

VertiGIS

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	2.3.2	Brandstetter
		und SOLR Server	2.5	



Inhaltsverzeichnis

1 Einführu	ing	4
1.1	Allgemeine Informationen	4
1.2 H	Hinweise zur Verwendung des Dokuments	4
1.3 E	Betroffene Komponenten	5
2 Aktu	alisierung 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 (<u>https://letsencrypt.org/</u>) 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
 - ISAPI-Redirect mit AJP-Anbindung an Apache Tomcat f
 ür 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
 - 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
 - Kernbestandteil für die indizierte über WebNAVpro von BARAL.



- ArcGIS Server, Portal for ArcGIS und ArcGIS Data Store

 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"

erfügbare Snap-Ins:				usgewählte Snap-Ins:	
Snap-in Colaie Benutzer und Colaie Sicherung Ordner Rabuting und RAS Sicherheitskonfgura S	Anbieter Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	^	Hinzufügen >	IIII Konsolenstamm ② Zerofikate (Lokaler Computer)	Erweiterungen bearbeiten. Entfernen Nach oben Nach unten
2ertifikate	Microsoft Cor Microsoft Cor	v			Erweitert

Dabei die generelle Verwaltung des Rechners auswählen:

Dieses Soan-In verwaitet die Zettifikati	e für:	
C Eserces Peru darefonde		
Computerkonto		

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

Wählen Sie den Computer a	aus, den dieses Snap-In verwalten soll.
Dieses Snap-In verwaltet:	
 Lokalen Computer (Co 	omputer, auf dem diese Konsole ausgeführt wird)
O Anderen Computer:	Durchsuchen
Anderungen zulasser git nur, wenn die Kor	1, wenn die Konsole von der Befehlszeile aus aufgerufen wird. Dies nsole zuvor gespeichet wurde.



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:

Datei Aktion Ansicht Favoriten Fenster ?	2								- 6
Concientame Concienta	Augentell för Ginaðit mánova-ag de Gill Missee SH42-IWA03T	Ausgestellt von mainova-ag-CA WMSvc-5H42-TWAQ3T	Abluddatum 08.02.202 25.04.2031	Besbichtigte Zwec Serverauthentifüier Serverauthentifüier	Anzigename «Keine» WMSVC-SHA2	Status	Zerti Web	Aktionen Zertrikate Weitere Aktionen	

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 Dateiexplorer:

-	Zertifi	katsinfo	ormatio	nen			
Diese	es Zertifi	kat ist	für folg	ende Zw	recke b	eabsichti	gt:
	Garance	FCOR IO	enuare	nes kem	otecomp	oters	
	Ausgest	ellt für:	IWA0	3T.maino	va-ag.d	e	
	Ausgest	ellt von	: maino	va-ag-C/	4		
	Gültig al	10.06	2021 b	is 08.02	2. 2022		
			-			A	11-
			Zertifika	t installie	ren	Ausstelle	srenklarun

Schritt 2: Auswahl der Funktion Zertifikat installieren...

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

Willkommen
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauensisten und Zertifikatssperilsten vom Datenträger in den Zertifikatspeicher.
Ein von einer Zertifizierungsstolle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert verden.
Speicherort
○ Aktueller Benutzer
Lokaler Computer:
Kicken Sie auf "Weiter", um den Vorgang fortzusetzen.



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:

Zertifikatspeiche Zertifikatspe	r icher sind Systembereich	ne, in denen Zert	fikate gespeiche	rt werden.
Windows kar Speicherort	nn automatisch einen Ze für die Zertifikate angeb	rtifikatspeicher au en.	uswählen, oder S	ie können einen
 Zertifi 	katspeicher automatisch	auswählen (auf	dem Zertifikattyp	basierend)
⊖ Alle Z	ertifikate in folgendem Sp	peicher speichern		
Zertif	ikatspeicher:			
				Durchauchen

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

🐓 Zertifikatimpo	rt-Assistent				
Fertigstel	len des Assis	tenten			
Das Zertifikat v	vird importiert, nach	dem Sie auf 1	Fertig stellen" ge	klickt haben.	
Sie haben folge	nde Einstellungen a	usgewählt:			
Gewählter Ze Inhalt	rtifikatspeicher Au Ze	swahl wird vo rtifikat	m Assistenten au	tomatisch fe	stgelegt



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

🚡 Konsole1 - [Konsolenstamm\Zertifikate (Lokaler C	omputer)\Eigene Zertifikate\Zertifik	ate]			
Tatei Aktion Ansicht Favoriten Fenster	?				
🗢 🔿 🙍 📅 📋 🙆 😹 🕅					
Konsolenstamm Zertifikate (Lokaler Computer) Eligene Zertifikate Zertifikate Zertifikate Zertifikate Granisationsvertrauen Servischensettifizierungsstellen Wertrauenswürdige Herautgeber	Ausgestellt für 및 WWA93T.mainova-ag.de 및 WMSvc-SHA2-IWA03T	Ausgestellt von mainova-ag-CA WMSvc-SHA2-IWA03T	Ablaufdetum 08.02.2022 25.04.2031	Beabsichtigte Zwec Serverauthentifizier Serverauthentifizier	Anzeigename <keine> WMSVC-SHA2</keine>

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 Internetinformationdienst (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:

yp	Hostname	Port	IP-Adresse	Bindungsinform	Hinzufügen
ttp		80			Passhaitan
ttps		443	•		bearbeiten
					Entfernen
					Durchsuchen

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

itebindung b	earbeiten				?	×
Тур:	_	IP-Adresse:	Po	rt:	1	
https	Y	Keine zugewiesen	44	13	ļ	
TO SCHOULD						
SNI (Serv	er Name l	ndication) erforderlich				
SNI (Serv	er Name l	ndication) erforderlich				
SNI (Serv	er Name li it:	ndication) erforderlich				
SNI (Servi SSL-Zertifika	er Name li it: inova-ag.e	ndication) erforderlich	Auswäh	len	Anzeigen	
SNI (Servi SSL-Zertifika WA03T.mai	er Name li it: inova-ag.o wahit	ndication) erforderlich	Auswäh	len	Anzeigen	
SNI (Servi SSL-Zertifika WA03T.mai Nicht ausge WMSVC-SH	er Name li it: inova-ag.s wahit A2	ndication) erforderlich	Auswäh	len	Anzeigen	

In einem Pulldown-Menü werden die Zertifikate des Severs 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\protecle.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\	\setminus
	security\cacert	S

🛐 Open Key	store File		×
Suchen in:	security		80 0-
B cacerts	Program Files AED-SICAD ApacheTomcat Java Jro11 Nib Security		
Dateiname:	cacerts		
Dateityp:	Keystore Files (*.ks;*.jks;*.jceks;*.p12	*.pfx:*.bks;*.ubr;*.bcfks;cac	erts) 🔽
		Öffnen Abbr	echen



Für das Öffnen des Zertifikatsspeicher ist ein Passwort erforderlich:

Password for Keystore 'cacerts'		
Enter Password:		
OK Cancel		

Im Auslieferungszustand von Java ist dies ,changeit'

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

C:\Program Files\AED-SICAD\ApacheTomcat\Java\jre11\lib	b\security\cacerts - P	\times
Eile Tools Examine Help		
C. = = # # # # # # •		
I Alias Name	Last Modified	
actalisauthenticationrootca (jdk)	22.09.2011, 13:22:02 MESZ	-
addtrustclass1ca [jdk]	30.05.2000, 12:38:31 MESZ	
addtrustexternalca (jdk)	30.05.2000, 12:48:38 MESZ	_
addtrustqualifiedca (jdk)	30.05.2000, 12:44:50 MESZ	
affirmtrustcommercialca (jdk)	29.01.2010, 15:06:06 MEZ	1
affirmtrustnetworkingca [jdk]	29.01.2010, 15:08:24 MEZ	
affirmtrustpremiumca (jdk)	29.01.2010, 15:10:36 MEZ	
affirmtrustpremiumeccca [jdk]	29.01.2010, 15:20:24 MEZ	
amazonrootca1 [jdk]	26.05.2015, 02:00:00 MESZ	
amazonrootca2 (jdk)	26.05.2015, 02:00:00 MESZ	
amazonrootca3 (jdk)	26.05.2015, 02:00:00 MESZ	
🖼 amazonrootca4 (jdk)	26.05.2015, 02:00:00 MESZ	
baltimorecybertrustca [jdk]	12.05.2000, 20:46:00 MESZ	
🔤 buypassclass2ca [jdk]	26.10.2010, 10:38:03 MESZ	
😂 buypassclass3ca [jdk]	26.10.2010, 10:28:58 MESZ	
camerfirmachambersca (jdk)	01.08.2008, 14:29:50 MESZ	
camerfirmachamberscommerceca [jdk]	30.09.2003, 18:13:43 MESZ	
🛅 camerfirmachambersignca [jdk]	01.08.2008, 14:31:40 MESZ	
certumca [jdk]	11.06.2002, 12:46:39 MESZ	
certumtrustednetworkca (jdk)	22.10.2008, 14:07:37 MESZ	
Chunghwaankirootea lidki	20.12.2004_03-31-27 ME7	-
Keystore type: JKS, provider: SUN, size: 97 entries		



17/27

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

🚝 C:\Program Files\AED-SICAD\ApacheTomcat	\Java\jre11\lib\security\cac	erts - P — 🗆	×
Eile Tools Examine Help			
	8. 0		
I Alias Name	Last I	Modified	
geotrustprimarycag2 (jdk)	05.11	.2007, 01:00:00 MEZ	•
geotrustprimarycag3 [jdk]	02.04	.2008, 02:00:00 MESZ	
geotrustuniversalca [jdk]	04.03	2004, 06:00:00 MEZ	
globalsignca [jdk]	01.09	.1998, 14:00:00 MESZ	
globalsigneccrootcar4 [jdk]	13.11	2012, 01:00:00 MEZ	
globalsigneccrootcar5 [jdk]	13.11	.2012, 01:00:00 MEZ	
globalsignr2ca [jdk]	15.12	.2006, 09:00:00 MEZ	
globalsignr3ca [jdk]	18.03	.2009, 11:00:00 MEZ	
globalsignrootcar6 [jdk]	10.12	.2014, 01:00:00 MEZ	-
godaddyclass2ca [jdk]	29.06	.2004, 19:06:20 MESZ	
godaddyrootg2ca [jdk]	01.09	.2009, 02:00:00 MESZ	-
identrustcommercial [jdk]	16.01	2014, 19:12:23 MEZ	
identrustdsb(3 (jdk)	30.09	.2000, 23:12:19 MESZ	-
identrustpublicca [jdk]	16.01	.2014, 18:53:32 MEZ	
Iwamap01t.mainova-ag.de (mainova-ag-ca)	.04.05	2021, 15:52:52 MESZ	
Iwawmps02t.mainova-ag.de (mainova-ag-c:	Contribute Dataila	2021, 15:53:05 MESZ	
🔤 keynectisrootca (jdk)	Cost Certificate Details	2009, 02:00:00 MESZ	
Ietsencryptisrgx1 [jdk]	B Export	.2015, 13:04:38 MESZ	
luxtrustglobalroot2ca [jdk]	1 Delete	.2015, 14:21:57 MEZ	
iuxtrustglobalrootca [jdk]	B Clone	.2011, 10:51:37 MEZ	-
i mainova		2021 15:52:24 MESZ	_
Delete the trusted certificate entry	E Kename		

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

🛐 Import Tri	isted Certificate ×
Suchen in:	Zertifikate
iwa03t.c iwamapi iwawmp iwawmp mainova mainova	or Micer S02tcer s02t_ALT.cer cer ca.cer
Dateiname:	iwawmps02t.cer
Dajeityp:	X.509 Certificate Files (*.cer;*.crt*.cert*.pem)
	Import Abbrechen

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

Trusted Certif	icate Er	ntry Alias	×			
Enter Alias: ainova-ag.de (mainova-ag-ca)						
	ок	Cancel				



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

identrustpublicca (jdk)	16.01.2014, 18:53:32 MEZ
iwa03t.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
keypertisrontra (idk)	26.05.2009.02:00:00 MES7

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:



Oder als Block:

```
"C:\Program Files\AED-SICAD\ApacheTomcat\Java\jre11\bin\keytool" -import
<path_to_crt-file>\<crt-file>.crt -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 *importRootOrIn-termediate* vorgenommen. Hierbei muss die entsprechende cer-Datei ausgewählt und auf den Server hochgeladen werden, in dem das Zertifikat für die Beglaubigung des Serverzertifikats enthalten

Vert	iGIS [™]	White Paper Aktualisierung http	s-Zertifikate				21/27
 Import R ← → C 	oot Certificate ×	IIS Windows Server at.evo-energie.de:6443/arcgi	× + s/admin/machines/EVO/	ے A9114.INT.EVO-ENERGI	 ✓ - 「 E.DE	×	
ArcGIS S	Server Administra achines > EVOA9114.	tor Directory INT.EVO-ENERGIE.DE >	Log ssicertificates > imp	gged in: arcgismanage	r [Administrator] iate API F	<u>Signout</u> Reference	
Import Import Alias Root C	Root Certificate Root Certificate EVO A Certificate: Date	te CA01 i auswählen EVOCA01.int.e	vo-energie.de.cer				-
Formati	HTML 🗸						

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:

Import Existing Certificate	× 📀 IIS Windows Server 🛛 🗙 📔	+	~ -		×		
← → C ☆ 🔒 evoa91	14.int.evo-energie.de:6443/arcgis/admin/mach	ines/EVOA9114.INT.EVO-ENERGIE.D	E 12 1	<u>ل</u>	:		
ArcGIS Server Adminis	ArcGIS Server Administrator Directory Logged in: arcgismanager [Administrator] Signou						
Home > machines > EVOA91	114.INT.EVO-ENERGIE.DE > <u>sslcertificate</u>	es > importExistingServerCerti	ficate <u>A</u>	PI Refer	<u>ence</u>		
Import Existing Ser	rver Certificate						
Import Existing Server	r Certificate						
Certificate password:							
Alias:	evoa9114_until_2022-12-09						
Certificate File:	Datei auswählen evoa9114.int.evo-energie.de	.pfx					
Format: HTML V							
Submit							

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 im 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:

S Edit Machine	× 🔇 IIS Windows Server	× +	<u>_</u>	~ – 🗆 X
← → C ☆ 🔒 evoa	a9114.int.evo-energie.de:6443/arcg	is/admin/machines/EVOA	9114.INT.EVO-ENERGI	E.DE 🖻 🖈 😩 :
ArcGIS Server Admin	istrator Directory	Log	ged in: arcgismanage	r [Administrator] <u>Signout</u>
Home > machines > EVOA	9114.INT.EVO-ENERGIE.DE >	edit		API Reference
Edit Machine				
 Warning Once this operation compluravailable. This may take 	etes, ArcGIS Server may be restarted several minutes. After the restart of	I. During this time, your Are smpletes, you may login to	GIS Server resources w the ArcGIS Server Admi	vill be temporarily inistrator Directory.
Server Machine Prope	erties			
Machine name:*	EVOA9114.INT.EVO-ENERGIE.D	E		
Admin URL:*	https://evoa9114.int.evo-energie.c	le:6443/arcgis/admin		
Web server maximum heap size (in MB):	-1			
Web server SSL Certificate :	evoa9114_until_2022-12-09			
SOC maximum heap size (in MB):	1024			
Under Maintenance:	false 🗸			
Ports				
Format: HTML 🗸				
Save Edits				

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





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 <u>https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html</u>) 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
```



Die im Bild markierte Zeichenfolge stellt dann den verschleierten 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:1f361n0mlneg1xmult331xmg1nbalmwolf18 106 set SOLR_SSL_TRUST_STORE=PASSWORD=OBF:1f361n0mlneg1xmult331xmg1nbalmwolf18 107 set SOLR_SSL_TRUST_STORE_PASSWORD=OBF:1f361n0mlneg1xmult331xmg1nbalmwolf18 108 REM Require clients to authenticate 109 REM set SOLR_SSL_NEED_CLIENT_AUTH=false 110 REM set SOLR_SSL_NEED_CLIENT_AUTH=false 111 REM Set SOLR_SSL_WATT_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_KEP_ER_NAME=true 115 REM Override Key/Trust Store types if necessary 116 set SOLR_SSL_KEY_STORE_TYPE=PKCS12

2.5.3 Verwendung eines Java-Key-Stores

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

halten 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 implictly 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	<pre>set SOLR SSL KEY STORE=etc/solr-ssl.keystore.jks</pre>
105	set SOLR_SSL_KEY_STORE_PASSWORD=OBF:lsnzlv2hlxtplp4flt33lp5blxttlvlxlspr
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. Settin
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).