# Prüfen einer digitalen Signatur in einer PDF

## Voraussetzungen -Wurzelzertifikate importieren

A Für das Prüfen einer Signatur in einem PDF-Dokument mit Adobe Acrobat müssen Sie vorab Wurzelzertifikate importieren - ohne eingebettetes Wurzelzertifikat erscheinen die Signaturen als ungültig. Folgen Sie dafür einfach den Anleitungen auf dieser Seite.

▲ To verify a signature in a PDF document with Adobe Acrobat, you must first import root certificates - without an embedded root certificate, the signatures appear as invalid. Simply follow the instructions on this page to set it up.

#### Inhalt dieser Seite

- Voraussetzungen Wurzelzertifikate importieren
- GÉANT-TCS Wurzelzertifikat (beantragt via Sectigo)
- importieren /
- - Update security settings
  - Wurzelzertifikat installieren mittels FDF-Datei /
  - Install root certificate using a FDF file
  - Zertifikats-Richtlinieneinschränkung ändern /
  - Change certificate policy restriction
     Tale See Weinschaftlicht (begestersterie DEN) important
- T-TeleSec Wurzelzertifikat (beantragt via DFN) importieren
- Fehlermeldung bei Fehlen des Wurzelzertifikats
  Erkennen einer (LTV-fähigen) Signatur

Wurzelzertifikate - Merkmale und Funktion

- auch Stammzertifikat oder Root-Zertifikat genannt
  - selbstsigniertes Zertifikat einer oberen Zertifizierungsstelle (Root-CA), welches somit auf kein übergeordnetes Zertifikat verweist
  - dient zur Validierung der Vertrauenswürdigkeit aller untergeordneten Zertifikate

Das bedeutet: Damit eine digitale Signatur, welche auf einem Nutzerzertifikat von der DFN oder GÉANT-TCS basiert, als gültig validiert wird, muss entweder das mit der Signatur verbundene Zertifikat oder das Wurzelzertifikat entsprechend importiert und als Vertrauensanker festgelegt werden. Am besten wird das Wurzelzertifikat bzw. das Zertifikat der obersten Zertifizierungsstelle in einer Kette von Zertifizierungsstellen importiert.

- self-signed certificate of an upper certification authority (root CA), which therefore does not refer to a higher-level certificate
- is used to validate the trustworthiness of all subordinate certificates

This means that in order for a digital signature based on a user certificate from DFN or GÉANT-TCS to be validated, either the **cer tificate associated with the signature** or the **root certificate** must be **imported** accordingly and defined as the **trust anchor**. It is best to import the root certificate or the certificate of the highest certification authority in a chain of certification authorities.

# GÉANT-TCS Wurzelzertifikat (beantragt via Sectigo) importieren /

# Import GÉANT-TCS root certificate (requested via Sectigo)

#### Sicherheitseinstellungen aktualisieren /

## Update security settings

Als Erstes sollten Sie ihre Sicherheitseinstellungen aktualisieren bzw. in Adobe Acrobat alle Wurzelzertifikate aus der Adobe Approved Trust-Liste (AATL) sowie aus der Trust-Liste der Europäischen Union (EUTL) importieren.

Firstly, you should update your security settings or import all root certificates from the Adobe Approved Trust List (AATL) and the European Union Trust List (EUTL) in Adobe Acrobat.

1. Klicken Sie in Adobe Acrobat im Menü "Bearbeiten" auf den Punkt "Ei nstellungen".

1. In Adobe Acrobat click on the hamburger **Menu** button and then on "**P** references…".

#### Adobe Acrobat Reader DC (32-bit)

Datei	Bearbeiten	Anzeige	Unterschreiben	Fenster	Hilfe
Start	<u> </u>	gängig	C	Ctrl+Z	
Q	C Wied	erherstellen	Shift+C	Ctrl+Z	
	A <u>u</u> ss	chneiden	C	Ctrl+X	
	E Kopie	eren	C	Ctrl+C	
	📋 Ein <u>f</u> ü	gen	C	Ctrl+V	
	<u>L</u> ösch	nen			
	<u>A</u> lles	auswählen	C	Ctrl+A	
	Aus <u>w</u>	ahl aufheber	n Shift+C	Ctrl+A	
	Datei	in <u>Z</u> wischen	ablage kopieren		
	<u>T</u> ext u	und Bilder be	arbeiten		
	🔟 Seite	n löschen			
	🞧 Seite	n drehen			
	Te <u>x</u> t u	ind Bilder sch	hwärzen		
	Schn	appschuss er	rstellen		
	Rech	tschreib <u>p</u> rüft	ung	•	
	Q <u>S</u> uch	en	C	Ctrl+F	
	Erwe	iterte Suche	Shift+C	Ctrl+F	
	Schu	tz		<b>→</b>	
	Ein-/	Ausgab <u>e</u> hilfe		· ·	
	Werk	zeuge <u>v</u> erwa	lten		
	Ei <u>n</u> st	ellungen	(	Ctrl+K	





2. Unter "Vertrauensdienste" klicken Sie auf beide "Jetzt aktualisieren" Schaltflächen, um alle von Adobe sowie von der Europäischen Union ausgelieferten vertrauenswürdigen Wurzelzertifikate zu importieren.

2. Click on the category **Trust Manager** and continue by clicking both "**U pdate Now**" buttons to import all trusted root certificates provided by Adobe and the European Union.



Wurzelzertifikat installieren mittels FDF-Datei /

## Install root certificate using a FDF file

Die Nutzerzertifikate vom GÉANT-TCS basieren auf den Wurzelzertifikaten von Sectigo und je nach Algorithmus des Schlüssels enden Zertifizierungsketten in TCS üblicherweise auf einem der beiden Root-Zertifikate "USERTrust".

Zur Vereinfachung des Imports finden Sie hier zwei FDF-Dateien, die beim Installieren der benötigten Wurzelzertifikate in Adobe Acrobat helfen.

The user certificates from GÉANT-TCS are based on the root certificates from Sectigo and, depending on the algorithm of the key, certification chains in TCS usually end on one of the two root certificates "USERTrust".

To simplify the import, there are two FDF files here that will help with installing the required root certificates in Adobe Acrobat.

Datenaustauschdatei - Kontakt importieren
Sie haben eine Acrobat-FDF-Datenaustauschdatei geöffnet, die die folgenden Daten enthält: Kontaktinformationen
Absender Name: Zentrum für Informations- und Medientechnologie (ZIM) E-Mail-Adresse:
Kontakte zur Liste der vertrauenswürdigen Identitäten hinzufügen Diese Datei beinhaltet Kontaktinformationen für den Versender. Klicken Sie auf "Vertrauen festlegen", um die Optionen zum Einfügen dieses Kontakts in die Liste der vertrauenswürdigen Identitäten festzulegen. Zu den Kontaktinformationen gehören Zertifikate, die nach ihrer Bestätigung zum Prüfen von Unterschriften und zum Verschlüsseln von Dokumenten für den zugehörigen Kontakt verwendet werden. Vertrauen festlegen Schließen

3. Zudem sollten Sie den Haken bei "Vertrauenswürdige Zertifikate von einem Adobe AATL-Server laden" rausnehmen, damit die noch folgenden Installationen von Wurzelzertifikaten nicht beim nächsten automatischen Update von Adobe Acrobat geändert werden

**3.** You should also **uncheck** the box "Load trusted certificates from an Adobe **AATL** server" so that subsequent installations of root certificates are not changed during the next automatic update of Adobe Acrobat

#### FDF-Datenaustauschdateien

Root-Zertifikat USERTrust ECC.fdf

Root-Zertifikat USERTrust RSA.fdf

1. Laden Sie die FDF-Datei "Root-Zertifikat USERTrust ECC.fdf" herunter und öffnen Sie zunächst die FDF-Datei mit Adobe Acrobat

1. Download the FDF file "Root-Zertifikat USERTrust ECC.fdf" and open it in Adobe Acrobat

2. Beim Starten öffnet sich ein Fenster, wo sie auf "Vertrauen festlegen..." klicken

2. When starting, a window opens. Click on "Set Contact Trust..."

3. Danach setzen Sie einen Haken bei "Dieses Zertifikat als vertrauenswürdigen Stamm verwenden" sowie bei "Zertifizierte Dokumente" und klicken auf "OK"

3. Check the "Use this certificate as a trusted root" checkbox as well as the "Certified documents" checkbox and confirm with "OK"

4. Zum Schluss bestätigen Sie die erscheinende Meldung mit "OK"

Kontakteinstellungen importieren	$\times$
Zertifikatdetails	
Thema: USERTrust ECC Certification Authority	
Aussteller: USERTrust ECC Certification Authority	
Verwendung : Zertifikat unterschreiben, Liste zurückgezogener Zertifikate (CRL) unterschreiben	
Ablaufdatum: 19.01.2038 00:59:59	
Vertrauenswürdigkeit Richtlinieneinschränkungen	
Zur erfolgreichen Signaturprüfung muss ein zum Signieren von Dokumenten verwendetes Zertifikat als Vertrauensanker festgelegt werden oder mit einem Vertrauensanker verkettet sein. Für einen Vertrauensanker wird keine Sperrungsüberprüfung des Zertifikas durchgeführt.	
Dieses Zertifikat als vertrauenswürdigen Stamm verwenden	
Bei Unterschriftsvalidierung gilt dieses Zertifikat für folgenden Zweck als vertrauenswürdig:	
Unterschriebene Dokumente oder Daten	
Zertifizierte Dokumente	
Dynamischer Inhalt	
Eingebettete JavaScripts mit hoher Berechtigungsstufe	
Privilegierte Systemvorgänge (Netzwerk, Drucken, Dateizugriff usw.)	
Zertifikatdetails	
Hilfe OK Abbrechen	

4. Finally, confirm the message that appears with "OK"

5. Mit der FDF-Datei "Root-Zertikifat USERTrust RSA.fdf" machen Sie die gleichen Schritte von 1-4.

5. Repeat the steps 1-4 with the FDF file "Root-Zertikifat USERTrust RSA.fdf"

#### Hinweis

Das Wurzelzertifikat der "**USERTrust RSA Certification Authority**" muss nicht unbedingt importiert werden, wenn die Sicherheitseinstellungen wie beschrieben aktualisiert wurden, da das Zertifikat von Adobe Acrobat ausgeliefert wird.

Falls dieses Zertifikat schon drin ist, bekommen Sie diese Meldung:

"1doppeltes(s) Zertifikat(e) verworfen" Klicken Sie einfach auf "OK"

The root certificate of the "**USERTrust RSA Certification Authority**" does not necessarily have to be imported if the security settings have been updated as described, as the certificate is supplied by Adobe Acrobat.

If this certificate is already included, you will receive this message:

"1 duplicate certificate(s) discarded." click "OK"

ie haben eine Ao	robat-FDF-Datenaustausch	datei geöffnet, die die folgen	iden Daten enthält:
Kontaktinfor	mationen		
Absender	Import abgeschlossen		
Na	Importdetails:		
E-Mail-Adre	1 doppelte(s) Zertifkat(e	e) verworfen.	
Kontakte zur L			
Diese Datei			Vertrauen
testlegen", i vertrauensw			en
Zertifikate, von Dokum		ОК	rschlüsseln
		V	ertrauen testlegen

Doch ohne Import mittels der FDF-Datei muss die Richtlinieneinschränkung für das Wurzelzertifikat der "USERTrust RSA Certification Authority" bearbeitet werd en.

However, without importing using the FDF file, the policy restriction for the root certificate of the "USERTrust RSA Certification Authority" must be edited.

## Zertifikats-Richtlinieneinschränkung ändern /

## Change certificate policy restriction



1. Klicken Sie in Adobe Acrobat im Menü "Bearbeiten" auf den Punkt "Einstellungen"

1. In Adobe Acrobat click on the hamburger **Menu** button and then on "**P** references...".

2. In den Einstellungen klicken Sie unter "Unterschriften" "Identitäten und vertrauenswürdige Zertifikate" auf "Weitere..."

2. In the settings, click on the "Signatures" category and then on the "More..." button next to "Identities and Trusted certificates"

3. In das sich öffnende Fenster sollten Sie nun unter "Vertrauenswürdi ge Zertifikate" auf das Zertifikat "USERTrust RSA Certification Authority" klicken bzw. dies markieren und auf "Einstellungen für Vertrauenswürdigkeit bearbeiten" klicken

3. In the window that opens click on "Trusted Certificates" and after selecting the "USERTrust RSA Certification Authority" certificate by clicking on it, click "Edit Trust"

4. Dann wechseln Sie auf den Tab "Richtlinieneinschränkungen" und I öschen den Eintrag bei "Zertifikatsrichtlinie" und bestätigen die Änderungen mit "OK"

**4.** In the window that has opened, switch to the "**Policy Restrictions**" tab and delete what is written in the "**Certificate Policies**" field and confirm the changes with "**OK**"

Digitale IDs	🥖 Einstellungen für Vert	trauenswürdigkeit bearbeite	n 🐂 Importieren	产 Exportieren	🔐 Zertifikatdetails	Entfernen	
Roaming-ID-Konten	Name	Aussteller des Zertifikats	Ablaufdatum				
	Swisscom Diamant CA 2	Swisscom Root CA 2	2022.01.12 08:45:00 Z				
Digitale ID-Dateen	Swisscom Root CA 2	Swisscom Root CA 2	2031.06.25 07:58:14 Z				
cets.p12	Swisscom Root CA 4	Swisscom Root CA 4	2038.11.24 10:21:53 Z				
	Swisscom Saphir CA 2	Swisscom Root CA 2	2022.01.12 08:37:00 Z				
Digitale IDs von Windows	Swisscom Saphir EU CA 4	Swisscom Root CA 2	2027.05.18 08:27:22 Z				
PRCS#11-Module und -Token	SwissSign Platinum CA - G2	SwissSign Platinum CA - G2	2036.10.25 08/36/00 Z				
	SwissSign Signature Services Root 2	SeissSign Signature Services Root 2	2052.09.30 10:19:32 Z				
Aertrauenzwürdige Zertifikate	Semanter Class 2 Signing RSA Inter.,	Symantee Class 2 Public Primary Ce.,	2030.01.21 23:59:59 Z				
	Symantec Document Signing RSA R.,	Symantec Document Signing RSA R.,	2035.01.14 23:59:59 Z				
	Tella Root CA x2	Tella Root CA v2	2043.11.29 11:53:54 Z				
	Thailand National Root Certification	Thaland National Root Certification	2036/03/27 10:10/22 Z				
	TrustFactory Client Issuing Certificat	TrustFactory Client Root Certificate	2032.12.01 12:36:24 Z				
	TrustFactory Client Root Certificate	TrustFactory Client Root Certificate	2047.11.28 11:48:36 Z				
	Trustante Time Stamping Authority	Trustoate Time Stamping Authority	2041.12.18 23:59:59 Z				
	TSCP SHA256 Bridge CA	TSCP SHA256 Bridge CA	2024/02/23 23:59:59 Z				
	TWCA Global Root CA	TWCA Global Root CA	2030.12.31 15:59:59 Z				
	UAE Global Root CA G4	LIAE Global Root CA Gd	2037.05.12 10:54:59 2				
	UAE Global Root CA G4 E2	UAE Global Root CA G4 E2	2043.02.06 08:54:25 Z				
	LICA Root	LICA Reef	2029 12 31 00 00 00 7				
	UCA Root G2	UCA Reet G2	2036.12.31 00:00:00 Z				
	Universign Primary CA hardware	Universion Primary CA hardware	2042.05.29 16:58:07 Z				
	Universion Timestamoing CA	Universion Timestamping CA	2020.05.06.0930.59.7				
	Universion Timestamping CA 2015	Universion Timestamping CA 2015	2025.01.29 14:03:15 Z				
	USERFruit ECC Certification Authority	USERTrust ECC Certification Authoria	2038/01/18 23:59:59 Z				
	USERTrust RSA Certification Authority	USERFruit RSA Certification Authority	2038.01.18 23:59.59 Z				
	VIALINK EU TRUSTED CA	VIALINK EU ROOT CA	2028/03/13 11:32/45 Z				
	VIDA Reet Certificate Authority	VIDA Root Certificate Authority	2038/01/07/53/41 Z				
	VIDA Sign Certificate Authority	VIDA Root Certificate Authority	2030.05.26 09:30:41 Z				
	7797-040KA	ApplicationCA	2017.12.12 15:00:00 Z				
	7:939-5:40-CA2 Root	ApplicationCA2 Root	2033.03.12 15:00:00 Z				
	W78428270	OfficialStatusCA	2017.09.26 15:00:00 Z				
	AV22041T BS IN CA	WEDDALF OF BLICK	3343 13 21 16 69 69 7				



Mit den vorherigen Schritten haben Sie das Wurzelzertifkat importiert, auf dem alle persönlichen Zertifikate basieren, die ab Beginn 2023 an der HHU ausgegeben wurden (bereits ab Mitte 2022 waren diese Zertifikate erhältlich). Um alle zuvor beantragten Zertifikate zu prüfen, müssen Sie noch folgende Schritte durchführen.

With the previous steps, you have imported the root certificate on which all personal certificates issued at HHU from the beginning of 2023 are based (these certificates were already available from mid-2022). To check all previously requested certificates, you still need to perform the following steps.

# T-TeleSec Wurzelzertifikat (beantragt via DFN) importieren

Neben dem GÉANT-TCS Wurzelzertifikat sollten Sie auch das T-TeleSec Wurzelzertifikat importieren, welches bis Oktober 2033 (https:// corporate-pki.telekom.de/downloads.html) gültig ist. Selbst wenn Ihr persönliches Nutzerzertifikat auf dem GÉANT-TCS Wurzelzertifikat beruht, sollten beide Wurzelzertifikate eingebunden werden, damit Sie auch die Signaturen von anderen prüfen können. Zudem ist das T-TeleSec Wurzelzertifikat notwendig, um den Zeitstempelserver nutzen zu können.



1. Zuerst gehen Sie bei "Bearbeiten" in die "Einstellungen".



2. Dort wählen Sie den Punkt "Unterschriften" aus und klicken unter "Identitäten und vertrauenswürdige Zertifikate" auf "Weitere...".



3. Im folgenden Fenster gehen Sie bei "vertrauenswürdige Zertifikate" auf den blauen Pfeil (Importieren).









<complex-block><complex-block><complex-block>

4. Bevor Sie auf "Durchsuchen" gehen laden Sie sich bitte das Wurzelzertifikat auf der Seite https://corporate-pki.telekom.de /GlobalRootClass2.html herunter: "T-TeleSec GlobalRoot Class 2" (GlobalRoot\_Class\_2.crt).

5. Falls Sie die Datei im Explorer nicht mehr finden, wenn Sie auf "Durchsuchen" gehen liegt das daran das andere Dateitypen erwartet werden und .crt-Dateien nicht angezeigt werden. Sie können diese Datei aber dennoch auswählen indem Sie einfach "\*.crt" im Suchfeld oben rechts reinschreiben und einmal die Enter-Taste bedienen. Jetzt müsste Ihnen die Datei angezeigt werden, die Sie jetzt anklicken müssen.

6. Jetzt wird Ihnen die Zertifikatsdatei unter "Kontakte" angezeigt. Klicken Sie diese einmal an, damit sie auch bei "Zertifikate" erscheint. Klicken Sie jetzt auf die unter "Zertifikate" erschienene Datei. Nun kann auch der Button "Vertrauenswürdigkeit..." angeklickt werden.

7. Danach setzen Sie einen Haken bei "Dieses Zertifikat als vertrauenswürdigen Stamm verwenden" sowie bei "Zertifizierte Dokumente" und klicken auf "OK". Zum Schluss bestätigen Sie die erscheinende Meldung mit "OK"

8. Klicken Sie nun auf "importieren".



1 /1 | 📐 🖑 🖸 🕀 20.16 - 😽 🐺

■ ∠ 众 党 前10

Digital unterschriebe Desare 2025.02.02 0936.12 +01100

☆ Φ 🖶 Q

4

9. Hier können Sie einfach auf "OK" klicken. Dieses Fenster bestätigt nur, dass der Import erfolgreich war.

**Fertig!** Sofern Sie den Anleitungen auf dieser Seite gefolgt sind, müssten die Signaturen, die auf persönlichen Nutzerzertifikaten, die von der HHU Düsseldorf ausgegeben wurden, als gültig erscheinen.

## Fehlermeldung bei Fehlen des Wurzelzertifikats

Eine digitale Signatur wird standardmäßig von Adobe Acrobat automatisch auf ihre Gültigkeit überprüft. Kann die Unterschrift nicht automatisch überprüft werden, erscheint die Fehlermeldung "Mindestens eine Unterschrift erfordert eine Validierung" und die Unterschrift müsste explizit über das Anklicken auf "Unterschriftsfenster" (oben rechts) sowie auf "Alle prüfen" überprüft werden.

Nach der Überprüfung der elektronischen Signaturen im Dokument erscheint eine blaue Anzeigeleiste. Erscheint dort der Text "Gültigkeit der Unterschrift ist UNBEKANNT" oder "Es gibt bei mindestens einer Unterschrift Probleme o.ä., dann kann dies darauf hindeuten, dass verwendete Signaturen auf Zertifikate basieren, welche nicht bei Ihnen als vertrauenswürdig eingestuft sind. Denn bei der Gültigkeitsprüfung wird u. a. überprüft, ob das Zertifikat des Unterzeichners oder ein entsprechend übergeordnetes Zertifikat in der Liste vertrauenswürdiger Identitäten des Prüfenden vorhanden ist.

R for	PDC, swapdf - Adulta Accitat Fra 2020 Restanting - Acatem Franker, Willia						0	×
24	t Workzeuge Teit POF,respot ×					• •	rest	den
	A 🖶 🖂 d		•	1.0 2 4	6			
4	Unterschrieben und alle Unterschriften alnd gülfig.					Unterschriftsferete	2	G,
P	Unterschriften	×					1	E6
	Alle pröfen			Malana Shee		0		
0				build or other states		8		
0	Dokument wijstege Dokument wijste soch-den Unterscheiden nicht mehr geandert.			Test PDF	day 1764 Fibildeds where Figure 1			6
	Unterchrieben vom aktuelen fanzeten. Die Signatur ist mit einem alsgebeteten Zeitstampel versehen, dieser konnterjoeksch nicht gepröft werden.		<ul> <li>Por dall reserver of invaligner ener agradia</li> </ul>					80
	Unimularity to 127 Gilling					0		
	Xana popul Initian Nata - Print							
	Feit Spraturiz auf Seite 1 Köcken Siz um diese Netelen anzumigen.							0
	Enkamont propert and Sparance							25

## Erkennen einer (LTV-fähigen) Signatur

Um zu prüfen, ob eine Signatur LTV-fähig ist, müssen Sie oben rechts auf das "Unterschriftenfenster" gehen, welches sich links öffnet.

Klicken Sie auf den Pfeil, der sich links neben "Revision 1: Unterschrieben von [...]" befindet.

Unter "Unterschrift ist gültig" sollte sich ein Stichpunkt mit "Unterschrift ist LTV-fähig" zeigen