# Sicherheitszertifikate

Serverzertifikate dienen zur Absicherung von Netzwerkverbindungen über das SSL-Protokoll (bzw. TLS-Protokoll). SSL-Protokolle werden meistens in Verbindung mit HTTP verwendet, was als HTTPS bezeichnet wird.

- Server authentisiert sich gegenüber Client
- Verbindung wird verschlüsselt

## Fehlermeldung bei fehlendem Zertifikat

Citrix	Receiver
4	Anwendung kann nicht gestartet werden. Wenden Sie sich an den Helpdesk und stellen Sie folgende Informationen bereit: Verbindung mit Citrix XenApp-Server ist nicht möglich.SSL-Fehler 61: Sie stufen den Aussteller 'BSZ-BW CA - G02' des Sicherheitszertifikats des Servers nicht als vertrauenswürdig ein.
	ОК

Sollte eine Meldung über fehlende Zertifikate erscheinen, kann hier das Zertifikat inkl. Kette heruntergeladen werden: https://pki.pca.dfn.de/dfn-ca-global-g2 /cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2&RA\_ID=330 Damit der Client der Zertifizierungsstelle vertraut, muss das zugehörige Wurzelzertifikat (z.B. Deutsche Telekom Root CA 2) vorinstalliert sein.

### Vorgehensweise bei manueller Installation eines Sicherheitszertifikats

• Internet Explorer

### Installation eines Sicherheitszertifikats im Internet Explorer

Um ein Zertifikat im Internet Explorer zu installieren, rufen Sie die Seite CA-Zertifikate auf und wählen Sie:

- ° Wurzelzertifikat
- DFN-PCA-Zertifikat
- DFN-CA Global G2-Zertifikat

Wählen Sie das gewünschte Zertifikat aus und gehen Sie auf "öffnen", folgen Sie anschließend unter "Zertifikat installieren" den Anweisungen des Zertifikatimport-Assistenten. Das Wurzelzertifikat wird unter Vertrauenswürdige Stammzertifizierungsstellen abgespeichert, alle weiteren Zertifikate unter Zwischenzertifizierungsstellen.

fikat	83	Contract (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
emein Details Zertifizierungspfad		Zertifikatspeicher auswählen Wählen Sie den Zertifikatspeicher, der verwendet werden soll
Zertifikatsinformationen Dieses Zertifikat ist für folgende Zwecke b	Zertifikatimport-Assistent	Eigene Zertifikate
<ul> <li>Garantiert die Identität eines Remotecomp</li> <li>Garantiert dem Remotecomputer Ihre Ider</li> <li>Schützt E-Mail-Nachrichten</li> <li>1.3.6.1.4.1.22177.300.1.1.4</li> <li>1.3.6.1.4.1.22177.300.30</li> <li>2.2.3.140.1.2.2</li> </ul>	Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Ze	Organisationsvertrauen     Organisationsvertrauen     Zwischenzertützierungsstellen     G. Active Directory-Benutzerobjekt     Vertrauenswirdige Herausgeber
	Windows kann automatisch einen Zertifikatspeicher Speicherort für die Zertifikate angeben.	Physikalischen Speicher anzeigen
Ausgestellt für: DFN-Verein Certificatio	<ul> <li>Zertifikatspeicher automatisch auswählen (au</li> <li>Alle Zertifikate in folgendem Speicher speiche</li> </ul>	OK Abbrecher
Ausgestellt von: T-TeleSec GlobalRoot C	Zertifikatspeicher:	Durchsuchen
Gültig ab 22. 02. 2016 bis 23. 02. 20		
Zertifikat installieren eitere Informationen über <u>Zertifikate</u>	Weitere Informationen über Zertifikatspeicher	

#### Wo sind alle abgespeicherten Zertifikate im Internet Explorer zu finden?

#### Internetoptionen: Zertifikate

Um sich alle im Browser gespeicherten Zertifikate anzeigen zu lassen, öffnen Sie "Extras" und wählen Sie den Menupünkt "Internetoptionen". Unter "Internetoptionen" können Sie sich unter dem Reiter "Inhalte" alle Zertifikate anzeigen lassen.

	n 🛧 🎕
Drucken	۰.
Datei	+
Zoom (100 %)	+
Sicherheit	•
Website dem Startmenü hinzufügen	
Downloads anzeigen	Strg+J
Add-Ons verwalten	
F12 Entwicklertools	
Zu angehefteten Sites wechseln	
Einstellungen der Kompatibilitätsansicht	
Websiteprobleme melden	
Internetoptionen	
Info	

Mozilla Firefox

### Installation eines Sicherheitszertifikats im Mozilla Firefox

Um ein Zertifikat im Firefox zu installieren, rufen Sie die Seite CA-Zertifikate auf und wählen Sie:

- Wurzelzertifikat
- DFN-PCA-Zertifikat
- ° DFN-CA Global G2-Zertifikat

Nachdem Sie das gewünschte Zertifikat ausgewählt haben, öffnet sich ein Fenster. Die Häkchen sollten bei allen Kritierien gesetzt werden. Unter "Ansicht" kann das Zertifikat überprüft werden.

Herunterladen des Zertifikats	X			
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.				
Soll "DFN-Verein Global Issuing CA" für die folgenden Zwecke vertraut werden?				
Dieser CA vertrauen, um Websites zu identifizieren.				
Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.				
Dieser CA vertrauen, um Software-Entwickler zu identifizieren.				
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.				
Ansicht CA-Zertifikat überprüfen				
OK Abbrechen	]			

### Wo sind alle abgespeicherten Zertifikate im Firefox zu finden?

Einstellungen: Zertifikate

Um sich alle im Browser gespeicherten Zertifikate anzeigen zu lassen, öffnen Sie das Menu und wählen Sie "Einstellungen". Unter "Einstellungen" können Sie sich unter "Erweitert" alle Zertifikate anzeigen lassen.



### Quellen

- https://www.pki.dfn.de/fileadmin/PKI/Mitteilungen/DFN86\_SSL\_Authentisierung.pdf
   https://www.pki.dfn.de/fileadmin/PKI/Anleitung\_DFN-Test-PKI.pdf
   https://www.pki.dfn.de/faqpki/