Prüfen einer digitalen Signatur in einer PDF

Voraussetzungen - Wurzelzertifikate importieren

⚠️ 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 /
- Import GÉANT-TCS root certificate (requested via Sectigo)
  - Sicherheitseinstellungen aktualisieren /
  - Update security settings
  - Wurzelzertifikat installieren mittels FDF-Datei /
  - Install root certificate using a FDF file
  - Zertifikats-Richtlinieneinschränkung ändern /
  - Change certificate policy restriction
- 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 **certificate 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 /

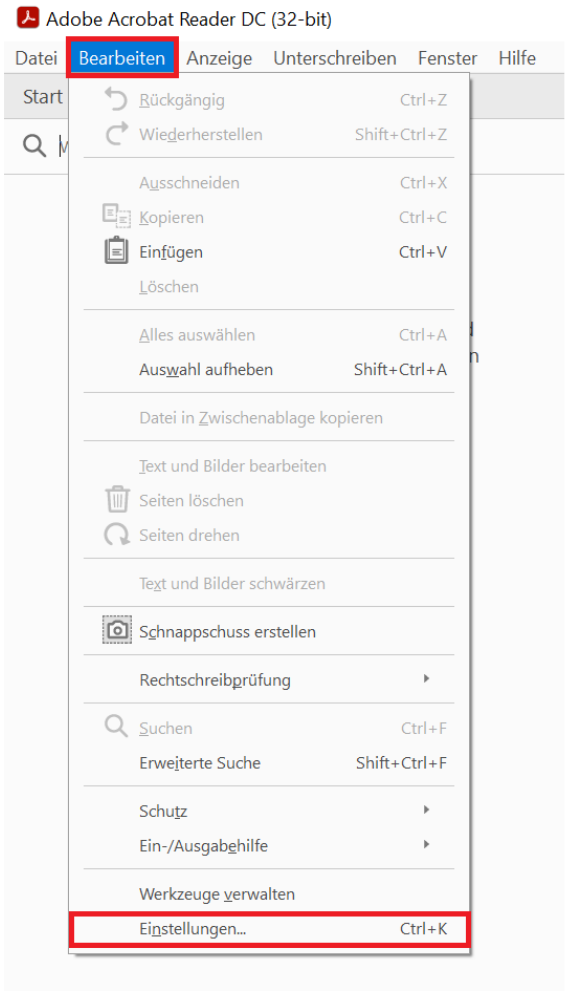
Update security settings

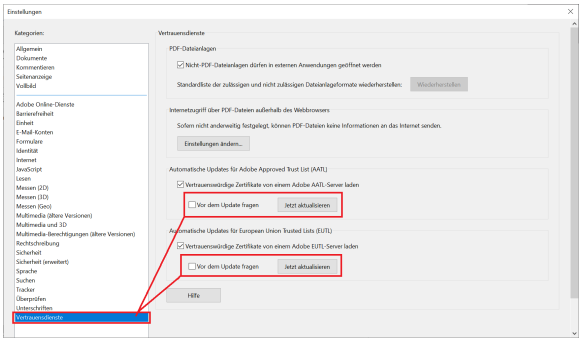
Als Erstes sollten Sie ihre Sicherheitseinstellungen aktualisieren bzw. in Adobe Acrobat alle Wurzelzertifikate aus der Adobe Approved Trust-Liste (AATL) sowie aus der Trust-Liste der Europäischen Union (EUTL) importieren.

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 „**Einstellungen**“.

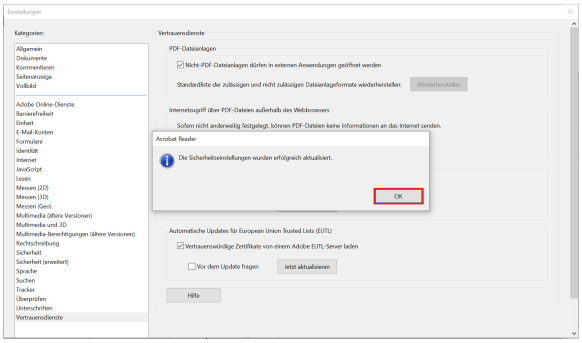
***1.** In Adobe Acrobat click on the hamburger **Menu** button and then on „**References...**“.*

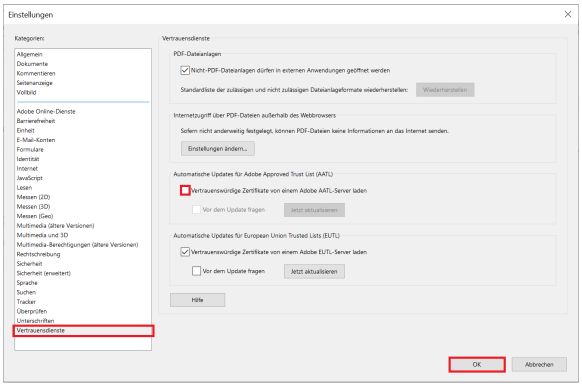




2. Unter "**Vertrauensdienste**" klicken Sie auf beide "**Jetzt aktualisieren**" Schaltflächen, um alle von Adobe sowie von der Europäischen Union ausgelieferten vertrauenswürdigen Wurzelzertifikate zu importieren.

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





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*

Wurzelzertifikat installieren mittels FDF-Datei /

Install root certificate using a FDF file

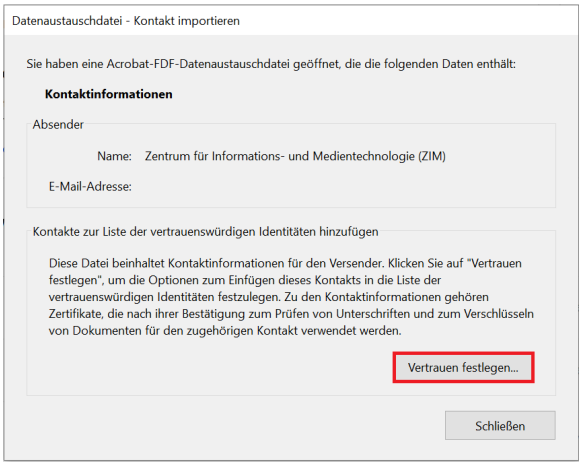
FDF-Datenaustauschdateien
Root-Zertifikat USERTrust ECC.fdf
Root-Zertifikat USERTrust RSA.fdf

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.



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

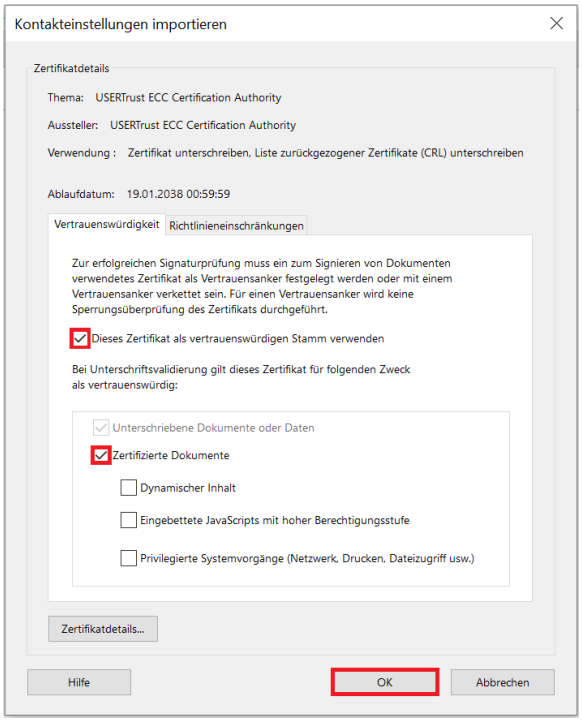
***2.** When starting, a window opens. Click on "**Set Contact Trust...**"*

---

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**"



***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.

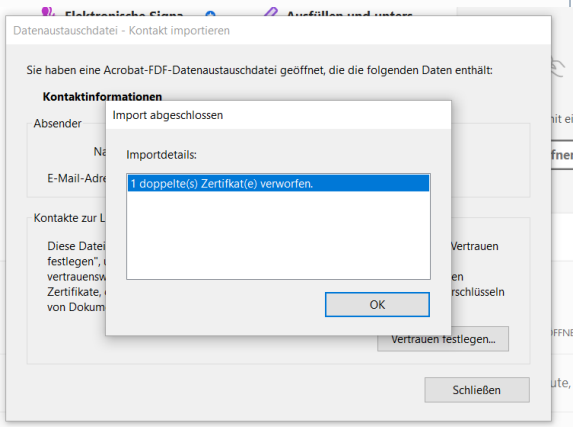
Falls dieses Zertifikat schon drin ist, bekommen Sie diese Meldung:

"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"

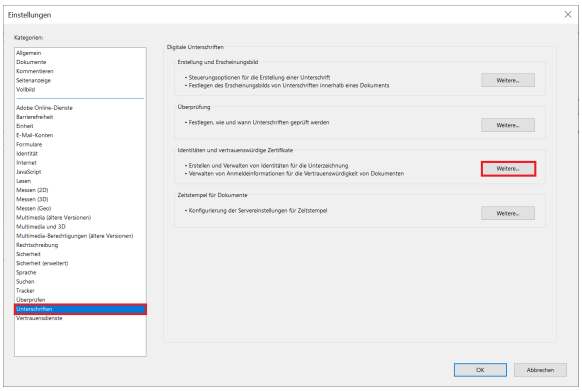


Doch ohne Import mittels der FDF-Datei muss die Richtlinieneinschränkung für das Wurzelzertifikat der "USERTrust RSA Certification Authority" bearbeitet werden.

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

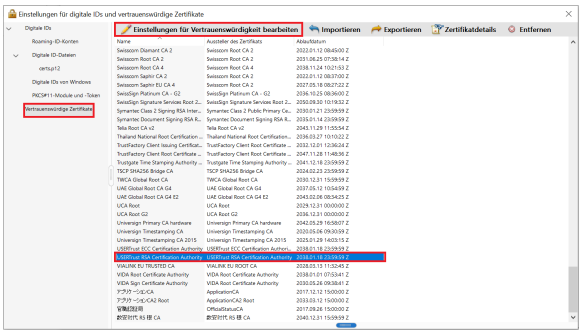


1. Klicken Sie in Adobe Acrobat im Menü „**Bearbeiten**“ auf den Punkt „**Einstellungen**“

1. *In Adobe Acrobat click on the hamburger* ***Menu*** *button and then on „****Preferences...****“.*

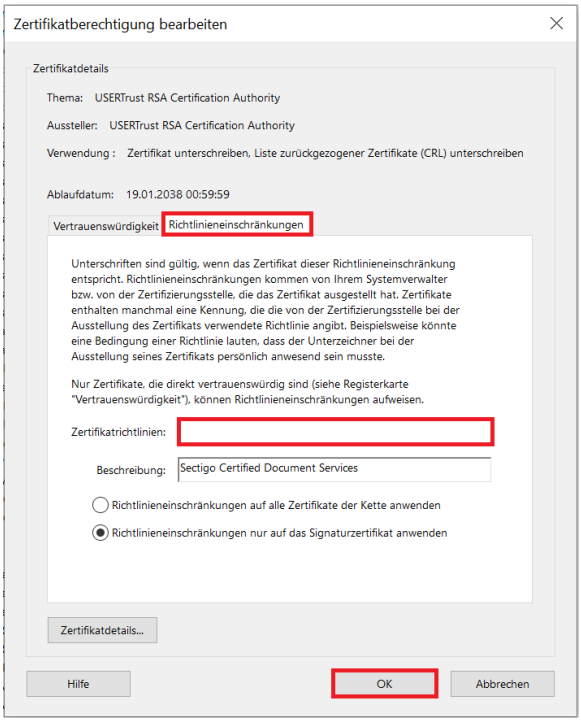
2. In den Einstellungen klicken Sie unter **"Unterschriften" "Identitäten und vertrauenswürdige Zertifikate"** auf **"Weitere..."**

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 **"Vertrauenswürdige 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 l öschen den Eintrag bei **"Zertifikatsrichtlinie"** und bestätigen die Änderungen mit **"OK"**

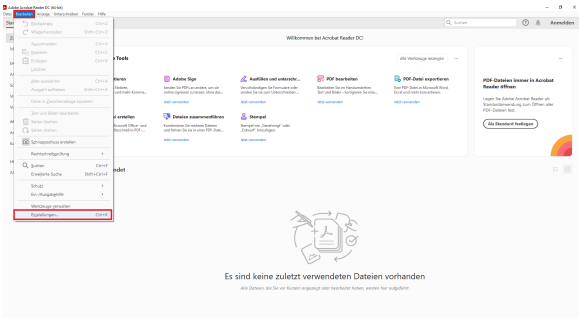
4. *In the window that has opened, switch to the "****Policy Restrictions****" tab and delete what is written in the "****Certificate Policies****" field and confirm the changes with "****OK****"*

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.

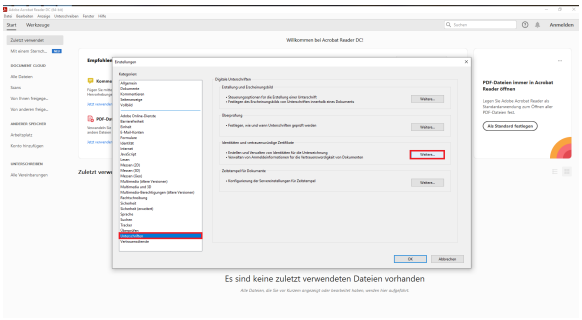
With the previous steps, you have imported the root certificate on which all personal certificates issued at HHU from the beginning of 2023 are based (these certificates were already available from mid-2022). To check all previously requested certificates, you still need to perform the following steps.

T-TeleSec Wurzelzertifikat (beantragt via DFN) importieren

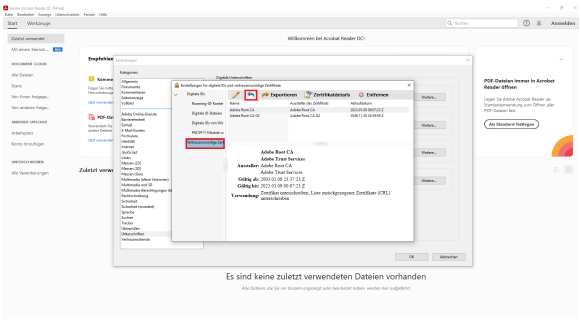
Neben dem **GÉANT-TCS Wurzelzertifikat** sollten Sie auch das **T-TeleSec Wurzelzertifikat** importieren, welches bis Oktober 2033 (https://corporate-pki.telekom.de/downloads.html) gültig ist. Selbst wenn Ihr persönliches Nutzerzertifikat auf dem GÉANT-TCS Wurzelzertifikat beruht, sollten beide Wurzelzertifikate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



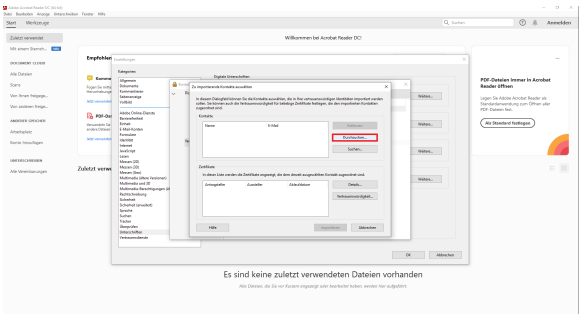
1. Zuerst gehen Sie bei "Bearbeiten" in die "Einstellungen".



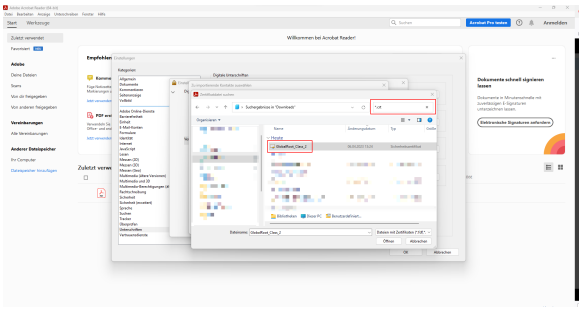
2. Dort wählen Sie den Punkt "Unterschriften" aus und klicken unter "Identitäten und vertrauenswürdige Zertifikate" auf "Weitere...".



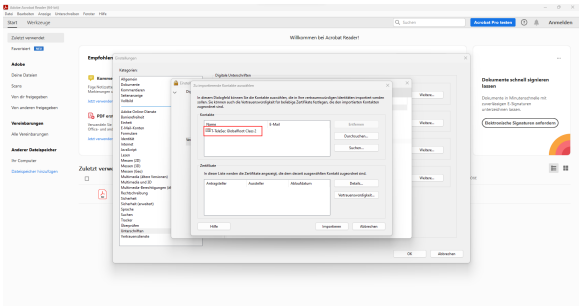
3. Im folgenden Fenster gehen Sie bei "vertrauenswürdige Zertifikate" auf den blauen Pfeil (Importieren).



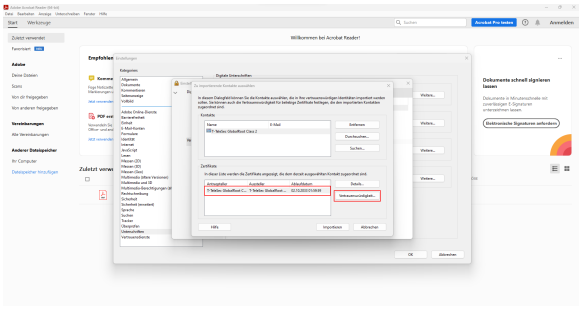
4. Bevor Sie auf "Durchsuchen" gehen laden Sie sich bitte das Wurzelzertifikat auf der Seite https://corporate-pki.telekom.de/GlobalRootClass2.html herunter: "T-TeleSec GlobalRoot Class 2" (GlobalRoot_Class_2.crt).

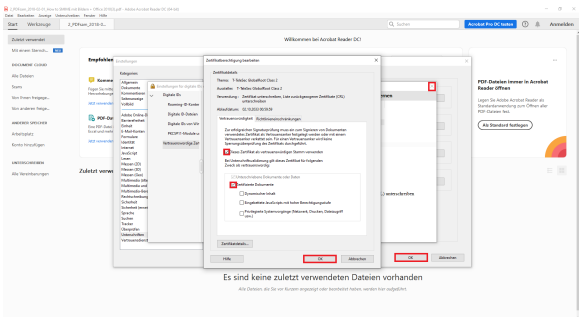


5. Falls Sie die Datei im Explorer nicht mehr finden, wenn Sie auf "Durchsuchen" gehen liegt das daran das andere Dateitypen erwartet werden und .crt-Dateien nicht angezeigt werden. Sie können diese Datei aber dennoch auswählen indem Sie einfach "*.crt" im Suchfeld oben rechts reinschreiben und einmal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



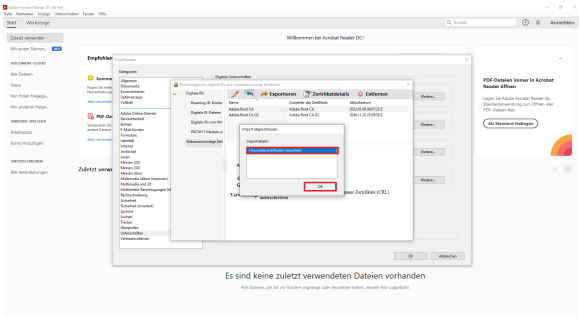
6. Jetzt wird Ihnen die Zertifikatsdatei unter "Kontakte" angezeigt. Klicken Sie diese einmal an, damit sie auch bei "Zertifikate" erscheint. Klicken Sie jetzt auf die unter "Zertifikate" erschienene Datei. Nun kann auch der Button "Vertrauenswürdigkeit..." angeklickt werden.





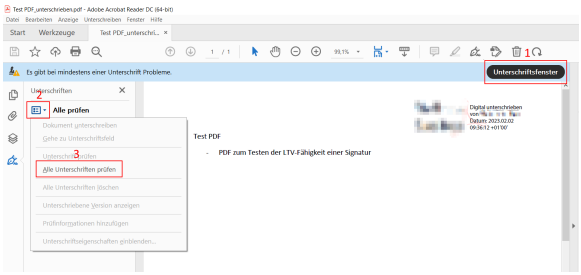
7. Danach setzen Sie einen Haken bei "Dieses Zertifikat als vertrauenswürdigen Stamm verwenden" sowie bei "Zertifizierte Dokumente" und klicken auf "OK". Zum Schluss bestätigen Sie die erscheinende Meldung mit "OK"

8. Klicken Sie nun auf "importieren".



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

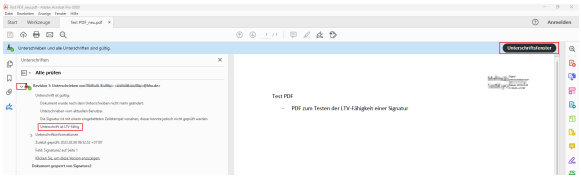
Fertig! Sofern Sie den Anleitungen auf dieser Seite gefolgt sind, müssten die Signaturen, die auf persönlichen Nutzerzertifikaten, die von der HHU Düsseldorf ausgegeben wurden, als gültig erscheinen.



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.



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