Manuelle Installation/Importierung des TeleSec GlobalRoot Class 2 Zertifikates

Windows

Überprüfung des Zertifikats

Drücken Sie die Windows Taste + R

Geben Sie nun certmgr.msc in das Suchfeld ein:

💷 Ausfi	ühren X
	Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.
Ö <u>f</u> fnen:	certmgr.msc 🗸 🗸
	OK Abbrechen Durchsuchen

Klicken Sie am linken Verzeichnisbaum auf den Eintrag Vertrauenswürdige Stammzertifizierungstellen, dann auf Zertifikate.

Nun sollte innerhalb der rechten Liste das Zertifikat zu finden sein unter der Bezeichnung **TeleSec** GlobalRoot Class 2.

藩 certmgr - [Zertifikate - Aktueller Benutzer\Vertrauenswürdige Stammzertifizierungsstellen\Zerti — 🛛 🛛 🗙							
Datei Aktion Ansicht ?							
🗢 🄿 🙍 📰 🔏 🖦 🗙 🗟 😖 📓 🖬	🗢 🔿 🙍 📧 🐇 🖼 🗙 🗟 🔒 📓 🖬						
🗊 Zertifikate - Aktueller Benutzer	Ausgestellt für	Ausgestellt von	AI ^				
> iii Eigene Zertifikate	Starfield Class 2 Certificatio	Starfield Class 2 Certificatio	29				
 Vertrauenswürdige Stammzertifizierungsstellen 	Starfield Root Certificate A	Starfield Root Certificate A	01				
Zertifikate	StartCom Certification Aut	StartCom Certification Aut	17				
> Organisationsvertrauen	Symantec Enterprise Mobil	Symantec Enterprise Mobil	15				
Zwischenzertifizierungsstellen	Thawte Premium Server CA	Thawte Premium Server CA	01				
Vertrauenswürdige Herausgeber	Thawte Primary Root CA	thawte Primary Root CA	17				
Nicht vertrauenswürdige Zertifikate	Vicht vertrauenswürdige Perausgebei Nicht vertrauenswürdige Zertifikate Drittanbieter-Stammzertifzierungsstellen Thavte Timestamping CA						
> Drittanbieter-Stammzertifizierungsstellen							
> 📔 Vertrauenswürdige Personen	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	02				
> 🧾 Clientauthentifizierungsaussteller	T-TeleSec GlobalRoot Class 3	T-TeleSec GlobalRoot Class 3	02				
> 📔 Andere Personen	🔄 UTN-USERFirst-Object	UTN-USERFirst-Object	09				
> Cocal NonRemovable Certificates	🔄 VeriSign Class 3 Public Pri	VeriSign Class 3 Public Pri	17				
> Zertifikatregistrierungsanforderungen	🔄 VeriSign Class 3 Public Pri	VeriSign Class 3 Public Pri	17				
> Smartcard vertrauenswürdige Stämme	📮 VeriSign Universal Root Cer	VeriSign Universal Root Cer	02 🗸				
< >	<		>				
Der Speicher enthält "Vertrauenswürdige Stammzertifizierungsstellen" 47 Zertifikate.							

Sollte das Zertifikat nicht vorhanden sein, folgen Sie den nächsten Schritten zur Nachinstallation.

Zertifikat nachinstallieren

Laden Sie sich das Zertifikat herunter unter:

https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.crt

Öffnen Sie das heruntergeladene Zertifikat

Nun erscheint folgendes Fenster:

- Windows
 - Überprüfung des Zertifikats
 - Zertifikat
 - nachinstallieren
- LinuxMacOS
 - MacOS
 - Überprüfung des Zertifikats
 - Zertifikat
 - nachinstallieren
 - Anpassung der Eigenschaften

属 Zertifikat	×				
Allgemein Details Zertifizierungspfad					
Zertifikatsinformationen					
Dieses Zertifikat ist für folgende Zwecke beabsichtigt:					
Garantiert die Identität eines Remotecomputers Garantiert dem Remotecomputer Ihre Identität Schützt E-Mail-Nachrichten Alle ausgegebenen Richtlinien					
Ausgestellt für: T-TeleSec GlobalRoot Class 2					
Ausgestellt von: T-TeleSec GlobalRoot Class 2					
Gültig ab 01.10.2008 bis 02.10.2033					
Zertifikat installieren Ausstellererklärung					
OK					

Hier auf Zertifikat installieren klicken und danach mehrmals fortfahren mit weiter

Im folgenden Fenster die Option "Lokaler Computer" auswählen:

 Frifikatimport-Assistent 	×
Willkommen	
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrilsten vom Datenträger in den Zertifikatspeicher.	
Ein von einer Zertifizierungsstelle 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 werden.	
Speicherort Aktueller Benutzer	
Klicken Sie auf "Welter", um den Vorgang fortzusetzen.	
Abbrech	en

Nun mit "Ja" die Installation nochmals bestätigen



Im nächsten Schritt die Option "Zertifikatsspeicher automatisch auswählen" setzen und mit weiter fortfahren:

Zertifikatimport-Assistent	
Zertifikatspeicher	
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.	
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.	
② Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)	
Alle Zertifikate in folgendem Speicher speichern	
Zertifikatspeicher:	
Durchsuchen.	
Weiter Abbrev	cher

Abschließend mit Fertig stellen die Installation abschließen:

 Ertifikatimport-Assistent 	×
Fertigstellen des Assistenten	
Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.	
Sie haben folgende Einstellungen ausgewählt:	_
Gewählter Zertifikatspeicher Auswahl wird vom Assistenten automatisch festgelegt Inhalt Zertifikat	
Fertig stellen Abbrech	ien

Nach erfolgreicher Installation erscheint die Meldung "Der Importvorgang war erfolgreich"



Nun haben Sie das Zertifikat erfolgreich installiert.

Linux

Anmerkung: Einige – vor allem Ubuntu basierte Distributionen – verfügen über einen automatisierten Zertifikate-Installer. Hier-zu müssen Sie die Zertifikate nur herunterladen und durch einen Doppelklick installieren.

Laden Sie sich das Zertifikat herunter unter:

https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.crt

Falls Ihre Distribution über keinen Zertifikate-Installer verfügt, können Sie auch folgendes Vorgehen via Terminal verwenden:

Öffnen Sie ein Terminal.

Verschieben Sie das heruntergeladene Zertifikat in den Ordner /usr/local/share/ca-certificates:

sudo mv <Pfad-zum-Zertifikat> /usr/local/share/ca-certificates

Falls der Ordner nicht existiert, kann dieser mit folgendem Befehl angelegt werden:

sudo mkdir /usr/local/share/ca-certificates

Nun das Zertifikat installieren:

sudo update-ca-certificates

```
sudo mkdir /usr/local/share/ca-certificates; sudo wget -P /usr/local/share
/ca-certificates https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-
TeleSec_GlobalRoot_Class_2.crt && sudo update-ca-certificates
```

Das Zertifikat befindet sich nun unter /etc/ssl/certs und lässt sich entsprechend importieren.

MacOS

Überprüfung des Zertifikats

Sie können das Vorhandensein des Zertifikats direkt mit der Schlüsselbundverwaltung überprüfen:

- 1. Rufen Sie über die globale Suche die Schlüsselbundverwaltung auf.
- Finden Sie dort mittels der lokalen Suchfunktion den Eintrag TeleSec GlobalRoot Class 2, sollten Sie wie unten beschrieben die Eigenschaften überprüfen. Ist kein derartiger Eintrag zu sehen, müssen Sie das Zertifikat einzeln nachinstallieren.

Schlüsselbundverwaltung					
Klicke hier, um den	Schlüsselbu	Q telesec	0		
Schlüsselbunde Anmeldung Lokale Objekte System System-Roots	Certificate	T-TeleSec GlobalR Root-Zertifizierungsins Ablaufdatum: Sonntag ⊘ Dieses Zertifikat ist	oot Class 2 stanz , 2. Oktober 2033 gültig.		
	Name	ec GlobalRoot Class 2 ec GlobalRoot Class 3	 Art Zertifikat Zertifikat 		
Kategorie					
Alle Objekte Passwörter Sichere Notizen Meine Zertifikate Schlüssel Zertifikate					

Wenn das Zertifikat bei Ihnen vorhanden ist, können Sie sofort zu den Eigenschaften springen.

Sollte dies bei Ihnen nicht der Fall sein, folgen Sie den nachfolgenden Schritten zur Nachinstallation des Zertifikats.

Zertifikat nachinstallieren

- 1. Laden Sie sich das Zertifikat herunter unter: https://www.pki.dfn.de/fileadmin/PKI/zertifikate/T-TeleSec_GlobalRoot_Class_2.crt
- 2. Starten Sie die Schlüsselbundverwaltung über die globale Suche
- 3. Wählen Sie nun den Reiter Anmeldung aus und anschließend Ablage Objekte importieren:

🗯 Schlüsselbundverwaltung		Ablage	Bearbeiten	Darstellung	Fenster	Hilfe
Klicke hier, um den Schlüsselbund "A		Neues Neues Neuer Neuel	Passwort sichere Notiz Schlüsselbun dentitätseinst	 Id tellung	2.	第N bu 企業N て第N
🔐 Anmeldung	(\circ)	Objekt	te importieren	1		☆ 第1
LOKAIE ODJEKTE		Objek	te exportieren			THE
System	Nama	Schlüs Schlüs	selbund hinzi selbund "Ann	ufügen neldung" löscl	nen	☆業A て業≪
1.	Y <key></key>	Schlie	Ben			жw
	% <key> /. Apple Per /. com.apple /. com.apple /. com.apple /. com.apple</key>	Ort öff Inform Schlüs Alle Sc	fnen ationen sselbund "Ann chlüsselbunde	neldung" sper sperren	ren	策I 発L
Kategorie	com.apple	Schlüs	selbund "Ann	neldung" als S	tandard sid	chern
Alle Objekte	/ com.apple	.gs.icloud.f	amily.auth.com.a	pple.account.App	lelDAuthentio	cation.token
🛴 Passwörter 🧧 Sichere Notizen	com.apple.gs.icloud.storage.buy.com.apple.account.AppleIDAuthentication.token com.apple.gs.idms.hb.com.apple.account.AppleIDAuthentication.token					
Meine Zertifikate	. com.apple.gs.idms.ln.com.apple.account.AppleIDAuthentication.token					
Schlüssel					ken	
📴 Zertifikate	com.apple	.gs.news.au .gs.pb.auth	.com.apple.ac	count.AppleIDAu unt.AppleIDAuthe	thentication.to intication.toke	oken en
	A comappie	.ga.po.autri	apple.acco	ant appletoAutrie	introactori.toki	

Wählen Sie nun das heruntergeladene Zertifikat aus und klicken Sie auf Öffnen

Das Zertifikat wird nun ohne weiter Eingabeaufforderung installiert.

Anpassung der Eigenschaften

Klicken Sie in der Schlüsselbundverwaltung doppelt auf das TeleSec GlobalRoot Class 2 Zertifikat.

Nun erscheint ein Fenster mit der Detailansicht.

Klappen Sie nun den Teilbaum Vertrauen auf (Doppelklick)

Ändern Sie die Einstellung Bei Verwendung dieses Zertifikats auf Immer vertrauen

	T-TeleSec GlobalRoot Class 2			
Certificate Certificate Certificate Certificate Certificate Construction Certificate Construction Certificate Construction Certificate Construction Certificate C	GlobalRoc zierungsinsta n: Sonntag, 2 iische Somm ertifikat ist gü	ht Class 2 nz . Oktober 2033 um 01:59:59 erzeit Itig.		
Bei Verwendung dieses	Zertifikats:	Immer vertrauen	○ ?	
Secure Sockets I S/MIME (S EAP (Extensible Auth IP Secu Code- 2 X.509-Standar	Layer (SSL) ecure Mail) eentication) rity (IPsec) Signierung Zeitstempel drichtlinien	Immer vertrauen		
♥ Details Name des Inhaber Lan Firm Organisationseinhe Allgemeiner Nam	d DE a T-System it T-System e T-TeleSec	is Enterprise Services GmbH is Trust Center : GlobalRoot Class 2		

Schließen Sie das Fenster und geben Sie auf Nachfrage Username und Passwort Ihres Administrator-Accounts an.