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.

Inhalt dieser Seite

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

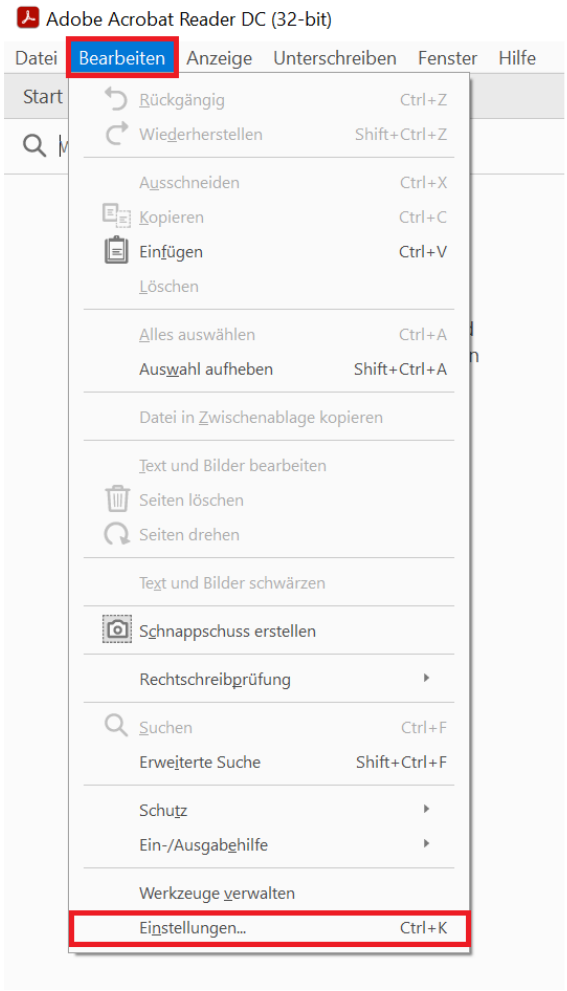
Das bedeutet: Damit eine digitale Signatur, welche auf einem Nutzerzertifikat von der DFN oder GÉANT-TCS basiert, als gültig validiert wird, muss entweder das mit der **Signatur verbundene Zertifikat** oder das **Wurzelzertifikat** entsprechend **importiert** und als **Vertrauensanker** festgelegt werden.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

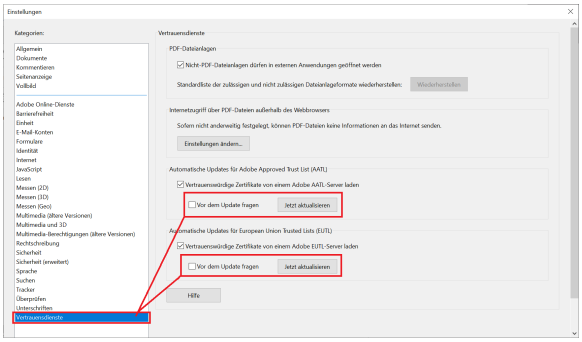
GÉANT-TCS Wurzelzertifikat (beantragt via Sectigo) importieren

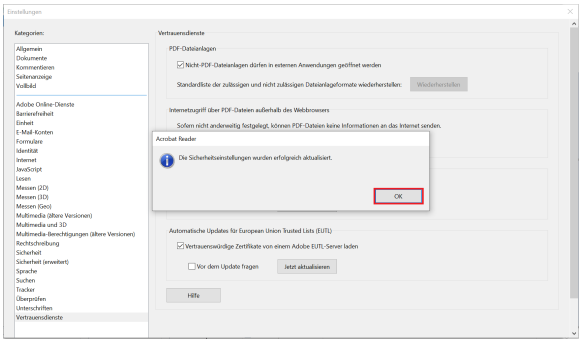
Sicherheitseinstellungen aktualisieren

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.

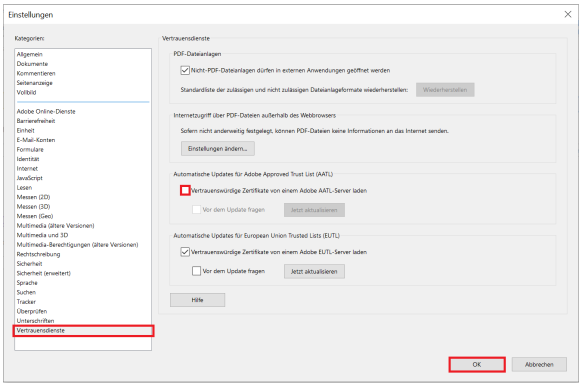
1. Klicken Sie in Adobe Acrobat im Menü „**Bearbeiten**“ auf den Punkt „**Einstellungen**“:







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



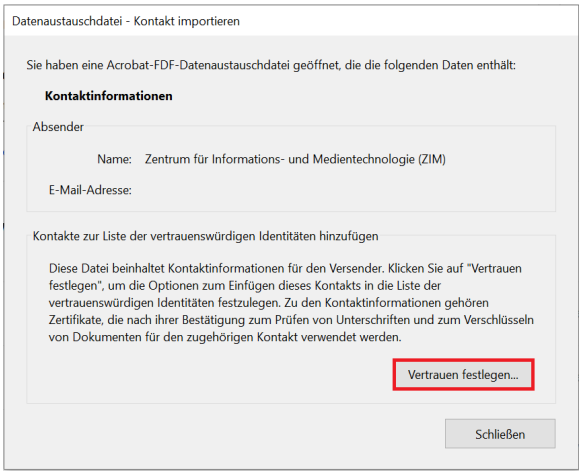
3. Zudem sollten Sie den **Haken bei "Vertrauenswürdige Zertifikate von einem Adobe AATL-Server laden" rausnehmen**, damit die noch folgenden Installationen von Wurzelzertifikaten **nicht** beim nächsten automatischen Update von Adobe Acrobat geändert werden.

Wurzelzertifikat installieren mittels FDF-Datei

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.

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

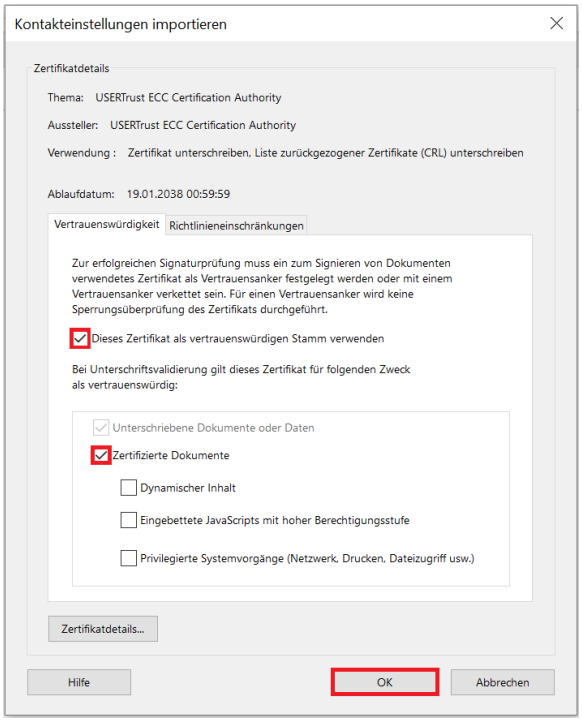
2. Beim Starten öffnet sich ein Fenster, wo sie auf "**Vertrauen festlegen...**" klicken

---

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

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

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

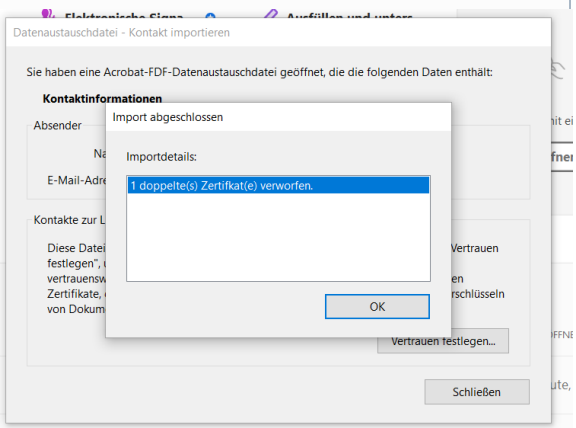


Hinweis

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.

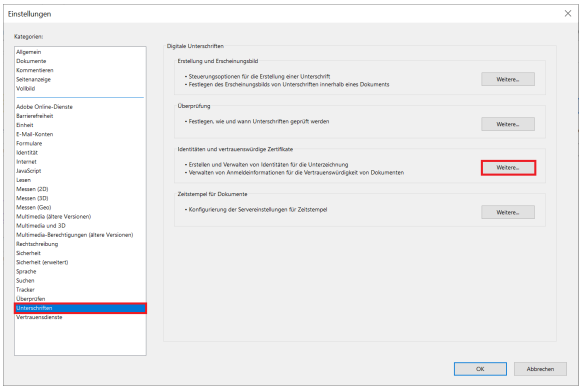
Falls dieses Zertifikat schon drin ist, bekommen Sie diese Meldung:

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



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

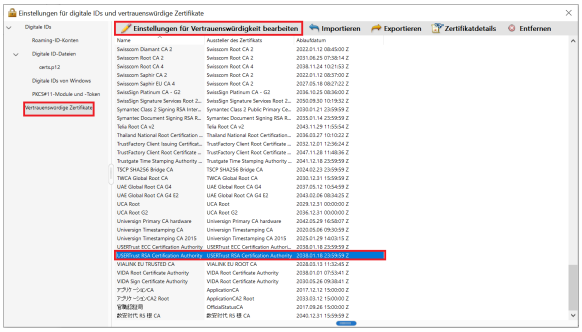
Zertifikats-Richtlinieneinschränkung ändern

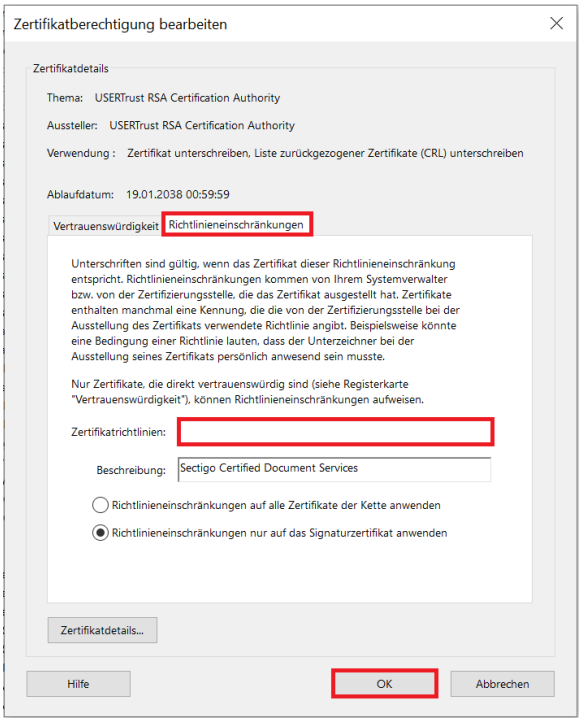


1. Klicken Sie in Adobe Acrobat im Menü „**Bearbeiten**“ auf den Punkt „**Einstellungen**“

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

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





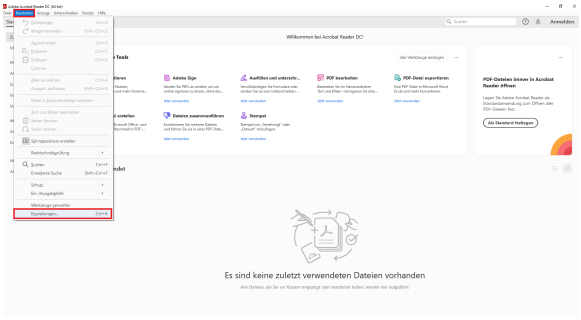
4. Dann wechseln Sie auf den Tab **"Richtlinieneinschränkungen"** und l öschen den Eintrag bei **"Zertifikatsrichtlinie"** und bestätigen die Änderungen mit **"OK"**

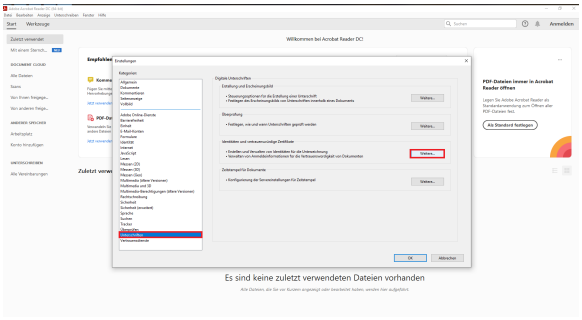
Mit den vorherigen Schritten haben Sie das Wurzelzertifkat importiert, auf dem alle persönlichen Zertifikate basieren, die ab Beginn 2023 an der HHU ausgegeben wurden (bereits ab Mitte 2022 waren diese Zertifikate erhältlich). Um alle zuvor beantragten Zertifikate zu prüfen, müssen Sie noch folgende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

T-TeleSec Wurzelzertifikat (beantragt via DFN) importieren

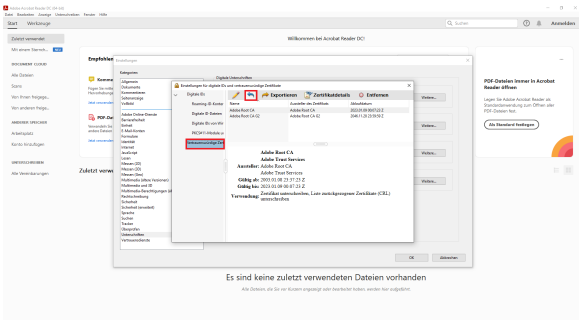
Neben dem **GÉANT-TCS Wurzelzertifikat** sollten Sie auch das **T-TeleSec Wurzelzertifikat** importieren, welches bis Oktober 2033 (https://corporate-pki.telekom.de/downloads.html) gültig ist. Selbst wenn Ihr persönliches Nutzerzertifikat auf dem GÉANT-TCS Wurzelzertifikat beruht, sollten beide Wurzelzertifikate 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".

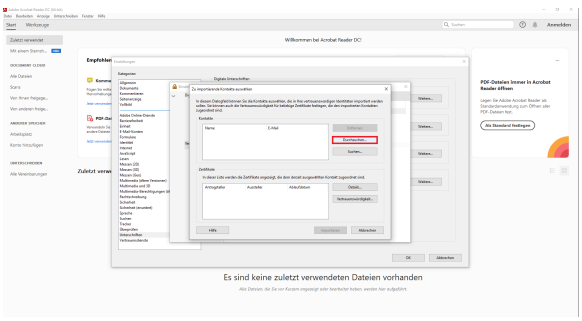




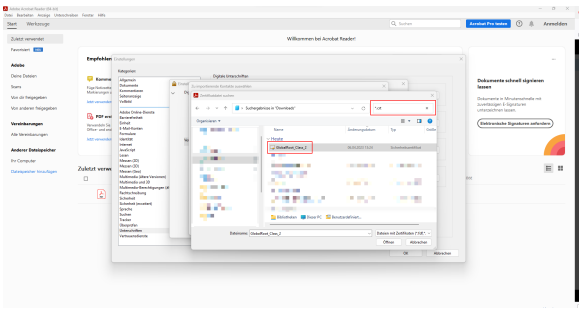
2. Dort wählen Sie den Punkt "Unterschriften" aus und klicken unter "Identitäten und vertrauenswürdige Zertifikate" auf "Weitere...".



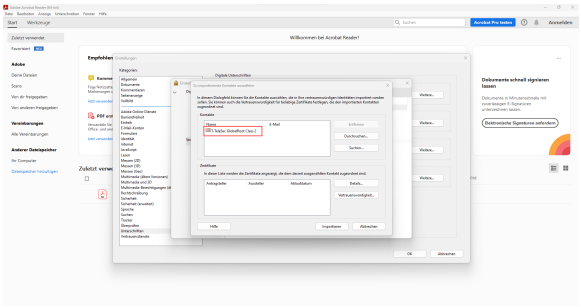
3. Im folgenden Fenster gehen Sie bei "vertrauenswürdige Zertifikate" auf den blauen Pfeil (Importieren).

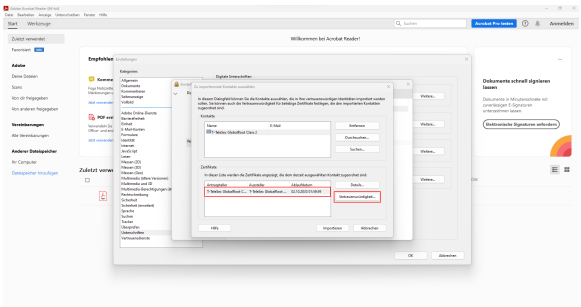


4. Bevor Sie auf "Durchsuchen" gehen laden Sie sich bitte das Wurzelzertifikat auf der Seite https://corporate-pki.telekom.de /GlobalRootClass2.html herunter: "T-TeleSec GlobalRoot Class 2" (GlobalRoot_Class_2.crt).

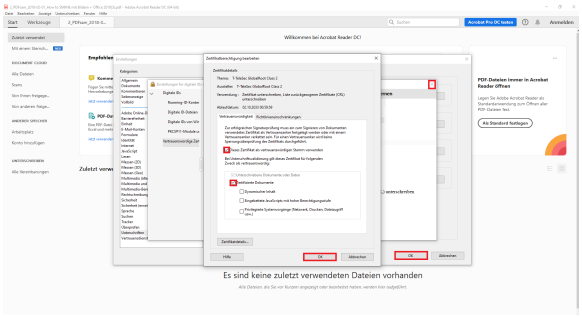


5. Falls Sie die Datei im Explorer nicht mehr finden, wenn Sie auf "Durchsuchen" gehen liegt das daran das andere Dateitypen erwartet werden und .crt-Dateien nicht angezeigt werden. Sie können diese Datei aber dennoch auswählen indem Sie einfach "*.crt" im Suchfeld oben rechts reinschreiben und einmal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



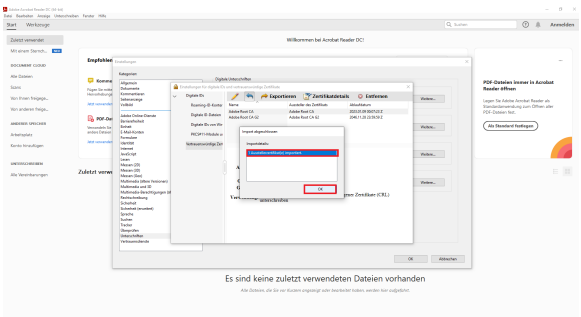


6. Jetzt wird Ihnen die Zertifikatsdatei unter "Kontakte" angezeigt. Klicken Sie diese einmal an, damit sie auch bei "Zertifikate" erscheint. Klicken Sie jetzt auf die unter "Zertifikate" erschienene Datei. Nun kann auch der Button "Vertrauenswürdigkeit..." angeklickt werden.



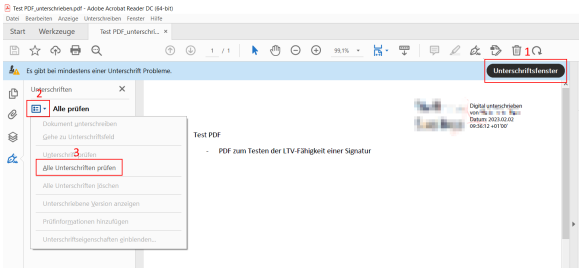
7. Danach setzen Sie einen Haken bei "Dieses Zertifikat als vertrauenswürdigen Stamm verwenden" sowie bei "Zertifizierte Dokumente" und klicken auf "OK". Zum Schluss bestätigen Sie die erscheinende Meldung mit "OK"

8. Klicken Sie nun auf "importieren".



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

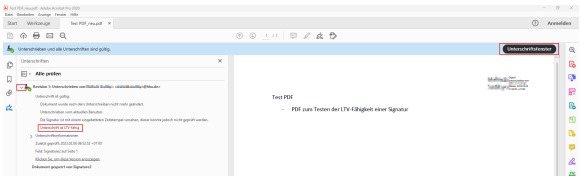
Fertig! Sofern Sie den Anleitungen auf dieser Seite gefolgt sind, müssten die Signaturen, die auf persönlichen Nutzerzertifikaten, die von der HHU Düsseldorf ausgegeben wurden, als gültig erscheinen.



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