

Aktualisierung https-Zertifikate

White Paper

Wie aktualisiere ich Zertifikate für https?

Autor: C. Brandstetter, M. Pichelmann

Abteilung: PS München - Web

Status: Freigegeben

Version: 1.0.0.0

Datum: 07.09.2022

Datei: HowTo - Aktualisierung Zertifikate.docx

Versionsübersicht

Version	Datum	Ursache der Änderung	Betroffene Kapitel	Bearbeiter
0.9.0.0	13.04.2022	Anlegen des Dokumentes	alle	Pichelmann
1.0.0.0	07.09.2022	Ergänzung ArcGIS Data Store und SOLR Server	2.3.2 2.5	Brandstetter

Inhaltsverzeichnis

1 Einführung	4
1.1 Allgemeine Informationen.....	4
1.2 Hinweise zur Verwendung des Dokuments	4
1.3 Betroffene Komponenten	5
2 Aktualisierung der Zertifikate	7
2.1 Aktualisierung Rechnerzertifikat im internen Zertifikatsspeicher	7
2.1.1 Bereinigen des Zertifikatsspeichers.....	7
2.1.2 Importieren eines Zertifikats	10
2.1.3 Zuweisen eines Zertifikats im IIS.....	12
2.2 Aktualisierung des Java-Zertifikatsspeicher	14
2.2.1 Hinweise mit dem Arbeiten mit dem Java-Zertifikatsspeicher.....	18
2.2.2 Einlesen der Zertifikate mittels Kommandozeile.....	18
2.3 Aktualisieren der Zertifikate im ArcGIS Server	20
2.3.1 ArcGIS-Server und Portal for ArcGIS.....	20
2.3.2 ArcGIS Data Store.....	22
2.4 Aktualisierung der Zertifikate in Apache Tomcat.....	24
2.5 Aktualisierung der Zertifikate in SOLR (WebNAV pro).....	25
2.5.1 Behandlung der Passwörter	25
2.5.2 Direktes Einbinden einer PFX-Datei	26
2.5.3 Verwendung eines Java-Key-Stores.....	26

1 Einführung

1.1 Allgemeine Informationen

Um die Kommunikation über https sicherer zu gestalten, dürfen die hierfür verwendeten Zertifikate inzwischen nur noch maximal 13 Monate gültig sein. Daher müssen die Zertifikate regelmäßig erneuert werden. Dieses Dokument soll bei dieser Arbeit unterstützen und aufzeigen, welche Komponenten dabei berücksichtigt werden müssen. Voraussetzung ist, dass die benötigten Zertifikate durch die IT korrekt bereitgestellt werden.

VertiGIS übernimmt keine Gewähr für die Korrektheit des Dokuments und möglichen Folgen, die aus einer möglicherweise fehlerhaften Beschreibung oder falschen Handhabung dieses Dokuments resultieren.

Das Dokument behandelt nicht die Vorgehensweise zum Ausstellen von Zertifikaten oder das automatisierte Erneuern von Zertifikaten, wenn diese z.B. über Let's encrypt (<https://letsencrypt.org/>) regelmäßig erneuert werden.

1.2 Hinweise zur Verwendung des Dokuments

Die im Rahmen dieses Dokuments angegebenen Pfadangaben beziehen sich auf die von uns (VertiGIS-Team PS München) im Rahmen von Projekten durchgeführten und betreuten Installationen. Daher kann es zu Abweichungen in den angegebenen Dateipfaden kommen, insbesondere bei den betrachteten Komponenten JAVA, Apache Tomcat und SOLR. Die Vorgehensweise für die Aktualisierung der Zertifikate ist dann entsprechend der lokalen Umgebung und der vorgenommenen Installation anzupassen.

1.3 Betroffene Komponenten

Bei den von VertiGIS im UT-Umfeld verwendeten Umgebungen müssen die Zertifikate für https an folgenden Stellen regelmäßig erneuert werden:

- **Internet Information Server (IIS):** Dienst als Frontendkommunikationsschnittstelle für https-Requests für
 - o WebConnector für ArcGIS Server und Portal for ArcGIS
 - o ISAPI-Redirect mit AJP-Anbindung an Apache Tomcat für WMPS, WBAU und UT Integrator
 - o Dokumentenanbindung im UT Server
- **Apache Tomcat Servlet Engine** ist der Host für die Software
 - o WebMapPlotService
 - o Bauauskunft /ClickBeforeYouDig
 - o UT Integrator
 - o UT Appconnector
 - o Software unseres Partners BARAL (UTJSC, WebNAV, WebGEN)

Eine Aktualisierung der Zertifikate ist nur dann notwendig, wenn die einzelnen Softwarelösungen direkt über den im Tomcat vorhandenen Webserver angesprochen werden. Dies erfolgt normal über den Port 8443 (bzw. einem ähnlichen Port wie 8444 oder 8453).

Ist der Dienst über AJP und ISAPI-Redirect an den IIS gekoppelt, muss das Zertifikat nicht erneuert werden, da die entsprechende Schnittstelle deaktiviert ist.

- **Java-Store**
 - o Kernbestandteil der Apache Tomcat Servlet Engine. Da die einzelnen Softwarekomponenten von VertiGIS untereinander über https kommunizieren, müssen die entsprechenden Zertifikate bzw. Stammzertifikate hier eingelesen und auch erneuert werden. Andernfalls erkennt Java das Zertifikat nicht als gültig an und blockiert die Kommunikation zwischen den einzelnen Softwarebausteinen.
- **SOLR-Server**
 - o Kernbestandteil für die indizierte über WebNAVpro von BARAL.

- ArcGIS Server, Portal for ArcGIS und ArcGIS Data Store
 - o Sind diese Komponenten über den WebConnector an einen Webserver angebunden, ist eine Aktualisierung bzw. Verwendung der Zertifikate nicht zwingend erforderlich aber für interne Verwaltungs- und Administrationsaufgaben hilfreich. Die notwendige Kommunikation für die Weblösungen läuft normal über den IIS und somit über den Port 443.

2 Aktualisierung der Zertifikate

Durch die zeitlich begrenzte Gültigkeit der einzelnen Zertifikate, sind diese immer wieder zu erneuern. Je nach Konfiguration und Einsatzszenario sind hierbei unterschiedliche Komponenten anzufassen.

Im Folgenden wird auf die Aktualisierung der Zertifikate in den einzelnen Bestandteilen des Systems eingegangen. Nicht in jedem System sind alle Komponenten betroffen und müssen daher angefasst werden. Im Normalfall sind immer aber die Punkte 2.1 (Aktualisierung Rechnerzertifikat im internen Zertifikatsspeicher) und 2.2 (Aktualisierung des Java-Zertifikatsspeicher) betroffen.

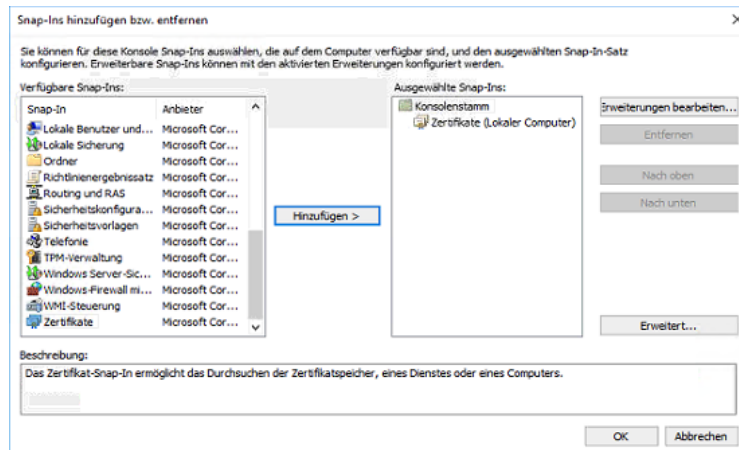
2.1 Aktualisierung Rechnerzertifikat im internen Zertifikatsspeicher

Die Verwaltung der Zertifikate wird durch das Windowsbetriebssystem durch einen internen Speicher vorgenommen. Darauf greifen nicht nur die auf dem System installierten Browser zu, es kann können auch weitere Dienste wie der Remote-Desktopdienst oder der Internet Information Server diesen nutzen. Entsprechend müssen die verwendeten Zertifikate in diesem Speicher eingelesen bzw. verwaltet werden.

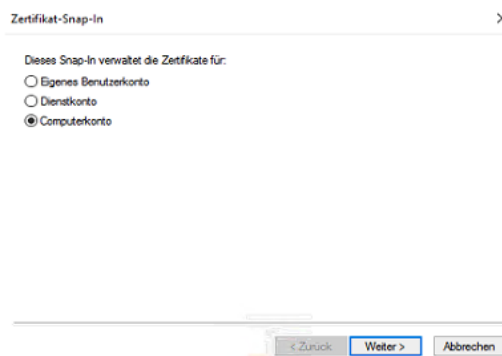
2.1.1 Bereinigen des Zertifikatsspeichers

Zunächst wird das vorhandene und veraltete Zertifikat aus dem Zertifikatsspeicher gelöscht. Dies wird über die Windows Management Konsole vorgenommen.

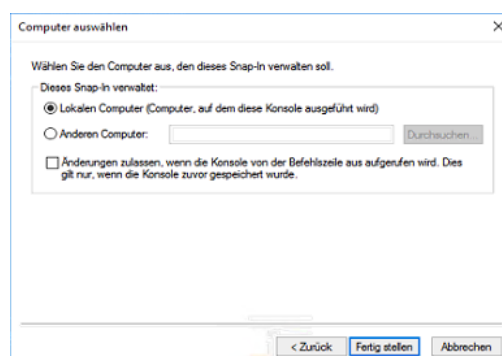
Schritt 1: Öffnen der Windows Management Konsole über den Befehl mmc in einem DOS-Fenster.

Schritt 2: Hinzufügen des Snap-Ins „Zertifikate“

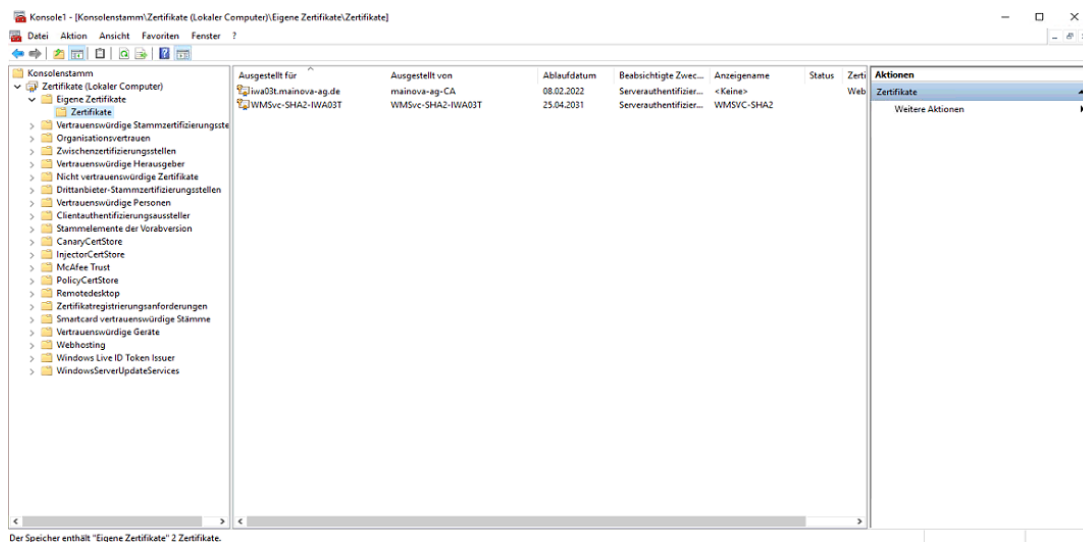
Dabei die generelle Verwaltung des Rechners auswählen:



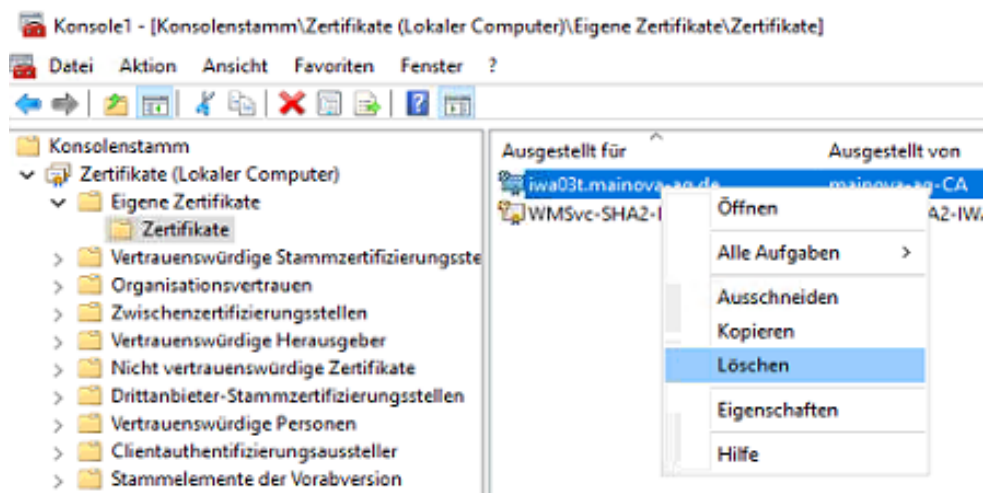
Da der lokale Rechner verwaltet werden soll, an dieser Stelle die Voreinstellung „Lokaler Computer“ belassen:



Schritt 3: Um die lokalen Zertifikate des Rechners auszuwählen und bearbeiten zu können, im Menübaum über *Eigene Zertifikate* > *Zertifikate* die auf dem Rechner lokal abgelegten Zertifikate anwählen:



Schritt 4: Alte, vorhandene Zertifikate können über das Kontextmenü der rechten Maustaste gelöscht werden:



2.1.2 Importieren eines Zertifikats

Der einfachste Weg, um ein Zertifikat auf einem Rechner in den internen Zertifikatsspeicher zu importieren, ist das Öffnen der cer-Datei auf dem Rechner und dann über die Funktion *Zertifikat installieren...* dieses einzulesen.

Schritt 1: Zertifikat öffnen (Entweder über Doppelklick oder über das Kontextmenü im Dateieexplorer:



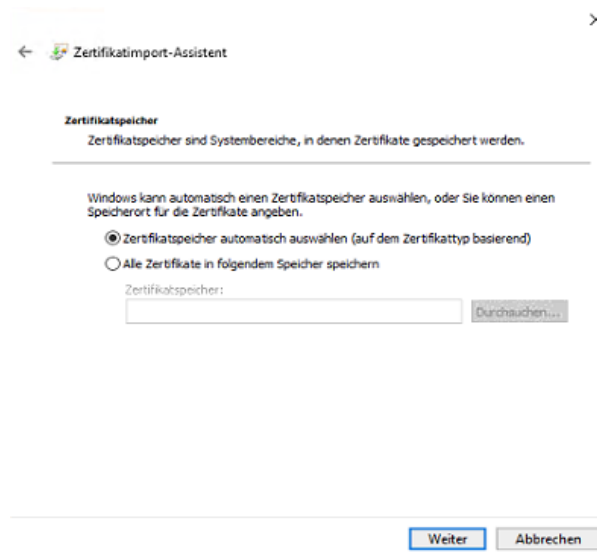
Schritt 2: Auswahl der Funktion *Zertifikat installieren...*

Schritt 3: Im Importassistenten als Speicherort *lokaler Computer* auswählen:

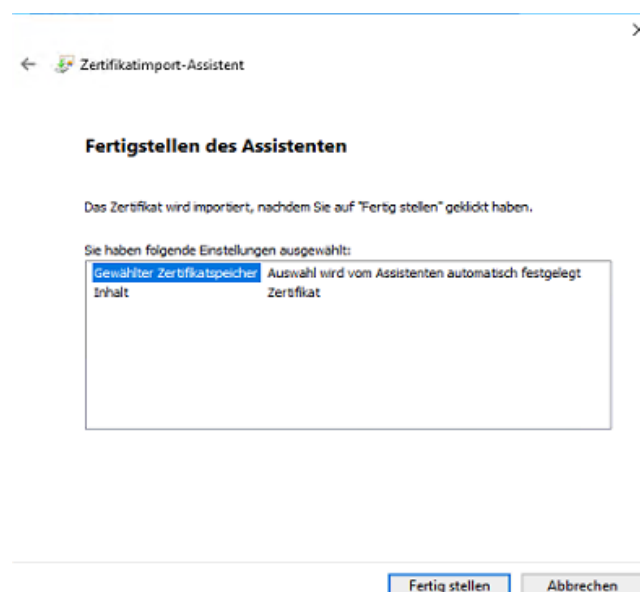


Dies ist notwendig, da das Zertifikat für die https-Bindung im IIS verwendet werden soll und nicht nur lokal für den angemeldeten (administrativen) Benutzer.

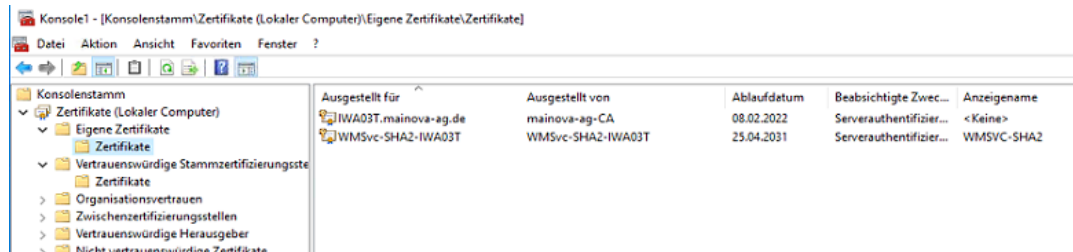
Schritt 4: Den Zertifikatsspeicher automatisch durch das System auswählen lassen:



Schritt 5: Nach erfolgreichem Import des Zertifikats über den Button *Fertig stellen* den Import abschließen:



Wird nun wieder in der Windows Management-Konsole der Knoten Zertifikate aufgerufen, taucht das neue Zertifikat an entsprechender Stelle auf:



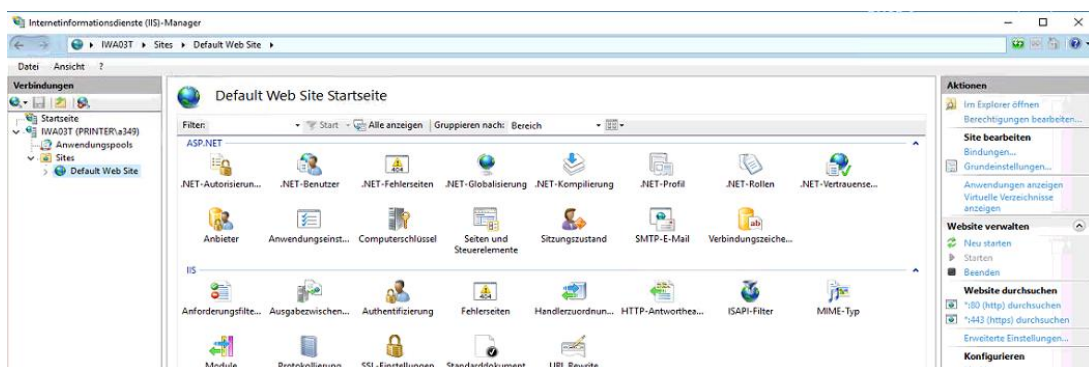
Durch das Importieren des Zertifikats in den zentralen Zertifikatsspeicher steht das Zertifikat nun auch dem Internet Information Server zur Verfügung.

2.1.3 Zuweisen eines Zertifikats im IIS

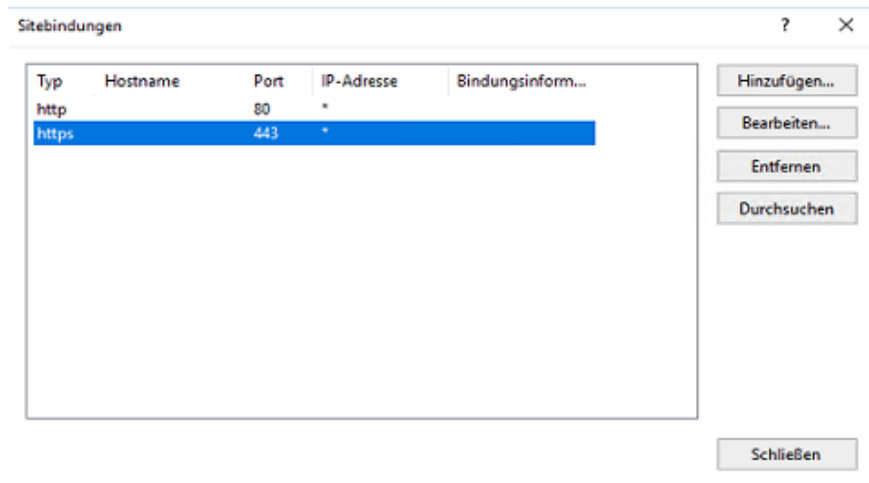
Die Konfiguration der Zertifikate für den Internet Information Server kann über die Managementkonsole des IIS einfach vorgenommen werden.

Der Aufruf des Internetinformationsdienst (IIS)-Manager erfolgt über

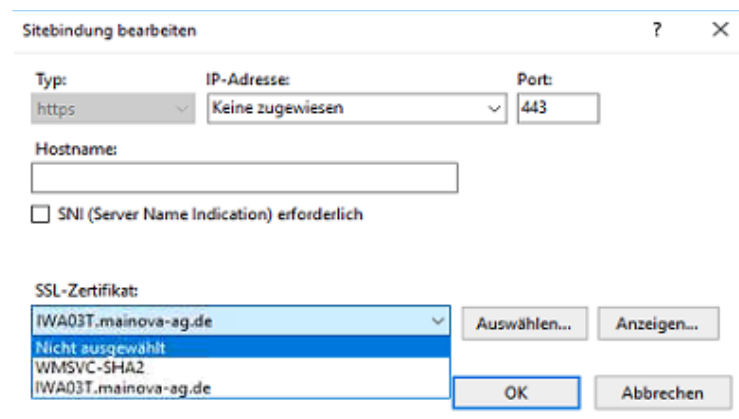
System & Sicherheit > Verwaltung > InternetInformationManager (IIS):



Für die Verwendung eines Zertifikats für https wird im Knoten des Default Web Servers der Eintrag Bindungen ausgewählt. Hier sollten zwei Bindungen vorhanden sein: http für eine http-Verbindung auf Port 80 und https für https-Verbindungen auf Port 443. Da nur die https-Verbindung ein Zertifikat benötigt, wird diese Bindung nun ausgewählt:



Über die Funktion *Bearbeiten* können nun die Details dieser Bindung eingestellt und verändert werden:



In einem Pulldown-Menü werden die Zertifikate des Servers angezeigt. Nun kann das aktuelle Zertifikat für die https-Verbindung ausgewählt und anschließend mittels OK übernommen werden.

2.2 Aktualisierung des Java-Zertifikatsspeicher

Für einen https-Zugriff ist es erforderlich, dass auch das im Apache Tomcat hinterlegte JAVA die für https-erforderlichen Zertifikate bekannt sind. Diese werden im eigenen Zertifikatsspeicher cacerts von JAVA abgelegt.

Dieser Zertifikatsspeicher liegt unter

```
<JAVA_HOME>\lib\security\cacerts
```

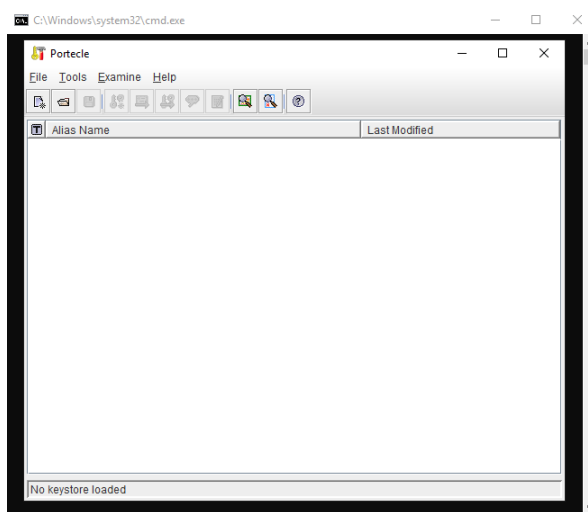
Dabei ist zu beachten, dass im Java-Zertifikatsspeicher alle Zertifikate der Server abgelegt werden, die über https miteinander kommunizieren, also z.B. auch das Zertifikat des WMPS-Servers oder ArcGIS-Servers im Zertifikatsspeicher des WBAU-Servers.

Für eine vereinfachte Verwaltung dieses Zertifikatsspeichers empfehlen wir das freie Tool Portecle. Bei den von uns durchgeführten Installationen liegt das Tool meist parallel zur ApacheTomcat-Installation in einem eigenen Verzeichnis.

Da das Tool ebenfalls auf Java basiert, ist es am einfachstem, es über eine Batch-Datei zu starten, in der die Angabe zur Java-Installation hinterlegt ist.

Starten Sie zunächst das Tool über die bereitgestellte Batch-Datei

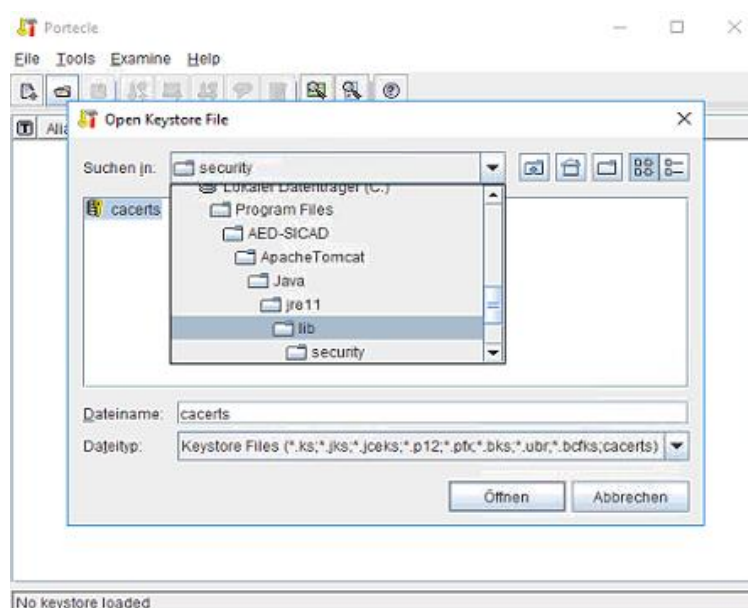
```
C:\Program Files\AED-SICAD\portecle-1.11_batch\portecle.bat
```



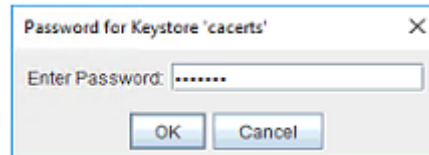
Über den Button "Open Keystore File" kann nun die entsprechende cacert-Datei ausgewählt werden.

In der Oberfläche kann man hierzu über das Dateiverzeichnis browsen. Die von uns für den Tomcat verwendete Java-Installation befindet sich parallel zur Tomcat-Installation. So findet man den Zertifikatsspeicher für Java unter

```
C:\Program Files\AED-SICAD\ApacheTomcat\Java\jre11\lib\security\cacerts
```

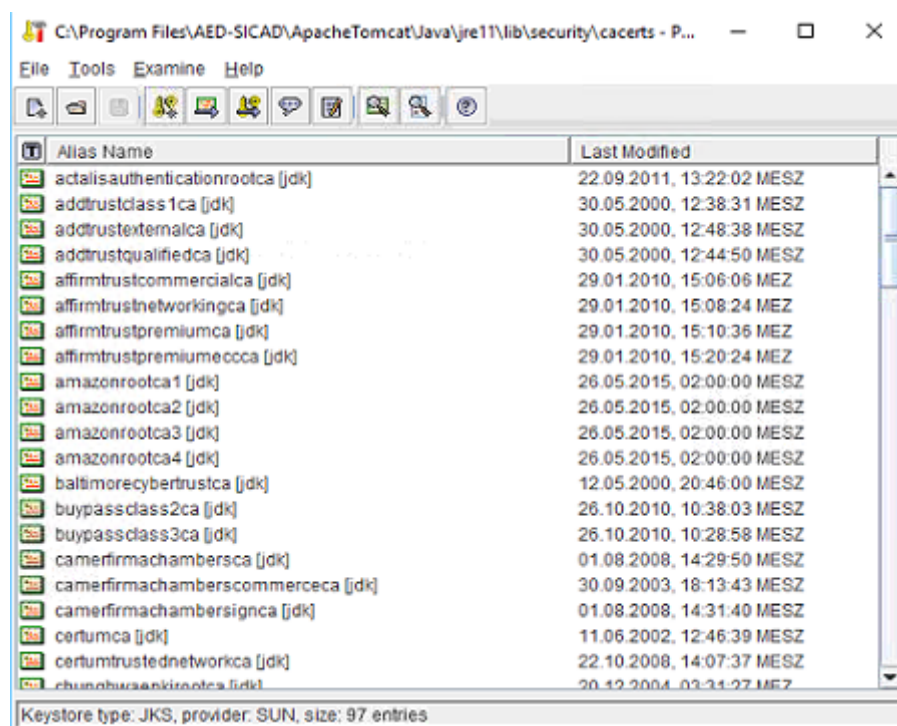


Für das Öffnen des Zertifikatsspeicher ist ein Passwort erforderlich:

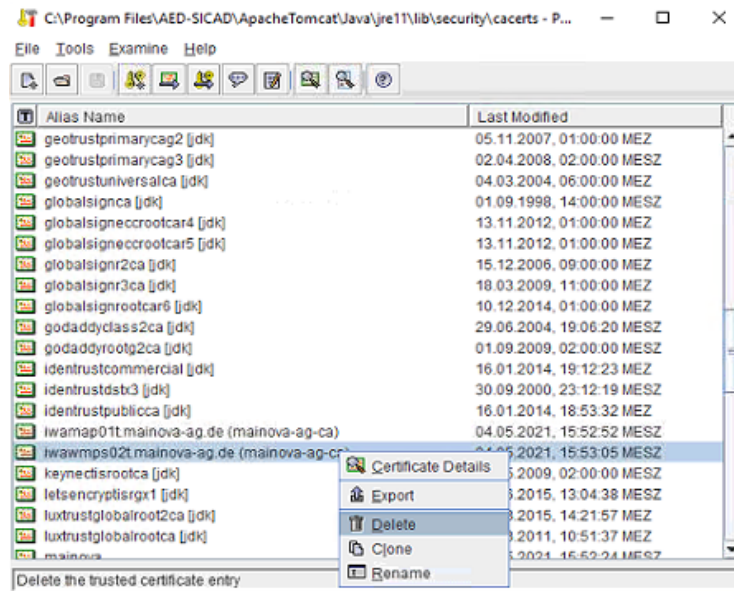


Im Auslieferungszustand von Java ist dies ‚changeit‘

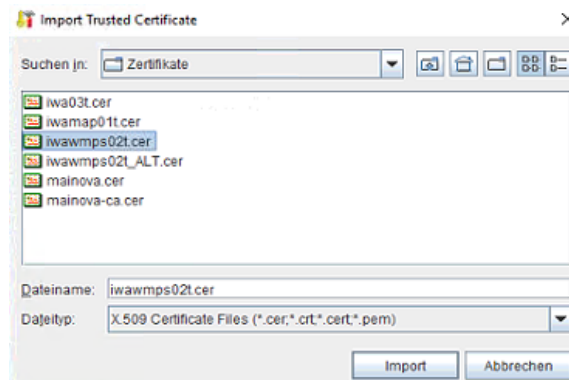
Anschließend öffnet sich der Zertifikatsspeicher und die vorhandenen und bereits importierten Zertifikate werden angezeigt:



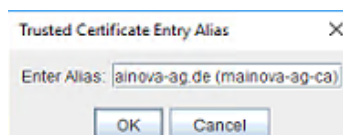
Im Zertifikatsspeicher können nun über das Kontextmenü der rechten Maustaste vorhandene (alte) Zertifikate gelöscht werden:



Über die Funktion „Import Trusted Certificate“ können neue (aktuelle) Zertifikate importiert werden.



Dabei fragt das Tool nach dem entsprechenden Anzeigenamen des Zertifikats. Diese Einstellung kann mittels OK einfach übernommen werden:



Das neu importierte Zertifikat ist nun im Zertifikatsspeicher eingelesen. Ein entsprechender Eintrag wird angezeigt:

identrustpublicca [jdk]	16.01.2014, 18:53:32 MEZ
iw903t mainova-ag.de (mainova-ag-ca)	17.06.2021, 14:46:42 MESZ
iwamap01t mainova-ag.de (mainova-ag-ca)	04.05.2021, 15:52:52 MESZ
iwawmps02t mainova-ag.de (mainova-ag-ca)	17.06.2021, 14:46:12 MESZ
keytool	06.05.2000, 02:00:00 MESZ

Anschließend sollte der Zertifikatsspeicher gespeichert und schließlich auch geschlossen werden.

Hinweis: Die Kennung, unter der das Batchskript aufgerufen wurde, muss über entsprechende Schreibrechte für die cacerts-Datei verfügen. Andernfalls kann die Datei nicht gespeichert werden.

Nach dem Import des Zertifikats in den Java-Zertifikatsspeicher muss der Tomcat für die Verwendung dieser Zertifikate noch durchgestartet werden

2.2.1 Hinweise mit dem Arbeiten mit dem Java-Zertifikatsspeicher:

Da alle Zertifikate der untereinander kommunizierenden Server in der cacerts-Datei abgelegt sein müssen, ist es ausreichend, die cacerts-Datei nur auf einem Server anzupassen und diese dann anschließend auf alle anderen Server zu kopieren.

2.2.2 Einlesen der Zertifikate mittels Kommandozeile

Alternativ kann ein Zertifikat auch mittels Kommandozeile in den Zertifikatsspeicher eingelesen werden. Hierzu muss das Kommandotool keytool verwendet werden, welches im /bin-Verzeichnis der Java-Installation liegt.

Damit ergibt sich dann folgende Kommando:

```
"C:\Program Files\AED-SICAD\ApacheTomcat\Java\jre11\bin\ \
    keytool" -import <path_to_cert-file>\<cert-file>.crt
    -alias <certificate_name>
- keystore "C:\Program Files\AED-SICAD\ApacheTomcat\Java\ \
    \jre11\lib\security\cacerts" -storepass changit
```

Oder als Block:

```
"C:\Program Files\AED-SICAD\ApacheTomcat\Java\jre11\bin\keytool" -import  
<path_to_cert-file>\<cert-file>.cert -alias <certificate_name> - keystore  
"C:\Program Files\AED-SICAD\ApacheTomcat\Java\jre11\lib\security\ca-  
certs" -storepass changit
```

Auch hier muss das Passwort für den Zertifikatsspeicher über den Aufrufparameter `-storepass` angegeben werden.

2.3 Aktualisieren der Zertifikate im ArcGIS Server

2.3.1 ArcGIS-Server und Portal for ArcGIS

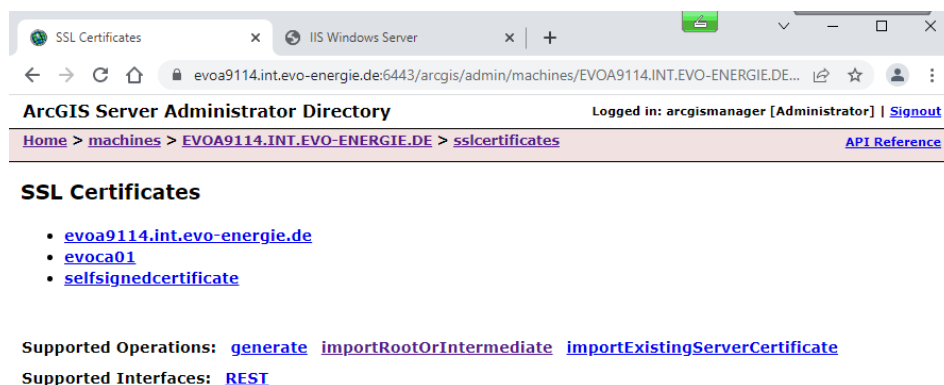
Für einige Verwaltungsarbeiten ist auch ein direkter Zugriff mittels https auf den ArcGIS Server bzw. Portal for ArcGIS notwendig. Dies wird gewöhnlich über den Port 6443 (ArcGIS-Server) bzw. 7443 (Portal for ArcGIS) vorgenommen. Über die administrative Oberfläche kann hier auch das für https notwendige Zertifikat eingespielt werden.

Der ArcGIS Server Administrator kann über die URL

https://<server_name>:<port>/arcgis/admin

aufgerufen werden. Die Anmeldung ist über dieselbe administrative Kennung geschützt, die auch für den ArcGIS Manager verwendet wird.

Die Zertifikatsverwaltung ist über die Menüpunkte *home* > *machines* > *<server_name>* > *sslcertificates* zu erreichen:



Für eine korrekte Auswertung des Zertifikats, welches für den Server bestimmt ist, muss auch das davon abgeleitete Stammzertifikat eingelesen werden. Dies wird über die Funktion *importRootOrIntermediate* vorgenommen. Hierbei muss die entsprechende cer-Datei ausgewählt und auf den Server hochgeladen werden, in dem das Zertifikat für die Beglaubigung des Serverzertifikats enthalten ist.

The screenshot shows a web browser window with the URL `evoa9114.int.evo-energie.de:6443/arcgis/admin/machines/EVOA9114.INT.EVO-ENERGIE.DE...`. The page title is "ArcGIS Server Administrator Directory" and the user is logged in as "arcgismanager [Administrator]". The breadcrumb navigation is "Home > machines > EVOA9114.INT.EVO-ENERGIE.DE > sslcertificates > importRootOrIntermediate". The main heading is "Import Root Certificate". The form contains the following fields:

- Alias:**
- Root CA Certificate:** `EVOCA01.int.evo-energie.de.cer`
- Format:**
-

Der Benutzer sollte dabei einen sprechenden Alias vergeben, so dass später das Zertifikat auch seinem Zweck zugeordnet werden kann.

Der Import des eigentlichen Serverzertifikats wird über die Funktion *importExistingServerCertificates* vorgenommen. Auch hier ist das Auswählen der entsprechenden Zertifikatsdatei erforderlich:

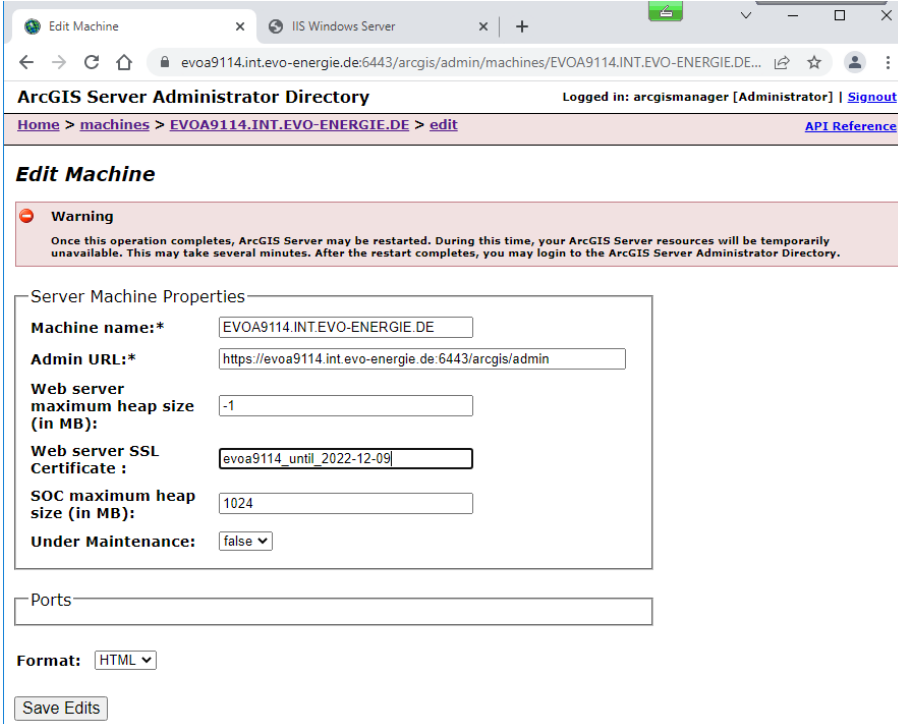
The screenshot shows a web browser window with the URL `evoa9114.int.evo-energie.de:6443/arcgis/admin/machines/EVOA9114.INT.EVO-ENERGIE.DE...`. The page title is "ArcGIS Server Administrator Directory" and the user is logged in as "arcgismanager [Administrator]". The breadcrumb navigation is "Home > machines > EVOA9114.INT.EVO-ENERGIE.DE > sslcertificates > importExistingServerCertificate". The main heading is "Import Existing Server Certificate". The form contains the following fields:

- Certificate password:**
- Alias:**
- Certificate File:** `evoa9114.int.evo-energie.de.pfx`
- Format:**
-

Auch hier sollte man einen entsprechend sprechenden Alias vergeben für das Zertifikat vergeben, so dass es später seinem Zweck zugeordnet werden kann.

Da es sich hier um das vom internen Webserver verwendete Zertifikat handelt, das dann die https-Verschlüsselung mit dem Clientrechner vornimmt, ist hier die Angabe des Zertifikatspassworts erforderlich. Zudem muss die Zertifikatsdatei als pfx-Datei vorliegen.

Die Zuordnung zum derzeit verwendeten Zertifikat wird über die Funktion *edit* unter dem Serverknoten im Menü vorgenommen:



The screenshot shows the ArcGIS Server Administrator Directory interface. The browser address bar indicates the URL: `evoa9114.int.evo-energie.de:6443/arcgis/admin/machines/EVOA9114.INT.EVO-ENERGIE.DE...`. The page title is "ArcGIS Server Administrator Directory" and the user is logged in as "arcgismanager [Administrator]". The breadcrumb navigation shows "Home > machines > EVOA9114.INT.EVO-ENERGIE.DE > edit".

The main content area is titled "Edit Machine" and contains a warning message: "Warning: Once this operation completes, ArcGIS Server may be restarted. During this time, your ArcGIS Server resources will be temporarily unavailable. This may take several minutes. After the restart completes, you may login to the ArcGIS Server Administrator Directory." Below the warning is a form for "Server Machine Properties" with the following fields:

- Machine name:*
- Admin URL:*
- Web server maximum heap size (in MB):
- Web server SSL Certificate:
- SOC maximum heap size (in MB):
- Under Maintenance:

Below the properties form is a "Ports" section with an empty text input field. At the bottom, there is a "Format" dropdown menu set to "HTML" and a "Save Edits" button.

Als Wert wird das vorhin importierte Zertifikat des Servers angegeben.

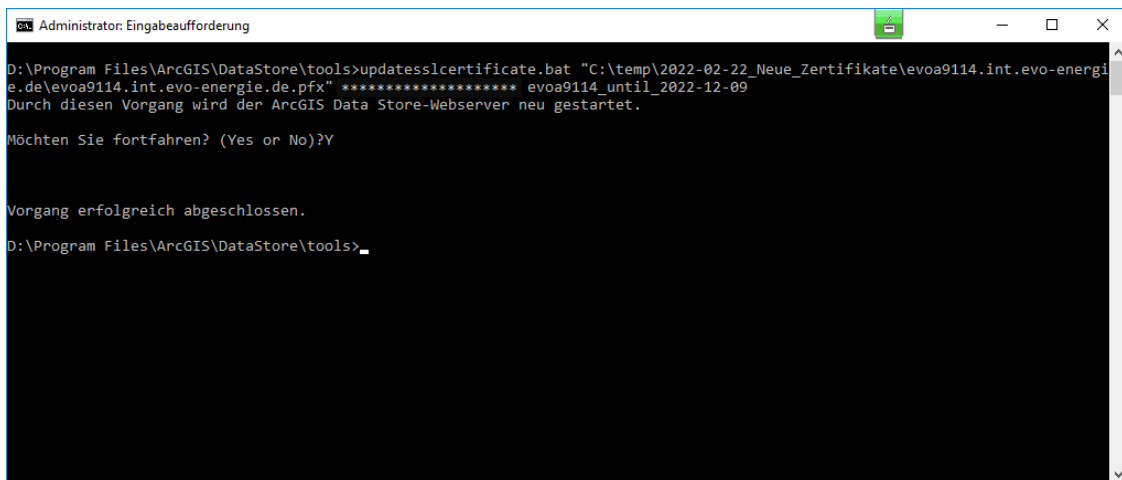
2.3.2 ArcGIS Data Store

Der ArcGIS Data Store bietet keine Weboberfläche für den Austausch des SSL-Zertifikats an. Die Aktualisierung erfolgt hier mit Hilfe der Batch-Datei *updatesslcertificate*. Dieses befindet sich auf dem ArcGIS-Data-Store-Server im Unterordner *tools* der ArcGIS-Data-Store-Installation, z.B.:

```
C:\Program Files\ArcGIS\DataStore\tools
```

Vorgehensweise:

1. Öffnen der Kommandozeile im administrativen Modus
2. Navigation zum Ordner *tools* der Data-Store-Installation
3. Eingabe des Kommandos
`updatesslcertificate <Pfad zum Zertifikat> <Passwort> <Alias-Name>`
4. Rückfrage bestätigen



```
Administrator: Eingabeaufforderung
D:\Program Files\ArcGIS\DataStore\tools>updatesslcertificate.bat "C:\temp\2022-02-22_Neue_Zertifikate\evoa9114.int.evo-energie.de\evoa9114.int.evo-energie.de.pfx" ***** evoa9114_until_2022-12-09
Durch diesen Vorgang wird der ArcGIS Data Store-Webserver neu gestartet.
Möchten Sie fortfahren? (Yes or No)?Y
Vorgang erfolgreich abgeschlossen.
D:\Program Files\ArcGIS\DataStore\tools>
```

2.4 Aktualisierung der Zertifikate in Apache Tomcat

Je nach Konfiguration des Apache Tomcats für die Kommunikation sind unterschiedliche Arbeitsschritte notwendig:

- Ist der Apache Tomcat über die AJP-Schnittstelle und einen ISAPI-Redirect direkt am Webserver angebunden, übernimmt dieser die Kommunikation über https. Damit sind keine weiteren Schritte im Falle einer Aktualisierung des Zertifikats notwendig. Diese ist schon durch die Aktualisierung im Webserver vorgenommen worden
- Wird der Apache Tomcat hingegen über den eingebauten Webserver angesprochen, muss auch hier das Zertifikat erneuert werden. Die genaue Konfiguration für die Einbindung des Zertifikats kann unterschiedlich sein. Details dazu kann der Tomcat-Dokumentation (siehe <https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html>) entnommen werden.

Sind die für die Zertifizierung verwendeten Dateien erneuert worden, ist normal ein Restart des Tomcats ausreichend, um das neue Zertifikat zu verwenden.

2.5 Aktualisierung der Zertifikate in SOLR (WebNAV pro)

Die SSL-Konfiguration des Apache SOLR wird über die Datei

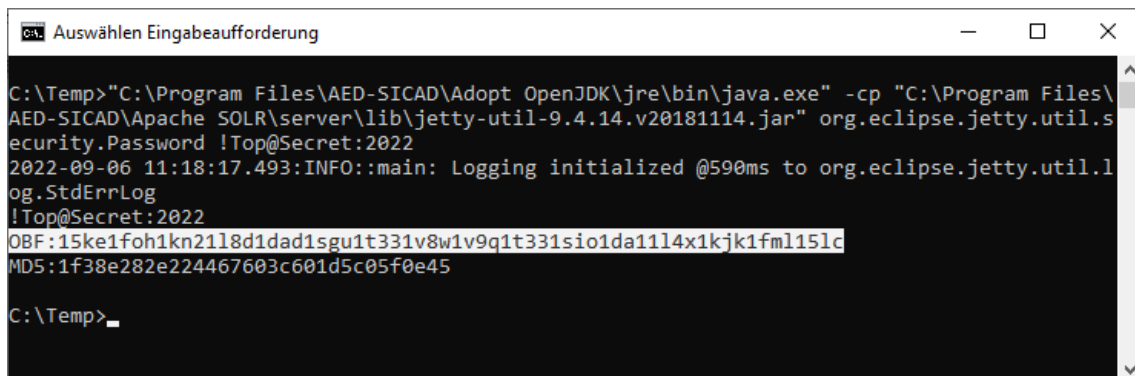
```
<SOLR-Ordner>\bin\solr.in.cmd
```

vorgenommen.

2.5.1 Behandlung der Passwörter

Die Passwort-Verarbeitung im Skript *solr.in.cmd* funktioniert nur dann fehlerfrei, wenn das Passwort ausschließlich aus Buchstaben und Zahlen besteht. Sind Sonderzeichen enthalten, sollte die Passwortverschleierung des SOLR-Servers verwendet werden, z.B.:

```
"<JAVA-Pfad>\bin\java.exe" -cp "<SOLR-Pfad>\server\lib\jetty-  
util-<Versionsangabe>.jar" org.eclipse.jetty.util.security.Pass-  
word !Top@Secret:2022
```



```
C:\Temp>"C:\Program Files\AED-SICAD\Adopt OpenJDK\jre\bin\java.exe" -cp "C:\Program Files\  
AED-SICAD\Apache SOLR\server\lib\jetty-util-9.4.14.v20181114.jar" org.eclipse.jetty.util.s  
ecurity.Password !Top@Secret:2022  
2022-09-06 11:18:17.493:INFO::main: Logging initialized @590ms to org.eclipse.jetty.util.l  
og.StdErrLog  
!Top@Secret:2022  
OBF:15ke1foh1kn21l8d1dad1sgu1t331v8w1v9q1t331sio1da11l4x1kjk1fml15lc  
MD5:1f38e282e224467603c601d5c05f0e45  
C:\Temp>
```

Die im Bild markierte Zeichenfolge stellt dann den verschleierte Wert des Passworts dar. Das "OBF:" am Anfang ist für den SOLR das Signal, die Angabe entsprechend zu behandeln.

2.5.2 Direktes Einbinden einer PFX-Datei

Sofern das auszutauschende Zertifikat im PFX-Format vorliegt, kann es direkt eingebunden werden.

Die Voraussetzungen dazu sind

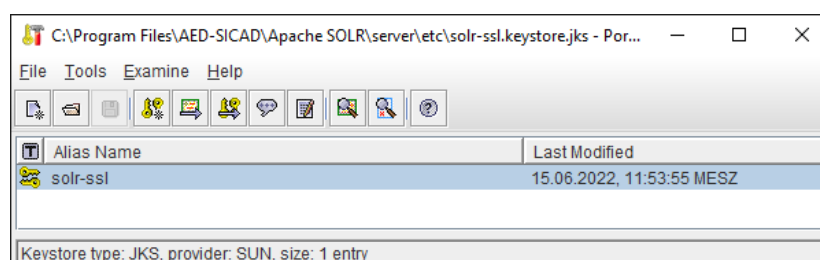
- der Dateiname darf keine Leerzeichen enthalten
- die PFX-Datei befindet sich im Ordner `<SOLR-Ordner>\server\etc`
- Passwort mit Sonderzeichen ist verschleiert angegeben
- die PFX-Datei wird auch als `TRUST-STORE` angegeben

```
99 REM Enables HTTPS. It is implicitly true if you set SOLR_SSL_KEY_STORE. Use this config
100 REM to enable https module with custom jetty configuration.
101 set SOLR_SSL_ENABLED=true
102 REM Uncomment to set SSL-related system properties
103 REM Be sure to update the paths to the correct keystore for your environment
104 set SOLR_SSL_KEY_STORE=etc/vhm-mn-xxx.pfx
105 set SOLR_SSL_KEY_STORE_PASSWORD=OBF:1f361n0mlneg1xmult331xmglnbalmwolf18
106 set SOLR_SSL_TRUST_STORE=etc/vhm-mn-xxx.pfx
107 set SOLR_SSL_TRUST_STORE_PASSWORD=OBF:1f361n0mlneg1xmult331xmglnbalmwolf18
108 REM Require clients to authenticate
109 set SOLR_SSL_NEED_CLIENT_AUTH=false
110 REM Enable clients to authenticate (but not require)
111 set SOLR_SSL_WANT_CLIENT_AUTH=false
112 REM SSL Certificates contain host/ip "peer name" information that is validated by default. Setting
113 REM this to false can be useful to disable these checks when re-using a certificate on many hosts
114 set SOLR_SSL_CHECK_PEER_NAME=true
115 REM Override Key/Trust Store types if necessary
116 set SOLR_SSL_KEY_STORE_TYPE=PKCS12
117 set SOLR_SSL_TRUST_STORE_TYPE=PKCS12
```

2.5.3 Verwendung eines Java-Key-Stores

Ein Java-Key-Store kann ebenfalls verwendet werden. Dabei sollten folgende Bedingungen eingehalten werden:

- der Dateiname des Key-Stores enthält keine Leerzeichen
- der Key-Store befindet sich im Ordner `<SOLR-Ordner>\server\etc`
- der Alias für das importierte Zertifikat lautet `solr-ssl`
- selbes Passwort für den Key-Store und das Zertifikat
- Passwort mit Sonderzeichen wird verschleiert angegeben



In der Konfigurationsdatei des Service ist dann folgender Eintrag vorzunehmen:

```
99 REM Enables HTTPS. It is implicitly true if you set SOLR_SSL_KEY_STORE. Use this config
100 REM to enable https module with custom jetty configuration.
101 set SOLR_SSL_ENABLED=true
102 REM Uncomment to set SSL-related system properties
103 REM Be sure to update the paths to the correct keystore for your environment
104 set SOLR_SSL_KEY_STORE=etc/solr-ssl.keystore.jks
105 set SOLR_SSL_KEY_STORE_PASSWORD=OBF:lsnzlv2hlxtplp4flt33lp5blxttlvixlspr
106 REM set SOLR_SSL_TRUST_STORE=etc/solr-ssl.keystore.jks
107 REM set SOLR_SSL_TRUST_STORE_PASSWORD=secret
108 REM Require clients to authenticate
109 REM set SOLR_SSL_NEED_CLIENT_AUTH=false
110 REM Enable clients to authenticate (but not require)
111 REM set SOLR_SSL_WANT_CLIENT_AUTH=false
112 REM SSL Certificates contain host/ip "peer name" information that is validated by default. Setting
113 REM this to false can be useful to disable these checks when re-using a certificate on many hosts
114 REM set SOLR_SSL_CHECK_PEER_NAME=true
115 REM Override Key/Trust Store types if necessary
116 set SOLR_SSL_KEY_STORE_TYPE=JKS
117 REM set SOLR_SSL_TRUST_STORE_TYPE=JKS
```

Werden bezüglich TRUST-Store keine Angaben gemacht, wird der Standard-TRUST-Store der zugrunde gelegten Java-Installation verwendet (vgl. Kapitel 2.2).