Optionale Erweiterungen

- Single-Sign-On: Auslagerung der web.xml
- SSL

Single-Sign-On: Auslagerung der web.xml

Ein häufiger Kundenwunsch ist die automatische Anmeldung am System via Single-Sign-On. Hierfür müssen Anpassungen in der **web.xml** vorgenommen werden, welche sich im **webapps**-Ordner des Tomcats befindet. Nach einem Documents-Update soll jedoch immer der **webapps**-Ordner gelöscht werden und dadurch gehen auch diese SSO-Anpassungen in der **web.xml** verloren.

Hierfür kann die **web.xml** in den **..\DEXPRO\WEB-INF**-Ordner kopiert werden. Bei einem Documents-Update gehen die Anpassungen an der Datei nicht mehr verloren. Der Nachteil ist allerdings, dass dadurch ggf. benötigte Erweiterungen an der **web.xml** manuell hinzugefügt werden müssen.

Die Auslagerung der **web.xml** ist ausdrücklich nur als Option zu sehen.

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.

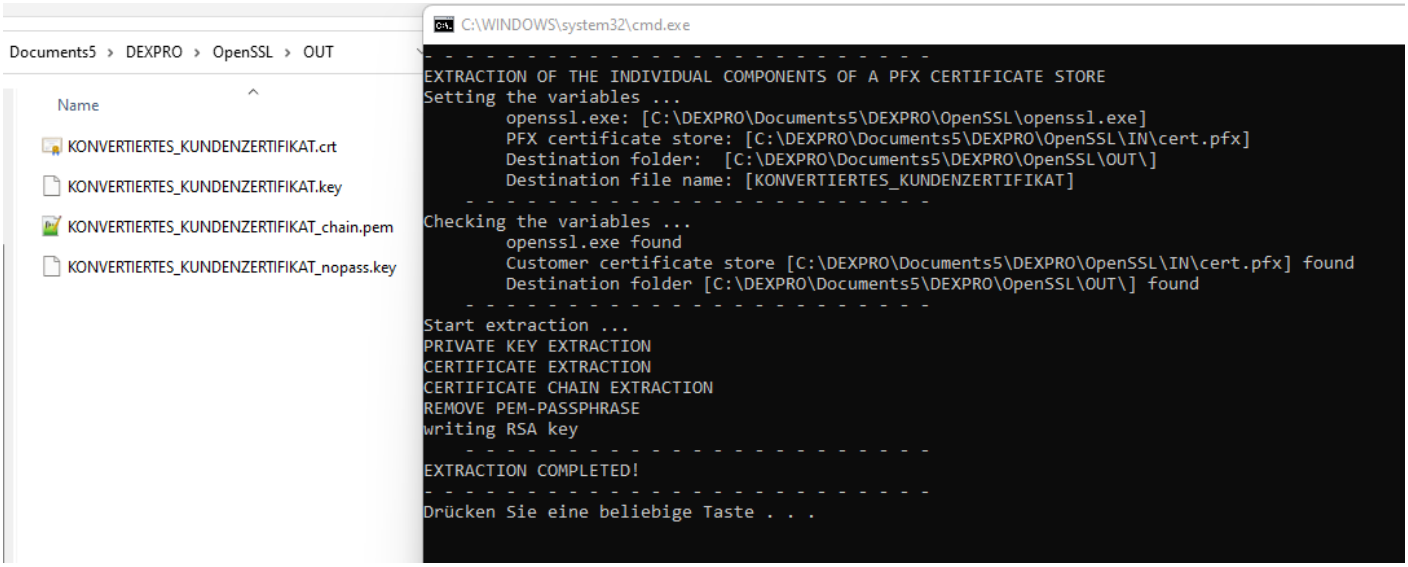
```
REM VARIABLES TO SET!
SET FILENAME=cert.pfx
SET PW=mySecretPW
SET PATH=D:\Documents5\DEXPRO\OpenSSL\
```

OPENSSL BINARIES

Durch die Extraktion werden die folgenden Dateien erstellt:

- Das eigentliche Zertifikat ist die `.crt` 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.



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.

KONVERTIERTES_KUNDENZERTIFIKAT.crt

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: [redacted]
subject=CN = [redacted]

issuer=C = US, O = DigiCert Inc, CN = RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1

-----BEGIN CERTIFICATE-----
MIIGnTCCBYWgAwIBAgIQBhW9rqpx5GMJdQt2vmAp6zANBgkqhkiG9w0BAQsFADBZ
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQDEypS
YXBpZFNTTCBUTFMgRFYgUlNBIE1peGVkIFNIQTI1NiAyMDIwIENBLTEwHhcNMjIw
NDEyMDAwMDAwWhcNMjMwNDEyMjM1OTU5WjAeMRwwGgYDVQQDDBMqLnBvbmQtc2Vj
dXJpdHkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwknLuZ0l
8ZnbsHKJLKVYZq3BsmfpsMCKWIS4ZbcIb5OE0Kl4osy5MSr9/Aqxw+Okkg8lXuX5
dFPxE2SYUOKKfBuX4AEATtroa0/Rj30h0XdmDor+fJOXdFoApJ3Ow2TjC9HIg74t
YaFrHoiu0199PLQe3Lnucj8fihahNRg0aZd7xDEZjnT8xu/zdGlyFX3JuGew40M5
A0FDAV4TOdbV5l+26qMUmajYoON9R6Xi50TX0p4PH8jDV1Ul8YRx3WsaFyEzY6ZT
FYkb64B1VcN9yt2nGfwvQ5lX34GAZEWB9yxwuEQjZxURr38NQ9CSPbuHAyPV7hVN
JQNVFJwcvnYpDwIDAQABo4IDmjCCA5YwHwYDVR0jBBgwFoAUpI3lvnx55HAjbS4p
NK0jWNzlMX8wHQYDVR0OBBYEFO0qYlGYzwkfJAKYdlwl4bq3ebnEMDEGA1UdEQQq
MCiCEyoucG9uZC1zZWN1cml0eS5jb22CEXBvbmQtc2VjdXJpdHkuY29tMA4GA1Ud
DwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwgZsGA1Ud
HwSBkzCBkDBGoESgQoZAaHR0cDovL2NybDMuZGlnaWNlcnQuY29tL1JhcGlkU1NM
VExTRFZSU0FNaXhlZFNIQTI1NjIwMjBDQS0xLmNybDBGoESgQoZAaHR0cDovL2Ny
bDQuZGlnaWNlcnQuY29tL1JhcGlkU1NMVExTRFZSU0FNaXhlZFNIQTI1NjIwMjBD
QS0xLmNybDA+BgNVHSAENzA1MDMGBmeBDAECATApMCcGCCsGAQUFBwIBFhtodHRw
Oi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwgYUGCCsGAQUFBwEBBHkwdzAkBggrBgEF
BQcwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tME8GCCsGAQUFBzAChkNodHRw
Oi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vUmFwaWRTU0xUTFNEVlJTQU1peGVkU0hB
MjU2MjAyMENBLTEuY3J0MAkGA1UdEwQCMAAwggF/BgorBgEEAdZ5AgQCBIIBbwSC
AWsBaQB3AOg+0No+9QY1MudXKLyJa8kD08vREWvs62nhd31tBr1uAAABgB2zqfAA
AAQDAEgwRgIhAOOCQi4BDjFRxpUBPsTfJ/DLfA60/aSb7xePnFCTQHgmAiEA0JuX
tqnEoJHlhC0SsFGb2btdepmF7qtx4Vj76taAIz0AdgA1zxkbv7FsV78PrUxtQsu7
ticgJlHqP+Eq76gDwzvWTAAAAYAds6oMAAAEAwBHMEUCIQCQgn0+mjSsURctUzNg
RJhgARDgNkxE8wHu/YD+6YRr4gIgNcJvy007C2SH1vMxClV3eT60P+1jwRtt99tu
aeSCcXYAdgCzc3cH4YRQ+GOG1gWp3BEJSnktsWcMC4fc8AMOeTalmgAAAYAds6pC
AAAEAwBHMEUCIHzxwHzKXygD/kwVOnOrUkm6P2G6nwHwdeAyxbPRdsVVAiEApNMx
/gmreyp+sT2OKrnhr4PxtVn3m+jf5VvnnaxJPrcwDQYJKoZIhvcNAQELBQADggEB
ALNF6Z+5fNJu2YK6MOov3Dx9EwC1pl/8SRoFs3Wa6eaZES9NhGQZvCCm9GpJx/y3
rs2aEX84TbNrsGrK7xR7ZLYvqeLFBEL9jgVUh4hvk/6N+F6RMKDYfvnB8qU4TLIv
kCISliZtz4+hO/ZOOG32H7qCW83g9uFeB1kkEOBaxuT8htsCAnOeHD571IFNaE11
+6yYEzzUQZvOi4COSTnrtvJ+Q1j6Tp4yhITV+l36j1igUpfoiDRdjMyuX5dkD14N
4bUm3wN8gvRi0OyvHPguWKjeKecNaPaQsEKvTykI6B2v+DCgNFuu+yk1aFnMvr0o
[redacted]=
-----END CERTIFICATE-----
```