Einrichtung einer sicheren https Verbindung

Um eine sichere Verbindung einzurichten muss im Apache ein neuer virtueller Host eingerichtet werden.

Voraussetzungen

Es wird ein **Zertifikat** und ein **privater Schlüssel** im **PEM-Format** (BASE64 kodierte Zeichenkette) benötigt.

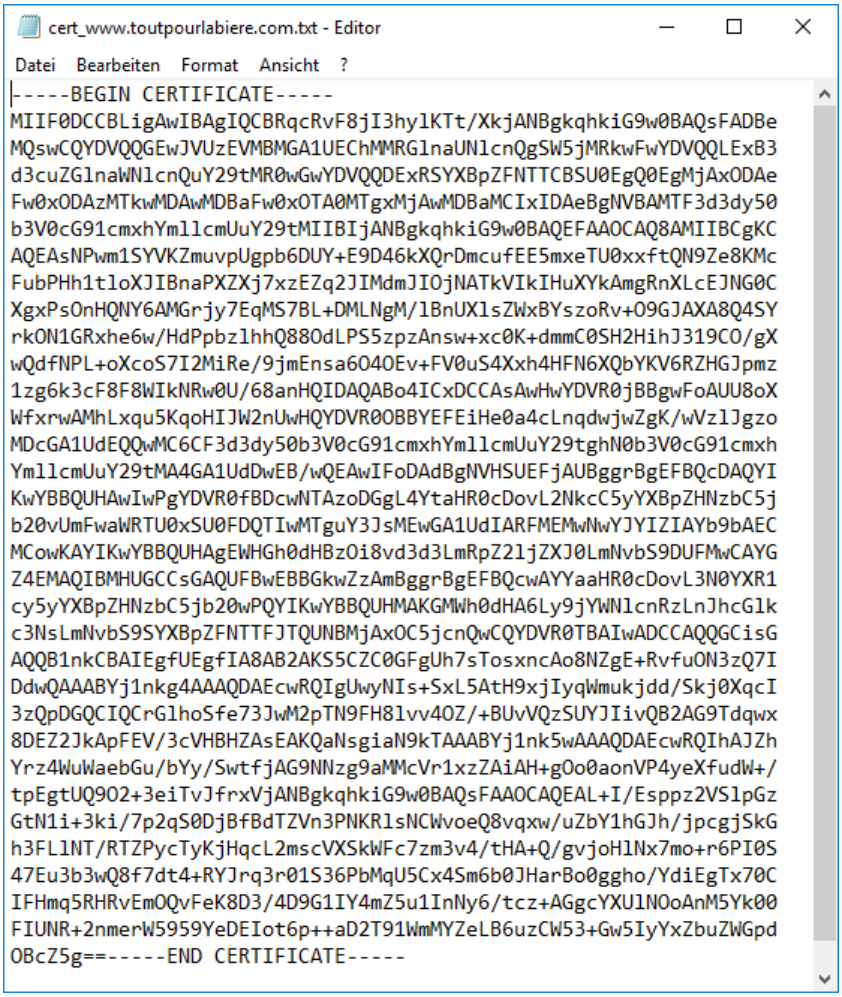
Außerdem muss das Zertifikat mit mindestens dem **SHA-256** Signaturalgorithmus signiert sein.

> All major webrowser vendors ceased acceptance of SHA-1 SSL certificates in 2017.
>
> Microsoft has discontinued SHA-1 code signing support for Windows Update in August 7, 2020.
>
> - Wikipedia (SHA-1)

Ein Zertifikatsspeicher (PFX / PKCS#12) kann ebenfalls verwendet werden.
Dazu muss das Zertifikat in seine Einzelteile (Zertifikat, privater Schlüssel und ggf. der Zertifikatskette) zerlegt werden.

Extraktion eines PFX-Zertifikatsspeicher

Am Ende der Voraussetzungen, steht mindestens das Zertifikat und der private Schlüssel zur Verfügung.
Ein Beispiel eines Zertifikats:



Sobald die Dateien vorliegen kann mit der Einrichtung des Virtuellen Hosts begonnen werden.

Konfiguration Webserver

httpd-vhosts.conf - Konfiguration

Das Zertifikat, den privaten Schlüssel des Zertifikats sowie eine etwaige Zertifikatskette unter dem Apache Konfigurationsordner `SQUEEZE\apache\conf\ssl` ablegen.

httpd-vhosts.conf - Konfiguration

Der virtuelle Host für den SSL Port `*: 443` muss in der Datei `SQUEEZE\apache\conf\extra\httpd-vhosts. conf` eingetragen werden.

Die `vhosts. conf` Konfiguration muss in der `httpd. conf` geladen werden, damit die `vhosts` in der Konfiguration des Webserver berücksichtigt werden (bei SQUEEZE bereits eingerichtet).

```
<VirtualHost *: 443>
  ServerName host. domain. net
```

```
  ServerAdmin admin@host.domain.net
  ServerSignature Off
  SSLEngine on
  SSLCertificateFile "conf/ssl/server.crt"
  SSLCertificateKeyFile "conf/ssl/server.key"
  SSLCertificateChainFile "conf/ssl/fullchain.pem"
  # DER FOLGENDE TEIL WIRD NUR BEI EINEM PROXY BENÖTIGT
  # SSLProxyEngine On
  # SSLProxyVerify none
  # SSLProxyCheckPeerCN off
  # SSLProxyCheckPeerName off
  # SSLProxyCheckPeerExpire off
</VirtualHost>
```

Die Pfade zum Zertifikat, den privaten Schlüssel des Zertifikats sowie eine etwaige Zertifikatskette sind entsprechend zu setzen.

Der **host.domain.net** Wert ist durch den entsprechenden Hostnamen zu ersetzen.

Zuletzt den Virtuellen Host (`VirtualHost *:80`) auskommentieren.

httpd.conf - Konfiguration

Der Webserver muss nun auf den SSL (HTTPS) Port hören.

Dies stellen wir in der Date `apache\conf\httpd.conf` ein.

```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
Listen 443
```

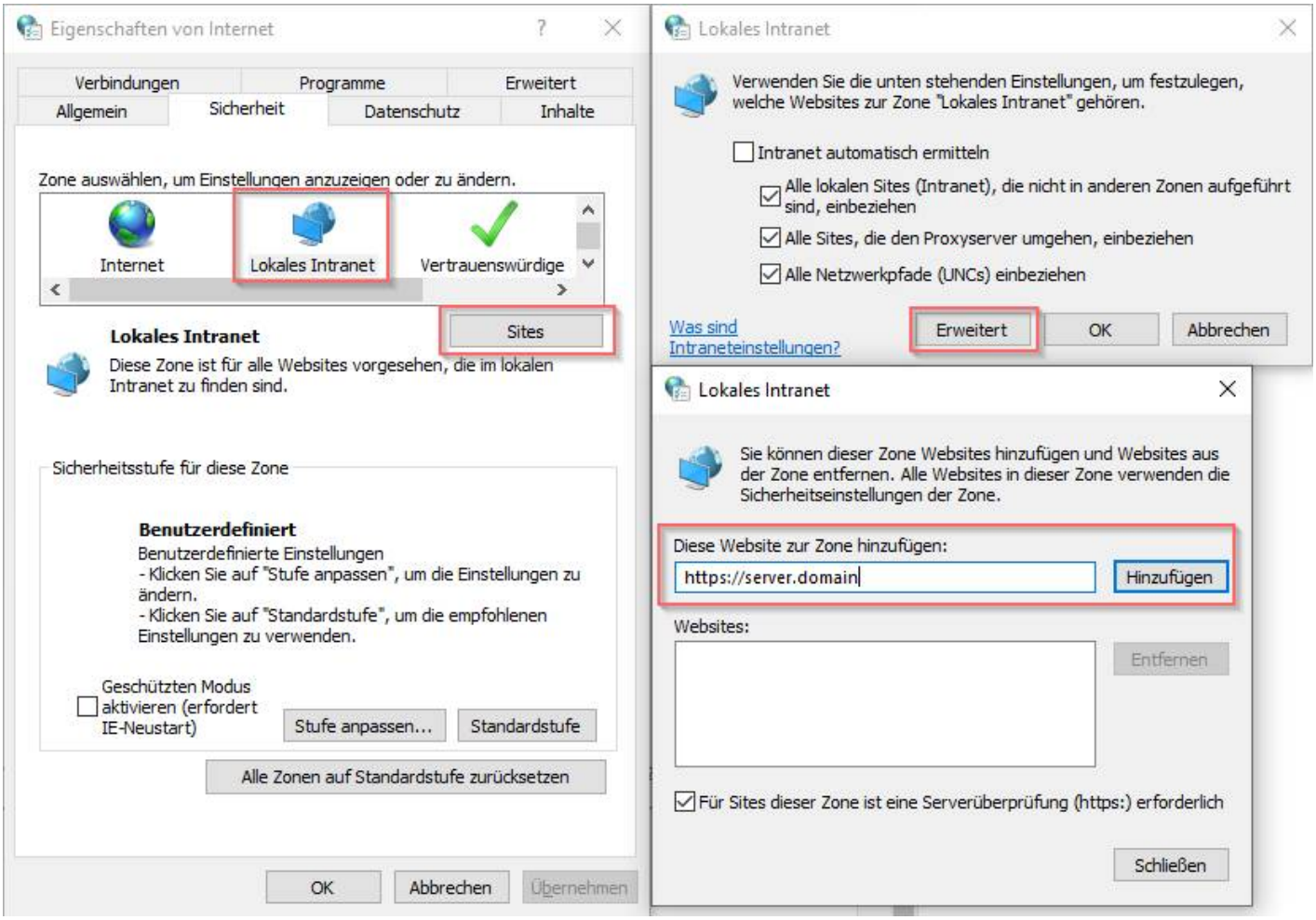
Weiter unten in der Konfigurationsdatei müssen wir noch das SSL Modul suchen und dieses einkommentieren.

```
LoadModule ssl_module modules/mod_ssl.so
```

Troubleshooting

Die Seite kann auf den Clients nicht aufgerufen werden?

Handelt es sich um eine Intranet-Domäne (`*.local` bspw.), dann muss die Server FQDN (URL) (https://servername.domäne) in den Internetoptionen der Clients bei den Intranetsites hinzugefügt werden. Sollte dies nicht funktionieren, ist die Seite bei den Vertrauenswürdigen Sites unterzubringen.



Seit den Windows Servern 2019 (und Windows 10) sind die TCP Ports `443`, `8443` in der Firewall standardmäßig nicht freigegeben.

Dazu sind also entsprechende eingehende und ausgehende Firewallregeln zu definieren.

Extraktion eines PFX -

Zertifikatsspeicher

Wenn das Zertifikat, die Zertifikatskette sowie der private Schlüssel (ohne Passphrase) für den Apache Webserver als Zertifikatsspeicher (PFX / PKCS#12) vorliegt, kann diese Batch (ohne jegliche Gewährleistung) ausgeführt werden, um an die notwendigen Einzelteile zu gelangen.

Dazu werden die OpenSSL Binaries benötigt (seit SQUEEZE 1.10 ausgeliefert).

Setzen der Batch-Variablen

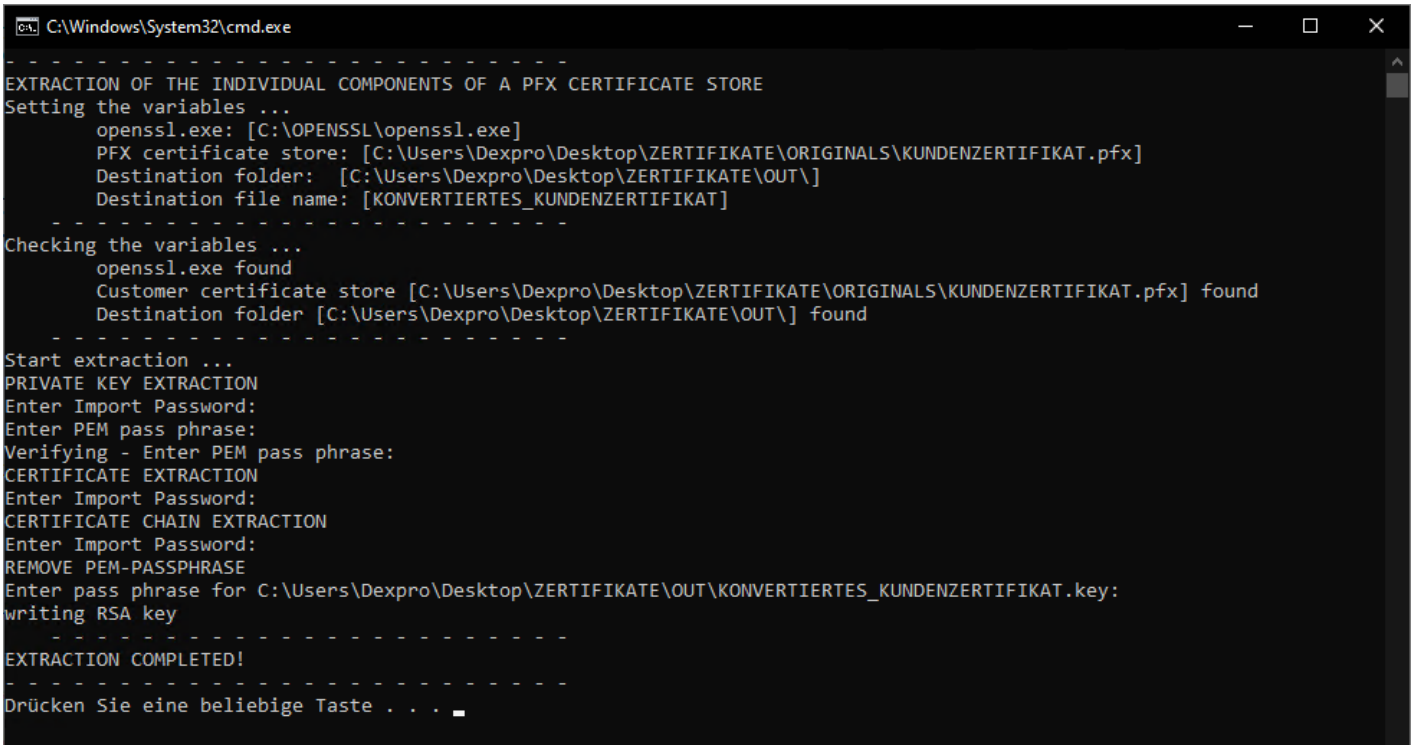
Es müssen im Batch-Script die folgenden Variablen gesetzt werden, damit das Script fehlerfrei arbeiten kann.

```
SET OPENSSL=D:\DEXPRO\TOOLS\OPENSSL\openssl.exe

SET PFXFILE=D:\DEXPRO\ZERTIFIKATE\ORIGINALS\KUNDENZERTIFIKAT.pfx
SET OUTPUTFOLDER=D:\DEXPRO\ZERTIFIKATE\OUT\
SET OUTPUTFILENAME=KONVERTIERTES_KUNDENZERTIFIKAT

SET REMOVEPASSPHRASE=true
```

Dabei werden die Pfade zu OpenSSL, dem Ausgabeordner und dem PFX Zertifikatsspeicher (PFX), sowie die Namen der zu erstellenden Zertifikatsbestandteile angegeben. Damit der private Schlüssel von etwa dem Apache Webserver gelesen werden kann, muss der private Schlüssel ohne PEM-Passphrase vorliegen. Dazu kann das Flag `REMOVEPASSPHRASE=true` gesetzt werden.

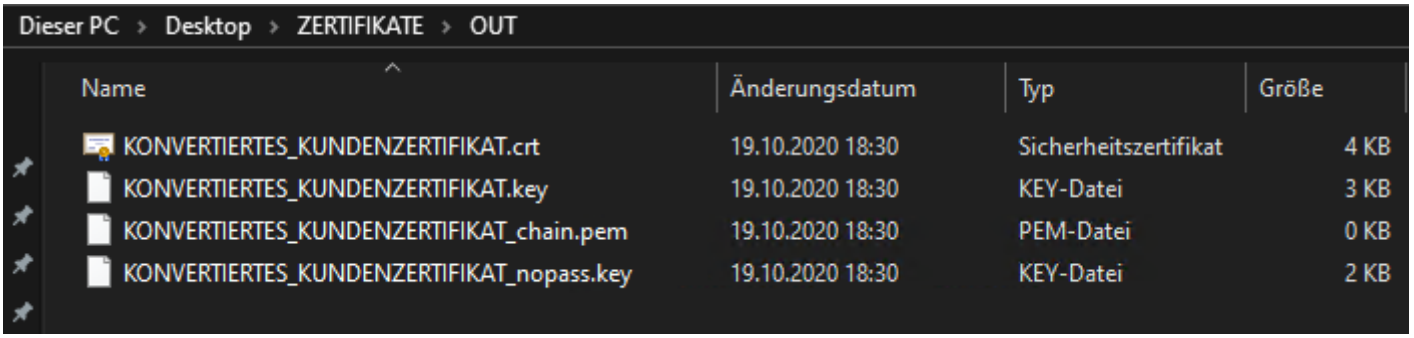
Ausführen der Batch

Einfach den Anweisungen der Batch-Datei folgen:



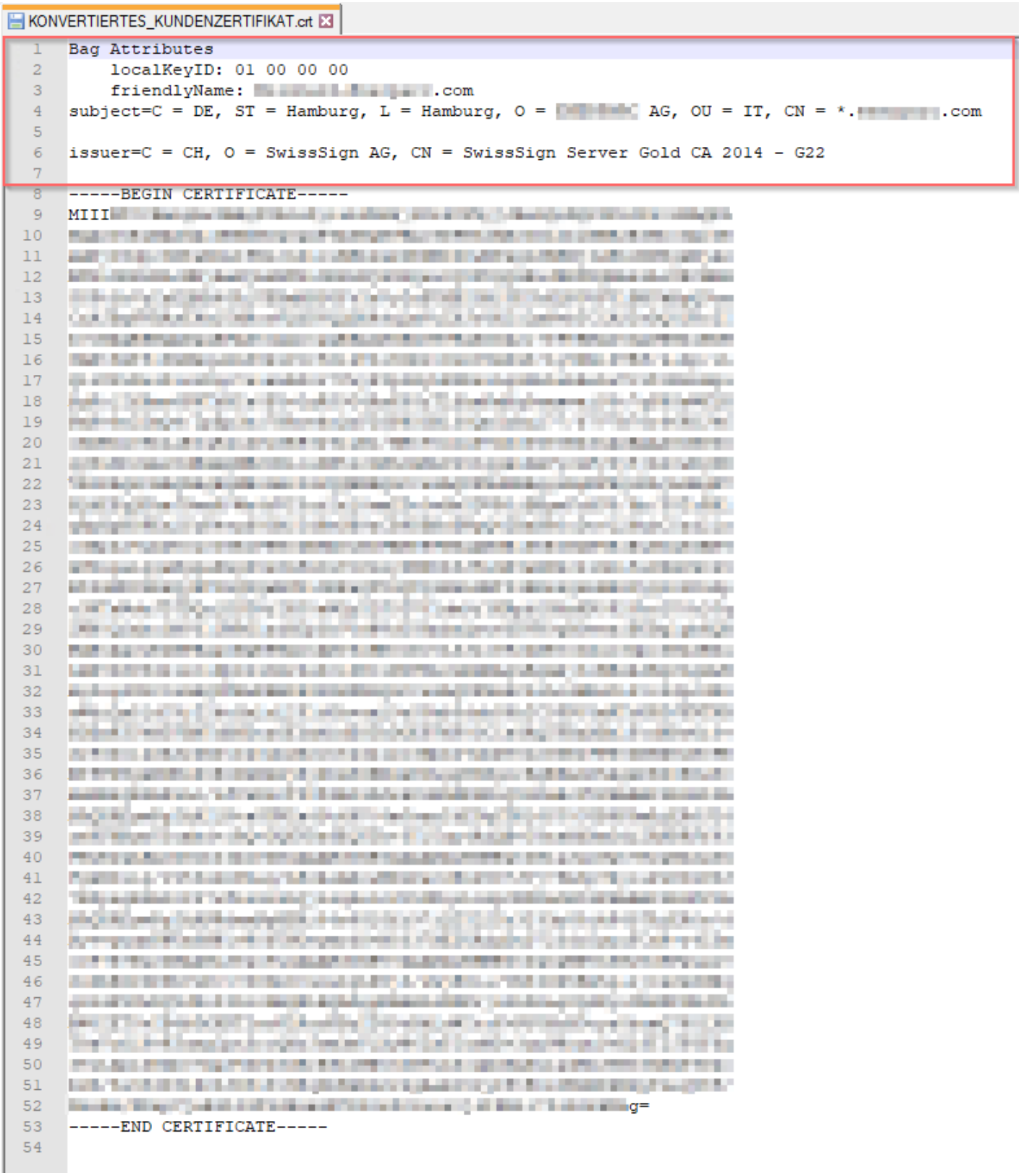
Ergebnis der Batch (Bestandteile des PFX)

Am Ende der Extraktion sind die folgenden Dateien im definierten Ausgabeordner zu finden:



- Das eigentliche Zertifikat (*.crt)
- Der private Key (mit PEM-Passphrase) (*.key)
- Der private Key (ohne PEM-Passphrase) (*_nopass.key)
- Die Zertifikatskette (*_chain.pem).
  Ist diese Datei leer, so gibt es in dem Zertifikatsspeicher keine auszugebende Kette.

Bei allen Dateien müssen im Anschluss die von OpenSSL generierten Informationen entfernt werden:



Batch Script Quellcode

Ohne jegliche Gewährleistung oder Anspruch auf Support.

```
@ECHO off
ECHO - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
REM VARIABLES TO SET!
SET OPENSSL=D:\DEXPRO\TOOLS\OPENSSL\openssl.exe

SET PFXFILE=D:\DEXPRO\ZERTIFIKATE\ORIGINALS\KUNDENZERTIFIKAT.pfx
SET OUTPUTFOLDER=D:\DEXPRO\ZERTIFIKATE\OUT\
SET OUTPUTFILENAME=KONVERTIERTES_KUNDENZERTIFIKAT
REM REMOVE PEM PASSPHRASE? -> TRUE / FALSE
SET REMOVEPASSPHRASE=true

REM START DER EXTRAKTION
ECHO EXTRACTION OF THE INDIVIDUAL COMPONENTS OF A PFX CERTIFICATE STORE
ECHO Setting the variables ...
ECHO  openssl.exe: [%OPENSSL%]
ECHO  PFX certificate store: [%PFXFILE%]
ECHO  Destination folder:  [%OUTPUTFOLDER%]
ECHO  Destination file name: [%OUTPUTFILENAME%]
ECHO     - - - - - - - - - - - - - - - - - - - - - -
ECHO Checking the variables ...
if exist %OPENSSL% (
    ECHO  openssl.exe found
) else (
    ECHO  openssl.exe [%OPENSSL%] not found - please adjust the path!
 goto ERROREND
)
if exist %PFXFILE% (
    ECHO  Customer certificate store [%PFXFILE%] found
) else (
    ECHO  Customer certificate store [%PFXFILE%] not found - please adjust the path!
 goto ERROREND
)
if exist %OUTPUTFOLDER% (
    ECHO  Destination folder [%OUTPUTFOLDER%] found
) else (
    ECHO  Destination folder [%OUTPUTFOLDER%] not found - please adjust the path!
 goto ERROREND
)
if "%OUTPUTFILENAME%"=="" (
    ECHO  No destination filename was specified!
 goto ERROREND
```

```
)
ECHO     - - - - - - - - - - - - - - - - - - - - - - -
ECHO Start extraction ...
ECHO PRIVATE KEY EXTRACTION
%OPENSSL% pkcs12 -in %PFXFILE% -nocerts -out %OUTPUTFOLDER%%OUTPUTFILENAME%.key
ECHO CERTIFICATE EXTRACTION
%OPENSSL% pkcs12 -in %PFXFILE% -clcerts -nokeys -out %OUTPUTFOLDER%%OUTPUTFILENAME%.crt
ECHO CERTIFICATE CHAIN EXTRACTION
%OPENSSL% pkcs12 -in %PFXFILE% -cacerts -nokeys -chain -out
%OUTPUTFOLDER%%OUTPUTFILENAME%_chain.pem


REM REMOVE PEM PASSPHRASE
IF "%REMOVEPASSPHRASE%"=="true" (
ECHO REMOVE PEM-PASSPHRASE
%OPENSSL% rsa -in %OUTPUTFOLDER%%OUTPUTFILENAME%.key -out
%OUTPUTFOLDER%%OUTPUTFILENAME%_nopass.key
) ELSE (
ECHO PEM-Passphrase is not removed
)
GOTO END

:END
ECHO     - - - - - - - - - - - - - - - - - - - - - - -
ECHO EXTRACTION COMPLETED!
ECHO - - - - - - - - - - - - - - - - - - - - - - - - -
PAUSE
EXIT

:ERROREND
ECHO     - - - - - - - - - - - - - - - - - - - - - - -
ECHO EXTRACTION FAILED!
ECHO PLEASE CHECK ALL PARAMETERS!
ECHO - - - - - - - - - - - - - - - - - - - - - - - - -
PAUSE
EXIT
```

Alternative Konfiguration

Einrichtung des Virtuellen Hosts

In der Datei `D:\SQUEEZE\apache\conf\extra\httpd-vhosts.conf` eintragen:

```
# Alternative Konfiguration:
LoadModule ssl_module modules/mod_ssl.so
<VirtualHost *:8443>
  ServerName host.domain.net
  DocumentRoot "${SQZROOT}\htdocs\public"
    <IfModule mod_ssl.c>
      SSLEngine on
      SSLCertificateKeyFile "conf/ssl/package.key"
      SSLCertificateFile "conf/ssl/package.cer"
      SetEnvIf User-Agent ".*MSIE.*" \
      nokeepalive ssl-unclean-shutdown \
      downgrade-1.0 force-response-1.0
    </IfModule>
</VirtualHost>
```

Der **host.domain.net** Wert ist durch den entsprechenden Hostnamen zu ersetzen.

Revision #10
Created 15 June 2020 11:07:14 by Phillip Langer
Updated 5 March 2021 10:32:12 by Maximillian Weitze