [clientAuth="false"
    sslProtocol="TLS"
    maxPostSize="8388608"
    maxHttpHeaderSize="32768"
  />
```

- **TableService**

Zertifikat BASE64 codiert (PEM Datei, wobei die Endung keine große Rolle spielt)

Private Key (unverschlüsselt – kein RSA Key) ebenfalls BASE64 codiert

- **Squeeze**

Zertifikat BASE64 codiert (PEM Datei, wobei die Endung keine große Rolle spielt)

Private Key (unverschlüsselt – kein RSA Key) ebenfalls BASE64 codiert

Zertifikatskette (wenn vorhanden) ebenfalls BASE64 codiert.

Der Zertifikatsspeicher (PFX) bzw. das Zertifikat muss mindestens mit dem Signaturalgorithmus SHA-256 signiert sein.

Es kann bei veraltet konfigurierten CAs (Certificate Authority) vorkommen, dass ein Exportvorgang mit SHA-256 erfolgreich abgeschlossen, das Zertifikat jedoch immer noch mit SHA-1 signiert wurde. SHA-1 gilt seit 2017 als **NICHT SICHER!**

Der Kunde soll einen PFX Zertifikatsspeicher bereitstellen und das Passwort mitteilen. Gegebenenfalls wird im DEXPRO-Ordner bereits der Unterordner **OpenSSL** ausgeliefert. Der Ordner enthält die openssl.exe und 2 DLL's sowie eine **ExtractPfx.bat**. In der BAT-Datei müssen

lediglich der Dateiname, das Passwort und der Pfad angepasst werden. Die PFX-Datei muss in den Unterordner "IN" abgelegt werden.

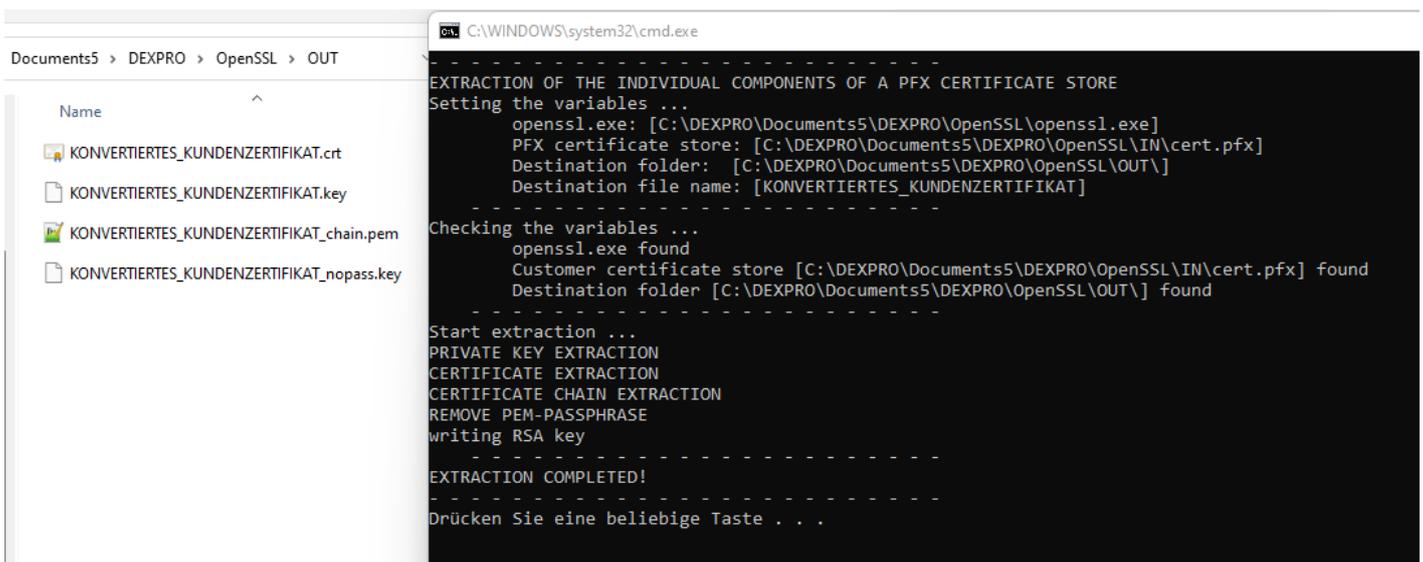
```
REM VARIABLES TO SET!  
SET FILENAME=cert.pfx  
SET PW=mySecretPW  
SET PATH=D:\Documents5\DEXPRO\OpenSSL\
```

OPENSSL BINARIES

Durch die Extraktion werden die folgenden Dateien erstellt:

- Das eigentliche Zertifikat ist die `.cert` Datei.
- Der Private Key (mit PEM-Passphrase) ist `.key` Datei.
- Die Zertifikatskette ist die `_chain.pem` Datei, wenn diese leer ist, dann gibt es keine weitere Kette.
- Der Private Key (ohne PEM-Passphrase) ist die `_nopass.key` Datei.

Die **ExtrctPfx.bat** sollte mit Administrator-Berechtigungen ausgeführt werden. Das Ergebnis sollte wie im folgenden Screenshot zu sehen aussehen.



The screenshot shows a Windows File Explorer window on the left with the path 'Documents5 > DEXPRO > OpenSSL > OUT'. It contains four files: 'KONVERTIERTES_KUNDENZERTIFIKAT.crt', 'KONVERTIERTES_KUNDENZERTIFIKAT.key', 'KONVERTIERTES_KUNDENZERTIFIKAT_chain.pem', and 'KONVERTIERTES_KUNDENZERTIFIKAT_nopass.key'. On the right, a Command Prompt window shows the execution of the script. The output includes: 'EXTRACTION OF THE INDIVIDUAL COMPONENTS OF A PFX CERTIFICATE STORE', 'Setting the variables ...', 'openssl.exe: [C:\DEXPRO\Documents5\DEXPRO\OpenSSL\openssl.exe]', 'PFX certificate store: [C:\DEXPRO\Documents5\DEXPRO\OpenSSL\IN\cert.pfx]', 'Destination folder: [C:\DEXPRO\Documents5\DEXPRO\OpenSSL\OUT\]', 'Destination file name: [KONVERTIERTES_KUNDENZERTIFIKAT]', 'Checking the variables ...', 'openssl.exe found', 'Customer certificate store [C:\DEXPRO\Documents5\DEXPRO\OpenSSL\IN\cert.pfx] found', 'Destination folder [C:\DEXPRO\Documents5\DEXPRO\OpenSSL\OUT\] found', 'Start extraction ...', 'PRIVATE KEY EXTRACTION', 'CERTIFICATE EXTRACTION', 'CERTIFICATE CHAIN EXTRACTION', 'REMOVE PEM-PASSPHRASE', 'writing RSA key', 'EXTRACTION COMPLETED!', and 'Drücken Sie eine beliebige Taste . . .'

Die konvertierte crt- und die ky-Datei enthalten zusätzliche Informationen, welche manuell aus der Datei gelöscht werden müssen. Die Dateien können beliebig umbenannt und verwendet werden.

