Konfiguration einer elektronischen Unterschrift

Anleitung zur Konfiguration einer fortgeschrittenen elektronischen Signatur im Acrobat Reader DC unter Windows

Version 1.3, 27.04.2023

Inhalt

1 Allgemeines

Diese Anleitung umfasst die Konfiguration einer elektronischen Unterschrift (digitale Signatur) in Form einer fortgeschrittenen elektronischen Signatur im Acrobat Reader DC unter Windows.

1.1 Rechtsgültigkeit

Nach dem deutschen Signaturgesetz entspricht die, wie in diesem Dokument beschriebene, mittels eines Zertifikats der DFN-PKI angebrachte elektronische Unterschrift einer „fortgeschrittenen elektronischen Signatur“.

Im Rahmen der Digitalisierung der Geschäftsprozesse an der RWTH Aachen wird für immer mehr Geschäftsprozesse neben der eigenhändigen Unterschrift auch diese fortgeschrittene elektronische Signatur auf PDF-Dokumenten als gültige Unterschrift im internen Geschäftsverkehr akzeptiert.

Formulare, die neben der eigenhändigen Unterschrift auch elektronisch unterschrieben von den Fachabteilungen der RWTH akzeptiert werden, sind im Formularcenter des Intranets (**https://www.rwth-aachen.de/formularcenter**) mit einem eigenen Symbol  gekennzeichnet. Bei anderen Dokumenten aus den Geschäftsprozessen der RWTH klären Sie bitte im Vorfeld mit der Fachabteilung, ob eine elektronische Unterschrift akzeptiert wird.

1.2 Voraussetzungen

Um ein PDF-Dokument im Acrobat Reader DC mit einer elektronischen Unterschrift zu versehen, müssen folgende Voraussetzungen erfüllt sein:

a. Sie verfügen über ein persönliches Nutzerzertifikat. (Kapitel **2 Persönliches Nutzerzertifikat**, S. **2**)
b. Die Sicherheitseinstellungen wurden vorgenommen. (Kapitel **3 Sicherheitseinstellungen**, S. **6**)
c. Das Stammzertifikat Ihres Nutzerzertifikats ist konfiguriert. (Kapitel **4 Stammzertifikat konfigurieren**, S. **14**)
d. Sie haben die elektronische Unterschrift konfiguriert. (Kapitel **5 Elektronische Unterschrift konfigurieren**, S. **24**)

Haben Sie die Konfiguration des Acrobat Reader DC bereits vorgenommen, können Sie direkt zum Kapitel **6 PDF-Dokument elektronisch unterschreiben** (S. **30**) springen und die gewünschten Dokumente unterschreiben.

2 Persönliches Nutzerzertifikat

2.1 Persönliches Nutzerzertifikat beantragen

Für eine elektronische Unterschrift benötigen Sie ein persönliches Nutzerzertifikat welches von der DFN-PKI ausgestellt wurde. Sofern Sie dieses nicht schon für das Signieren Ihrer E-Mails beantragt haben und nutzen, können Sie dies online über das RWTH-DFN-Zertifizierungsportal vornehmen.

Eine Anleitung dazu finden Sie für verschiedene Browser im Dokumentationsportal des IT Centers (**https://www.rwth-aachen.de/zertifikate)** unter dem Stichwort „Nutzerzertifikat beantragen“ im Bereich *IT-Basisstruktur -> Sicherheit -> Zertifikate -> Nutzerzertifikat beantragen.*

Bitte beachten Sie, dass Gruppenzertifikate bzw. die digitale ID von Gruppenzertifikaten, wie sie bspw. für Funktions-E-Mail-Postfächer ausgegeben werden, nicht für die elektronische Unterschrift verwendet werden dürfen, weil Sie i.d.R. nicht die Bedingung erfüllen, dass sie genau einer Person zugeordnet werden können.

2.2 Persönliches Nutzerzertifikat importieren

Im Dokumentationsportal des IT Centers ist neben der eigentlichen Beantragung auch der Erhalt des Zertifikats beschrieben.

Bitte beachten Sie auch die dort beschriebene Notwendigkeit zur Erzeugung einer Sicherheitskopie und die Aufbewahrungshinweise. Eine Anleitung zum Importieren/Exportieren aus den jeweiligen Browsern finden Sie ebenfalls im Dokumentationsportal unter dem Stichwort „Nutzerzertifikat beantragen“.

Ihr persönliches Nutzerzertifikat (inkl. des zugehörigen Schlüsselpaares) können Sie über Doppelklick auf die von Ihnen erstellte Sicherheitskopie in den Zertifikatsspeicher von Windows importieren.

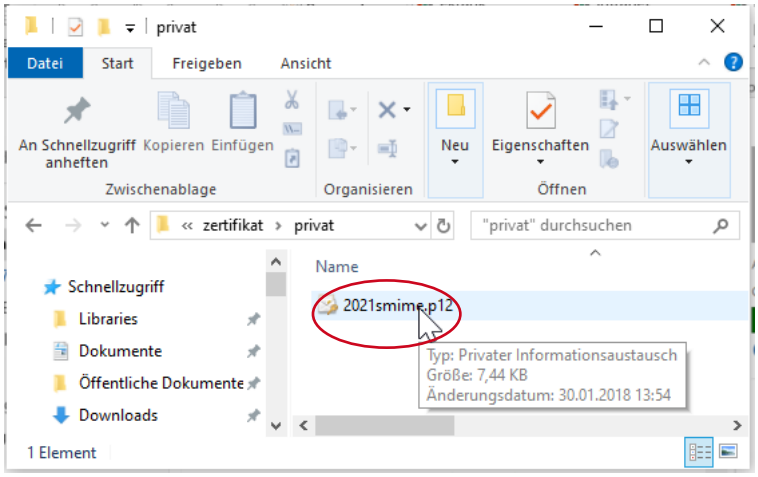


Abbildung 1: Doppelklick auf die Sicherheitskopie

Es öffnet sich der Zertifikatsimport-Assistent von Windows. Wählen Sie als Speicherort „Aktueller Benutzer“ aus und klicken Sie auf den Button Weiter.

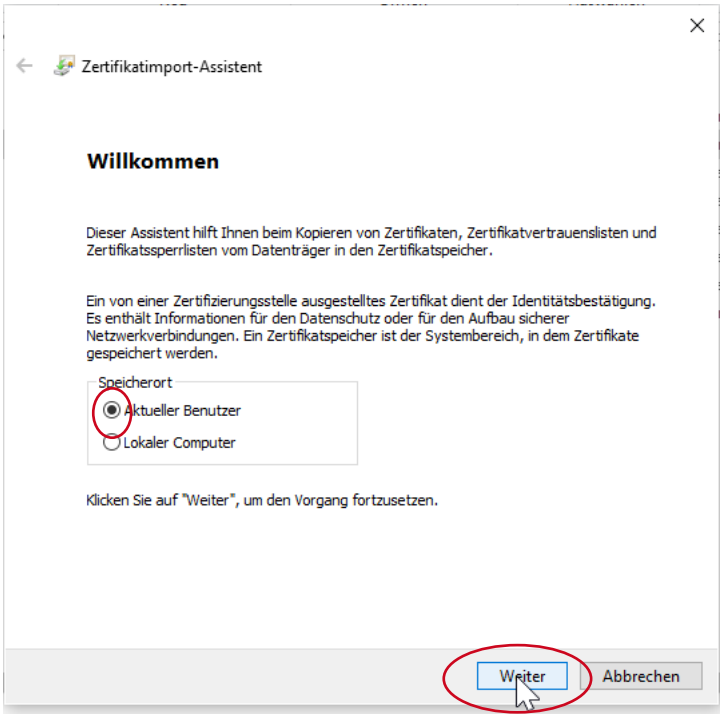


Abbildung 2: Import starten

Der Dateiname der Sicherungskopie ist vorausgewählt. Bitte bestätigen Sie die Auswahl mit Klick auf Weiter.

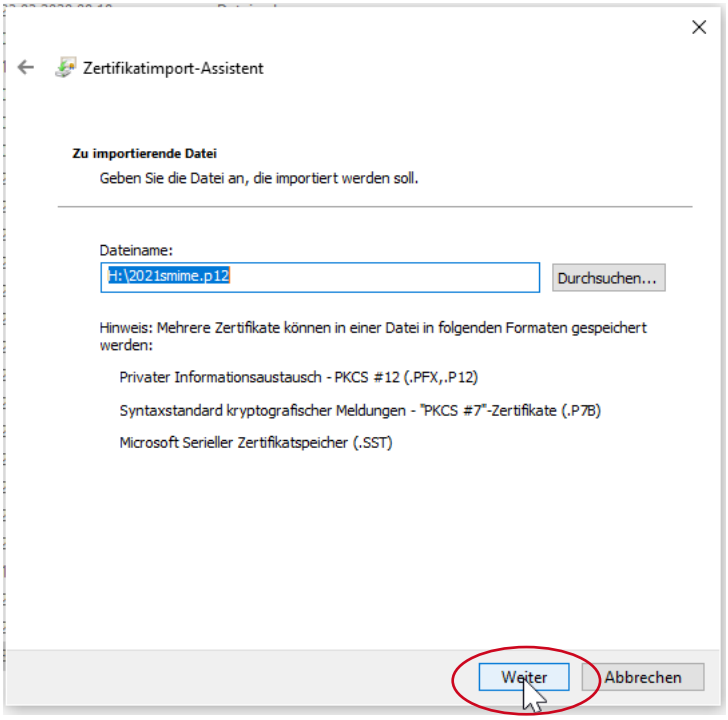


Abbildung 3: Auswahl bestätigen

Sie werden aufgefordert das zuvor beim Erstellen der Sicherungskopie vergebene Passwort einzugeben.

Bitte aktivieren Sie die Checkbox für hohe Sicherheit und das Einbeziehen der erweiterten Eigenschaften und bestätigen Sie dies mit Klick auf „Weiter“.

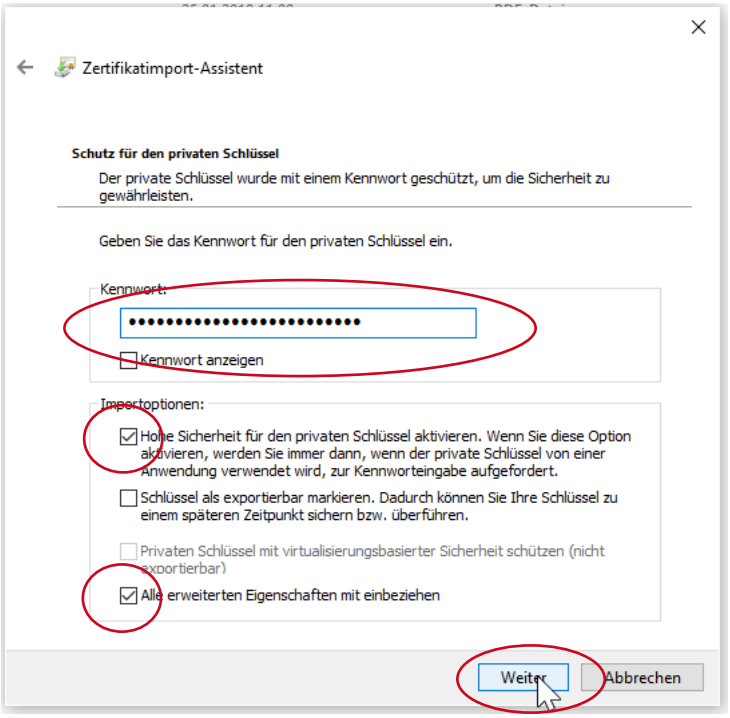


Abbildung 4: Kennwort eingeben

Bestätigen Sie die Auswahl des Zertifikatsspeichers mit Klick auf „Weiter“.

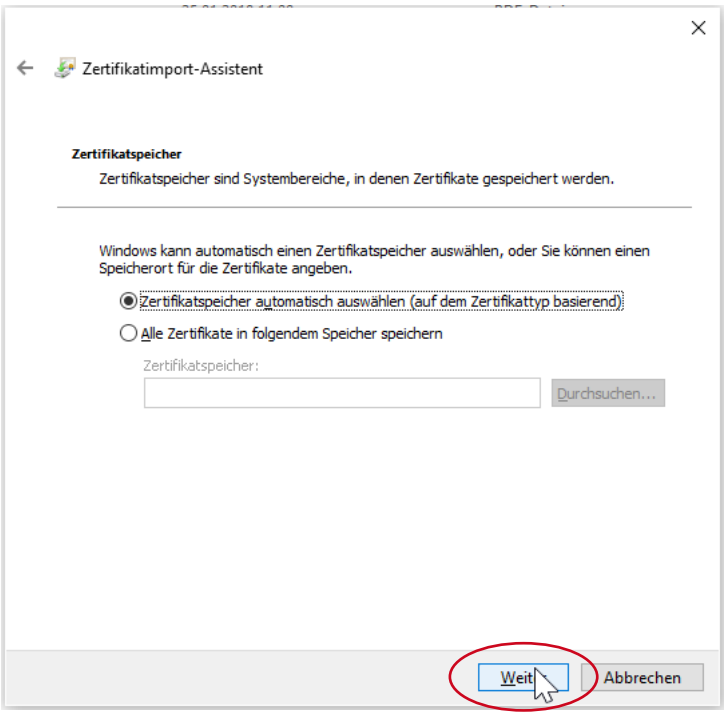


Abbildung 5: Zertifikatsspeicher auswählen

Bestätigen Sie den Import mit Klick auf „Fertig stellen“.

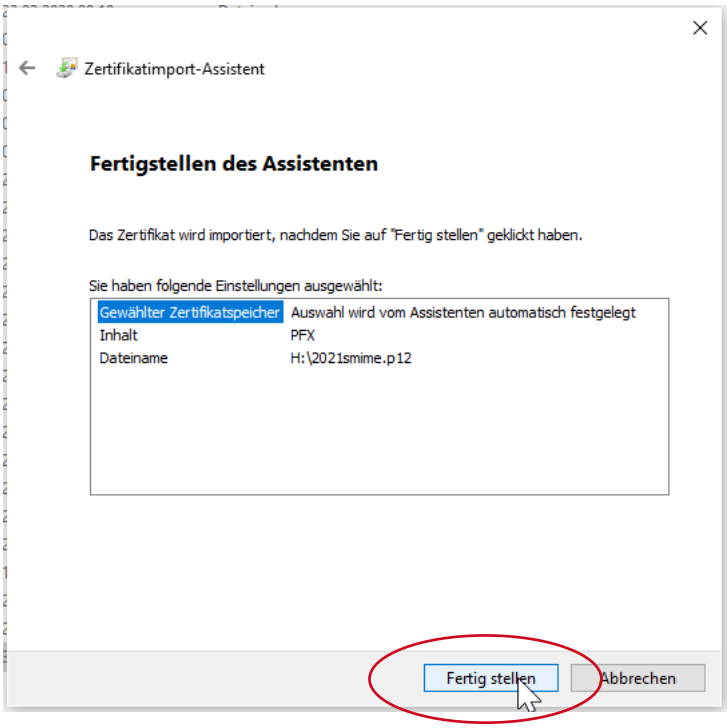


Abbildung 6: Import bestätigen

Quittieren Sie den Import mit Klick auf OK.

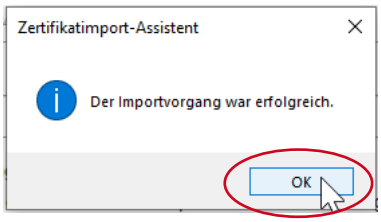


Abbildung 7: Zertifikatsimport abschließen

Dadurch steht Ihnen die unter Kapitel **6 PDF-Dokument elektronisch unterschreiben**, S. **30** beschriebene digitale ID unter Windows zur Verfügung.

3 Sicherheitseinstellungen

Bevor Sie das erste Mal ein Dokument elektronisch unterschreiben oder auch das erste Mal eine elektronische Unterschrift prüfen wollen, checken Sie bitte die Sicherheitseinstellung Ihres Acrobat Reader DC. Starten Sie dazu den Acrobat Reader DC ohne ein Dokument geöffnet zu haben.

Alle im Folgenden vorgenommenen Einstellungen zur elektronischen Unterschrift finden sich im Acrobat Reader DC im Bearbeitungsmenü unter dem Menüpunkt „Einstellungen“. (Bearbeiten -> Einstellungen)

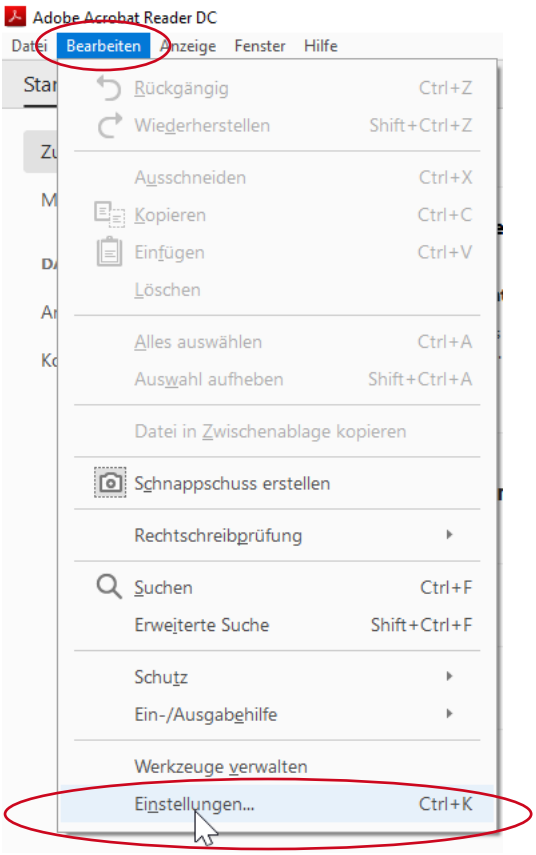


Abbildung 8: Dialogmenü Bearbeiten

3.1 Vertrauensdienste

Bitte stellen Sie sicher, dass Sie nur die Stammzertifikate konfiguriert haben, denen Sie wirklich vertrauen. Um vertrauenswürdige Stammzertifikate bewusst auszuwählen, schalten Sie im Dialogmenü „Einstellungen“ unter dem Navigationspunkt „Vertrauensdienste“ die automatischen Updates für die Adobe Approved Trustlist (AATL) und die European Union Trust Lists (EUTL) ab.

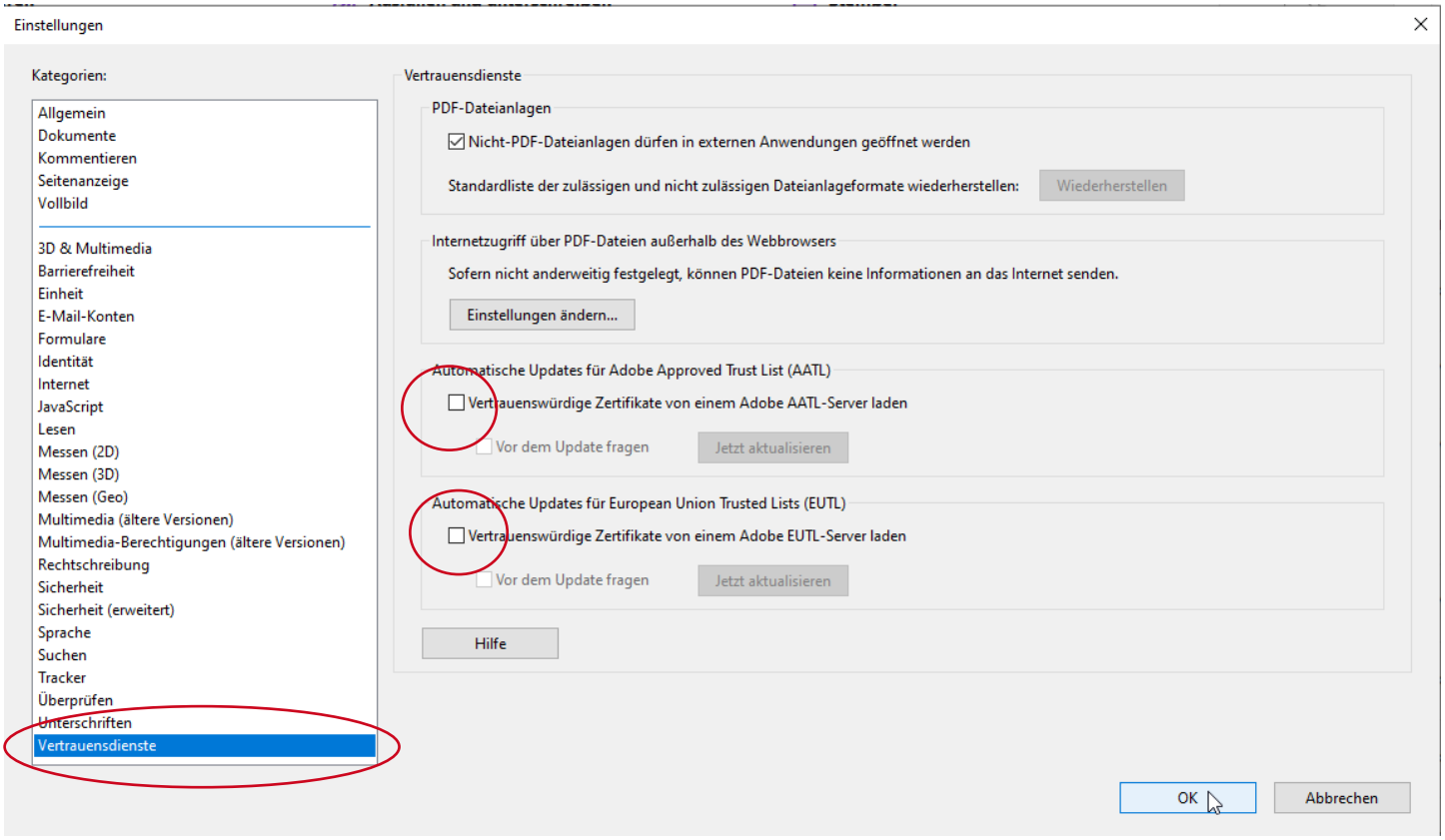


Abbildung 9: Konfiguration Vertrauensdienste

Löschen Sie ggf. die bereits durch Adobe als vertrauenswürdig eingestuften Stammzertifikate aus der Liste der vertrauenswürdigen Zertifikate. Navigieren Sie dazu im Dialogmenü „Einstellungen“ zum Navigationspunkt „Unterschriften“ und klicken Sie im Bereich „Identitäten und vertrauenswürdige Zertifikate auf den Button „Weitere“.

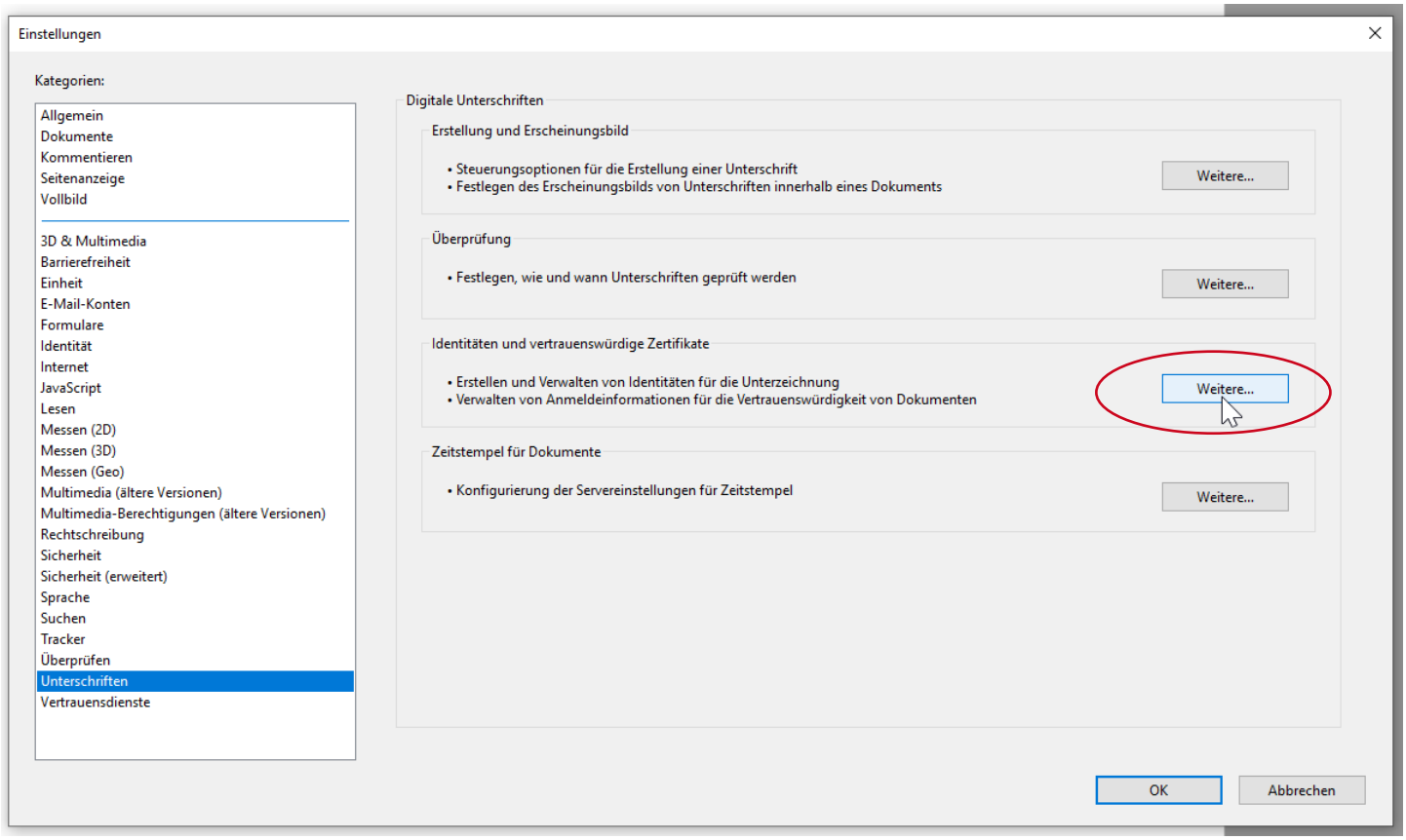


Abbildung 10: Dialogmenü Einstellungen

Durch die im vorangegangenen Schritt abgeschaltete Adobe Approved Trustlist (AATL) und die European Union Trust Lists (EUTL) ist nach wie vor eine lange Liste von vertrauenswürdigen Zertifikaten vorhanden.

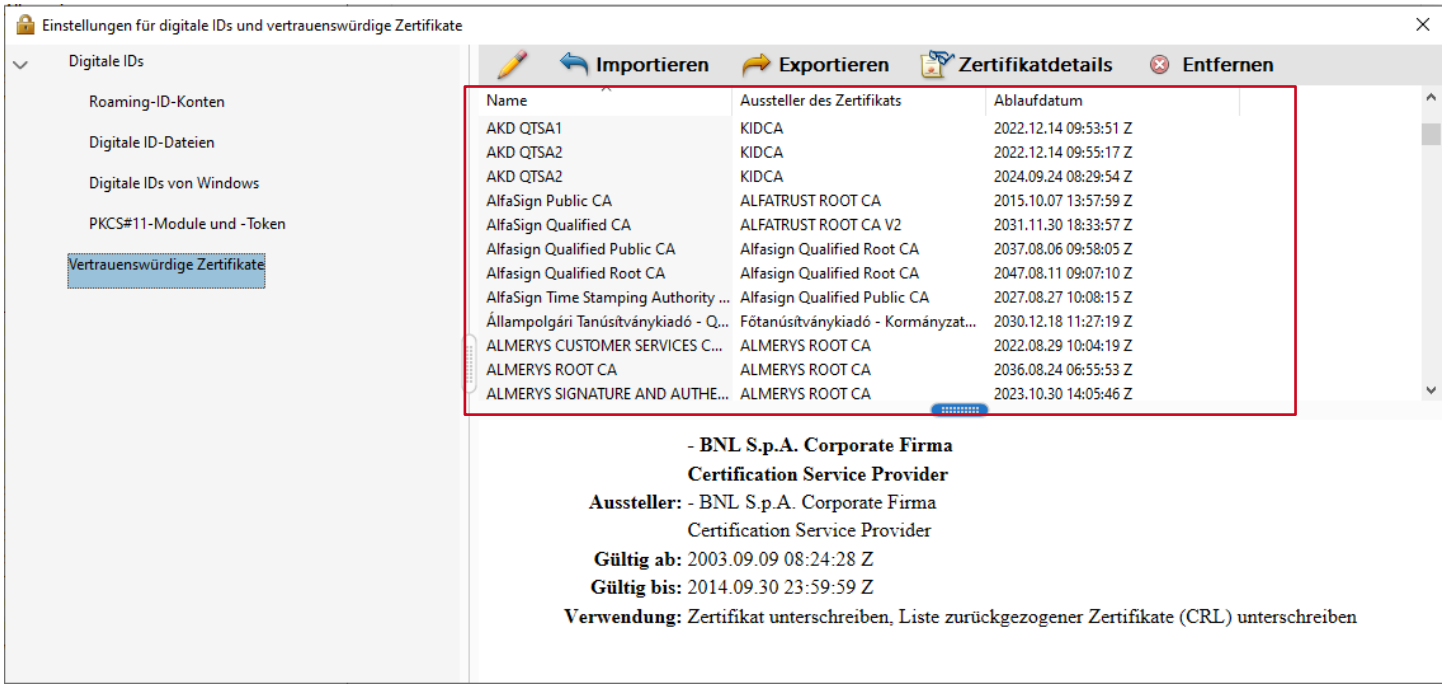


Abbildung 11: Liste der vertrauenswürdigen Zertifikate

Markieren Sie alle Zertifikate um sie und über den Button „Entfernen“ aus der Liste zu löschen.

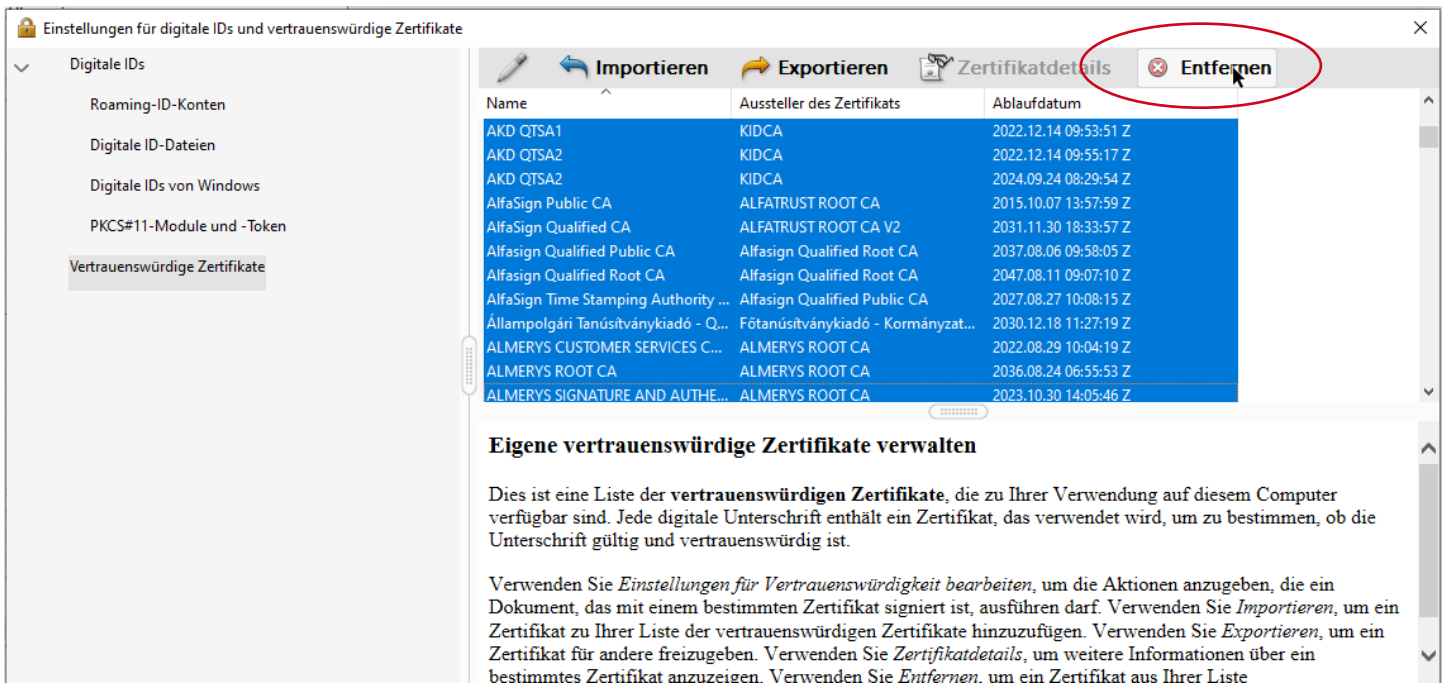


Abbildung 12: Zertifikate löschen

Das Adobe Root CA G2- Zertifikat (ggf. auch das Adobe Root CA) ist immer vorhanden und lässt sich auch nicht entfernen, bzw. wird nach dem Entfernen beim nächsten Öffnen automatisch wieder in die Liste aufgenommen.

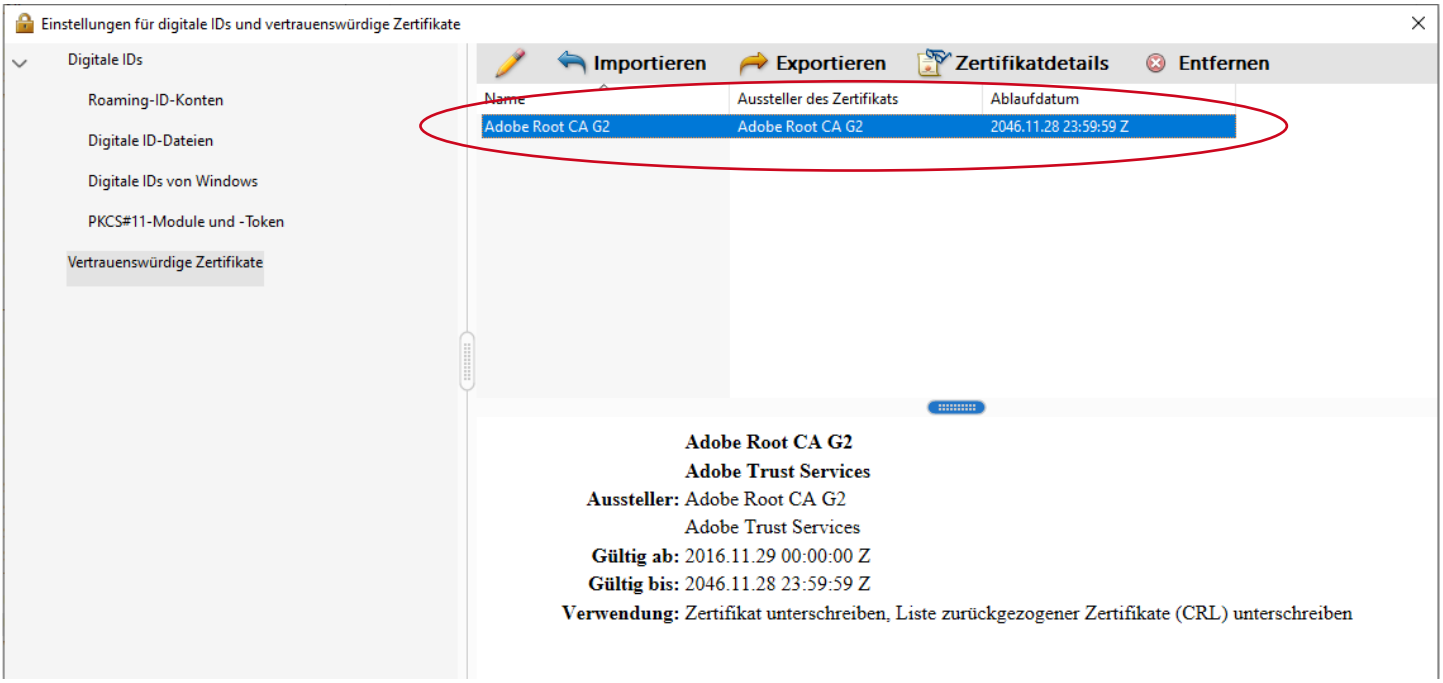


Abbildung 13: Adobe Root CA G2-Zertifikat

3.2 Zeitstempel konfigurieren

Der DFN stellt einen Zeitstempel-Dienst zur Verfügung. Dieser ermöglicht es unabhängig von der individuellen Zeitkonfiguration des lokalen Rechners einen überprüfbaren und vertrauenswürdigen Zeitstempel an die elektronische Unterschrift zu heften. Da die lokale Rechnerzeit unter Umständen manipulierbar ist, wird an der RWTH Aachen der DFN-Zeitstempelserver eingebunden.

Die Konfiguration ist im Dialogfenster zu den Einstellungen des Acrobat Reader DC unter dem Navigationspunkt „Unterschriften“ im Bereich „Zeitstempel für Dokumente“ über Klick auf den Button „Weitere“ zu erreichen.

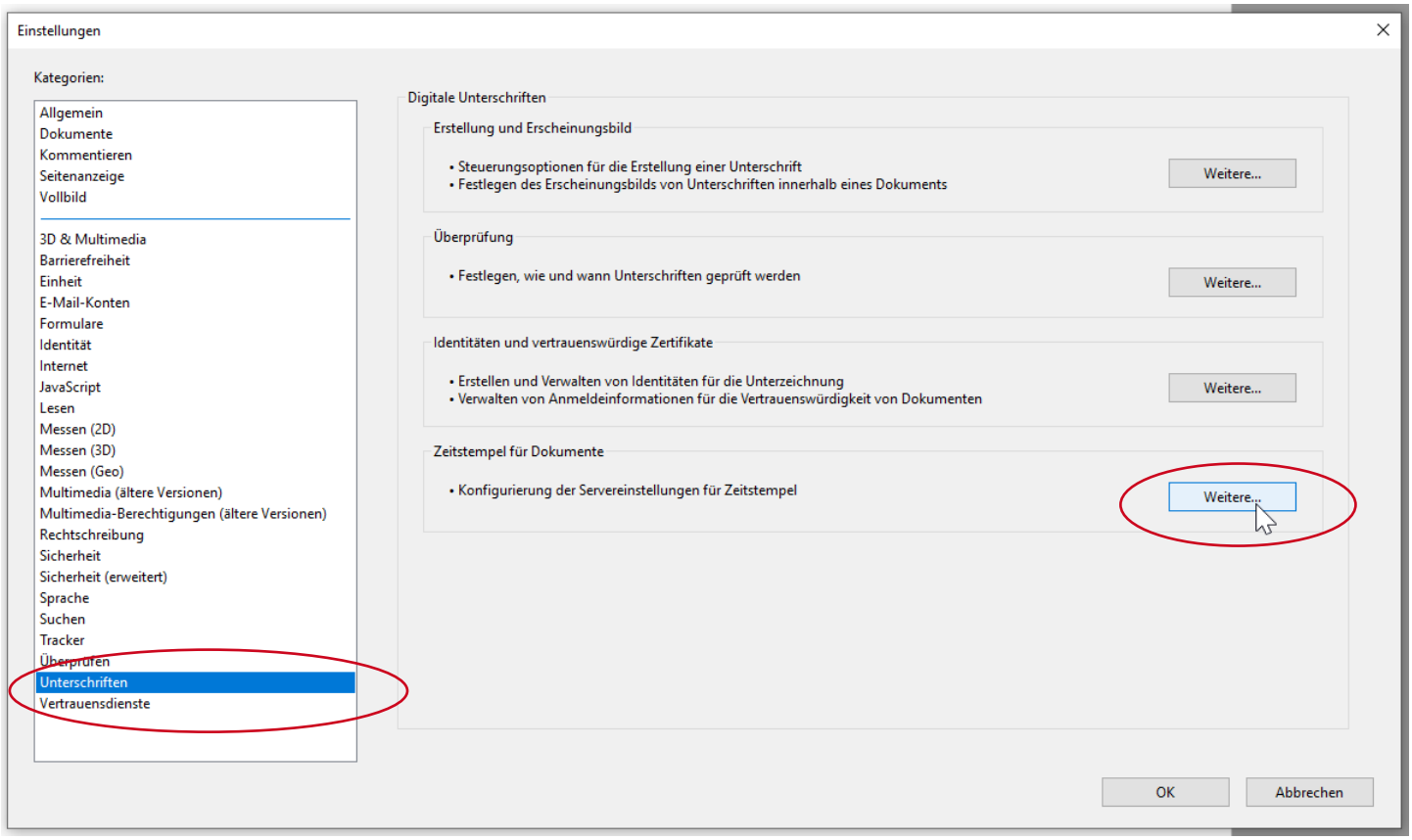


Abbildung 14: Unterschriften - Zeitstempel konfigurieren

Es öffnet sich das Dialogfenster „Servereinstellungen“.

Unter dem Navigationspunkt „Uhrzeitstempelserver“ wählen Sie bitte in der Top-Navigation den Button Neu (+) aus.

Abbildung 15: Uhrzeitstempelserver einstellen

Es öffnet sich das Dialogfenster „Neuer Uhrzeitstempelserver“. Geben Sie hier folgende Konfigurationsdaten ein:

- Name = DFN-Zeitstempel
- Server-URL = http://zeitstempel.dfn.de

und schließen Sie das Dialogfenster über den Button „OK“.

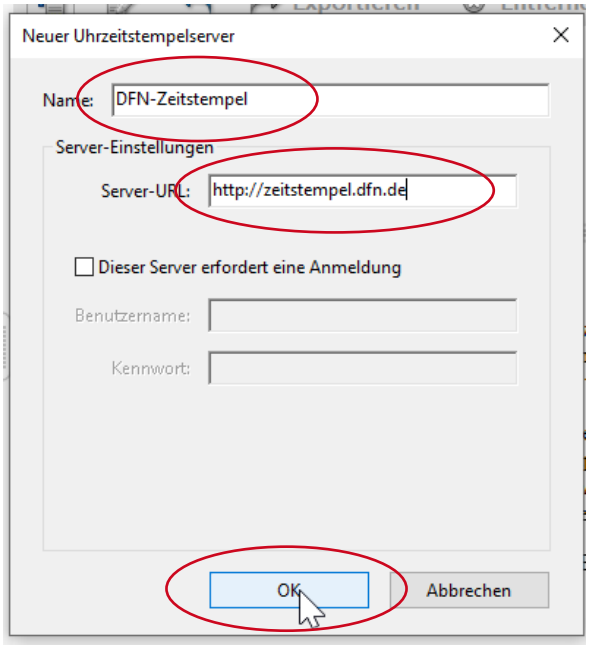


Abbildung 16: Neuen Uhrzeitstempelserver definieren

Legen Sie den DFN-Zeitstempel-Dienst als Standard fest. Wählen Sie dazu den DFN-Zeitstempel aus und klicken Sie auf „Standardeinstellung festlegen“.

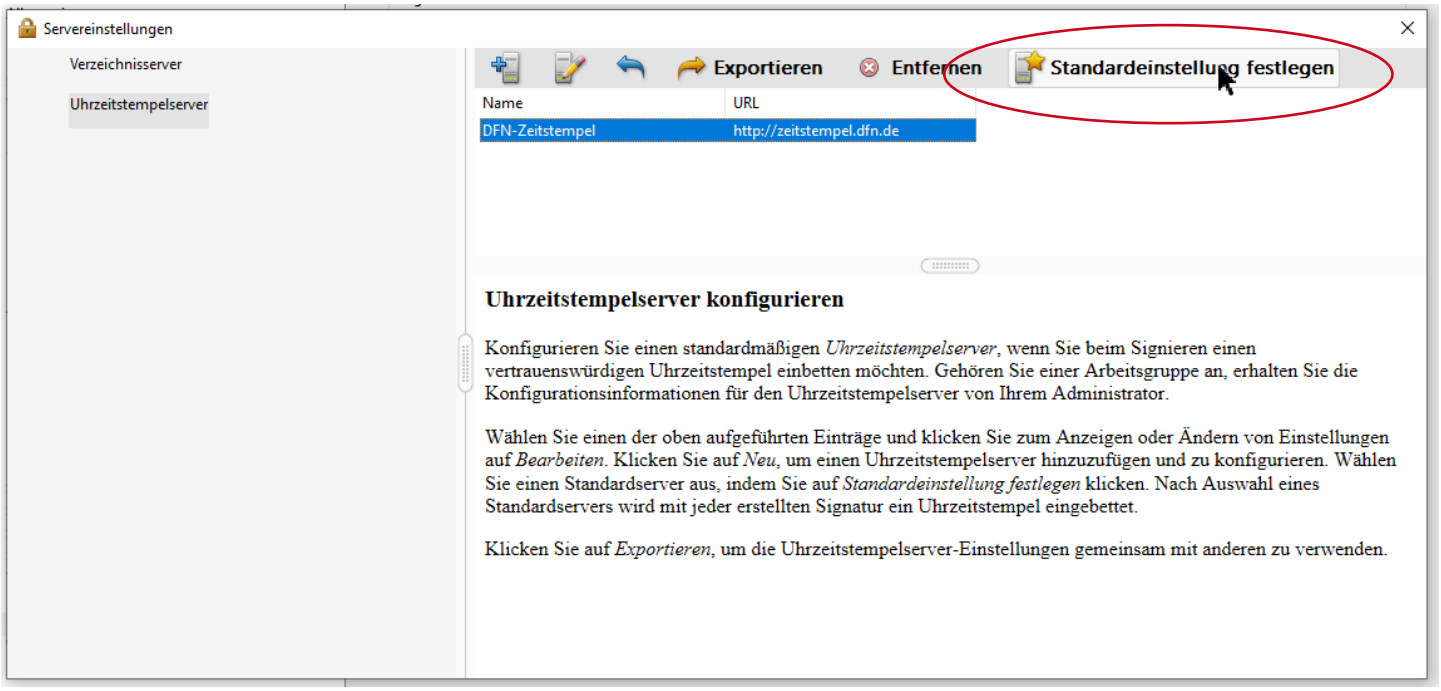


Abbildung 17: DFN-Zeitstempel-Dienst als Standard

Bestätigen Sie die Standardeinstellung mit OK.

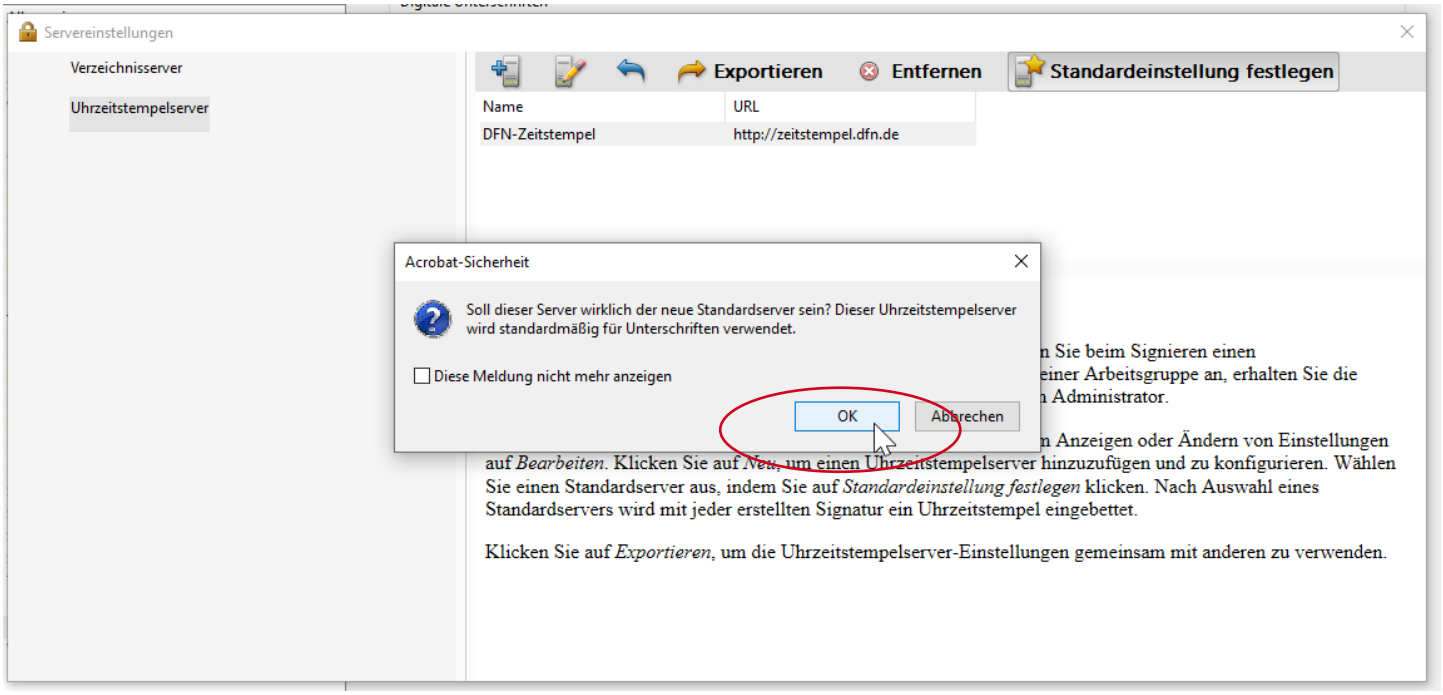


Abbildung 18: Zeitstempeldienst Einstellungen bestätigen

Weitere Informationen zum Zeitstempel-Dienst des DFN finden Sie unter

https://www.pki.dfn.de/faqpki/faq-zeitstempel/

4 Stammzertifikat konfigurieren

Starten Sie den Acrobat Reader DC ohne ein Dokument geöffnet zu haben.

Alle Einstellungen zur elektronischen Unterschrift finden sich im Acrobat Reader DC sich im Bearbeitungsmenü unter dem Menüpunkt „Einstellungen“. (Bearbeiten -> Einstellungen)

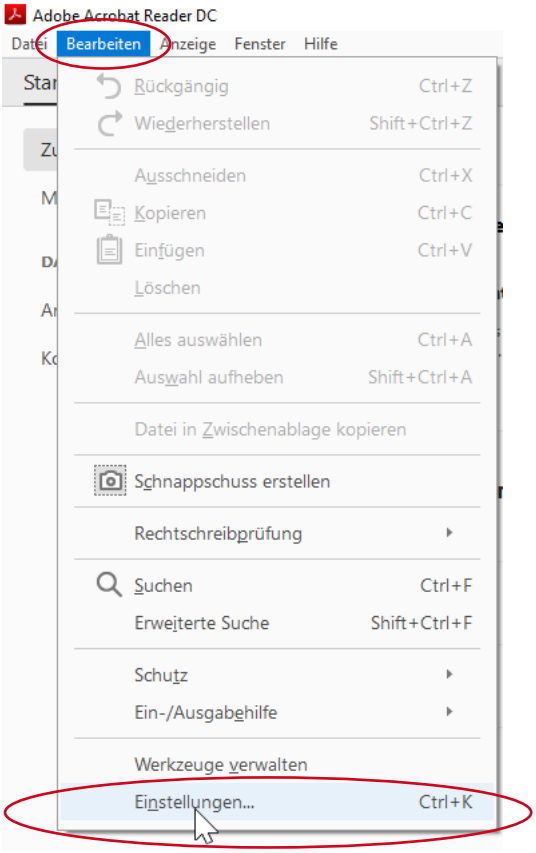


Abbildung 19: Dialogmenü Bearbeiten

In den Standardeinstellungen von Adobe Acrobat DC ist die Zertifikatskette bzw. das Stammzertifikat der an der RWTH verwendeten Nutzerzertifikate nicht enthalten.

Um das notwendige Stammzertifikat zu prüfen und ggf. zu importieren, wählen Sie bitte im Einstellungsmenü den Navigationspunkt „Unterschriften“ und dort im Bereich „Identitäten und vertrauenswürdige Zertifikate“ den Button „Weitere“.

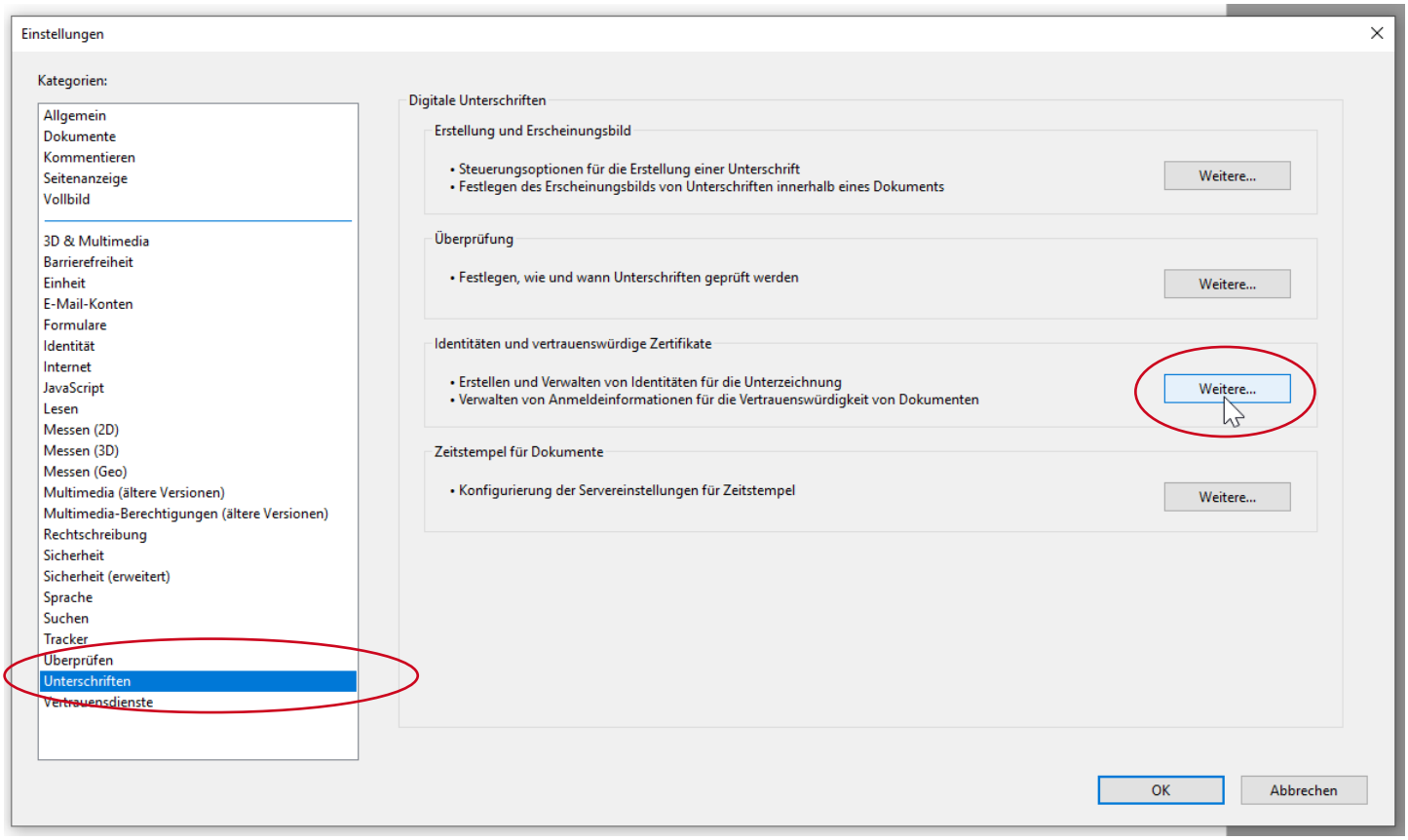


Abbildung 20: Dialogmenü Einstellungen

Dieser öffnet das Fenster mit den Einstellungen für digitale IDs und vertrauenswürdige Zertifikate.

Hier wählen Sie bitte den Navigationspunkt „Vertrauenswürdige Zertifikate“.

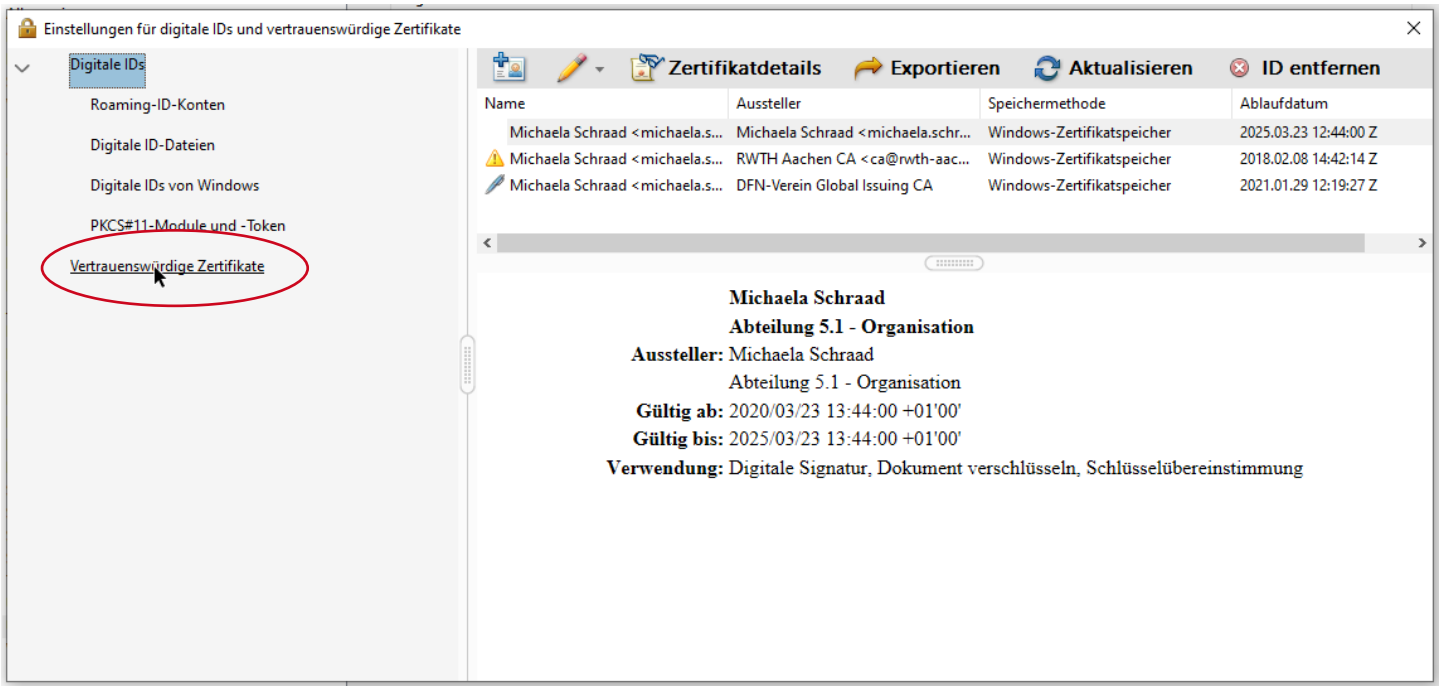


Abbildung 21: Navigationspunkt „Vertrauenswürdige Zertifikate“

Abhängig von der Konfiguration Ihrer Sicherheitseinstellungen zu den Vertrauensdiensten (Kapitel **3.1 Vertrauensdienste**, S. **7**) sind nur das Adobe Root CA G“-Zertifikat und ggf. das Adobe Root CA-Zertifikat per Default vorhanden.

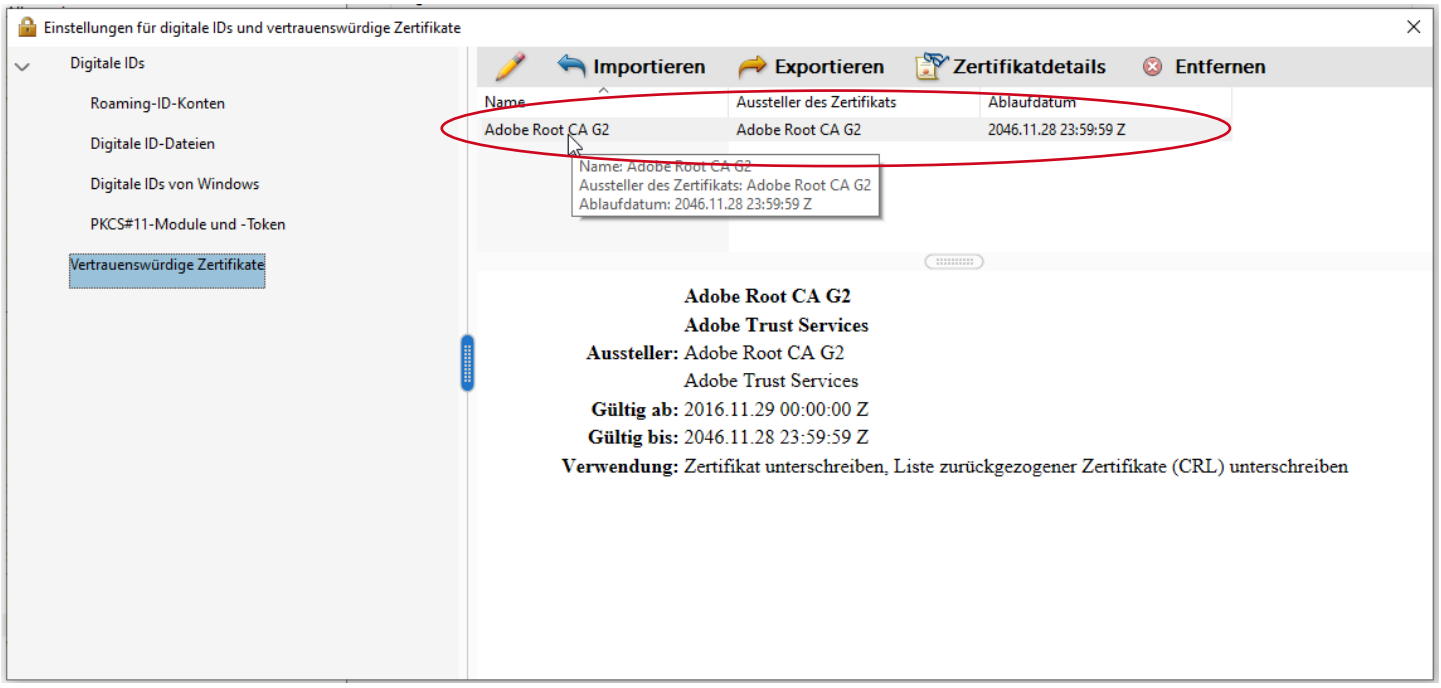


Abbildung 22: Dialogmenü Einstellungen für digitale IDs und vertrauenswürdige Zertifikate

Das Stammzertifikat T-TeleSec GlobalRoot Class 2 (rootcert.crt) der DFN-PKI Zertifikatskette, finden Sie im Dokumentationsportal des IT Centers (**https://help.itc.rwth-aachen.de**) unter dem Stichwort „Zertifikatskette der DFN-PKI“ im Bereich *IT-Basisstruktur -> Sicherheit -> Zertifikate -> Zertifikatskette der DFN-PKI* zum Download.

Zertifikat DFN-PKI-G1	CER-format (Base-64-codiert)	DER-format	PEM-format
Deutsche Telekom Root CA 2	rootcert.cer (Android, Windows)	Root cacert.der (Windows)	Root cacert.pem (Linux)
DFN-Verein PCA Global - G01	dfncacert.cer (Android, Windows)	DFN cacert.der (Windows)	DFN cacert.pem (Linux)
RWTH Aachen CA	rwthcacert.cer (Android, Windows)	RWTH cacert.der (Windows)	RWTH cacert.pem (Linux)

Abbildung 23: Zertifikate der DFN-PKI (Quelle: help.itc.rwth-aachen.de)

Bitte speichern Sie das T-TeleSec GlobalRoot Class2-Zertifkat mit Rechtsklick auf rootcert.crt -> „Speichern unter“ lokal auf Ihrer Festplatte um es im nächsten Schritt importieren zu können.

Den Import des Stammzertifikats T-TeleSec GlobalRoot Class2-Zertifikats können Sie über den Button „Importieren“ in der Top-Navigation anstoßen.

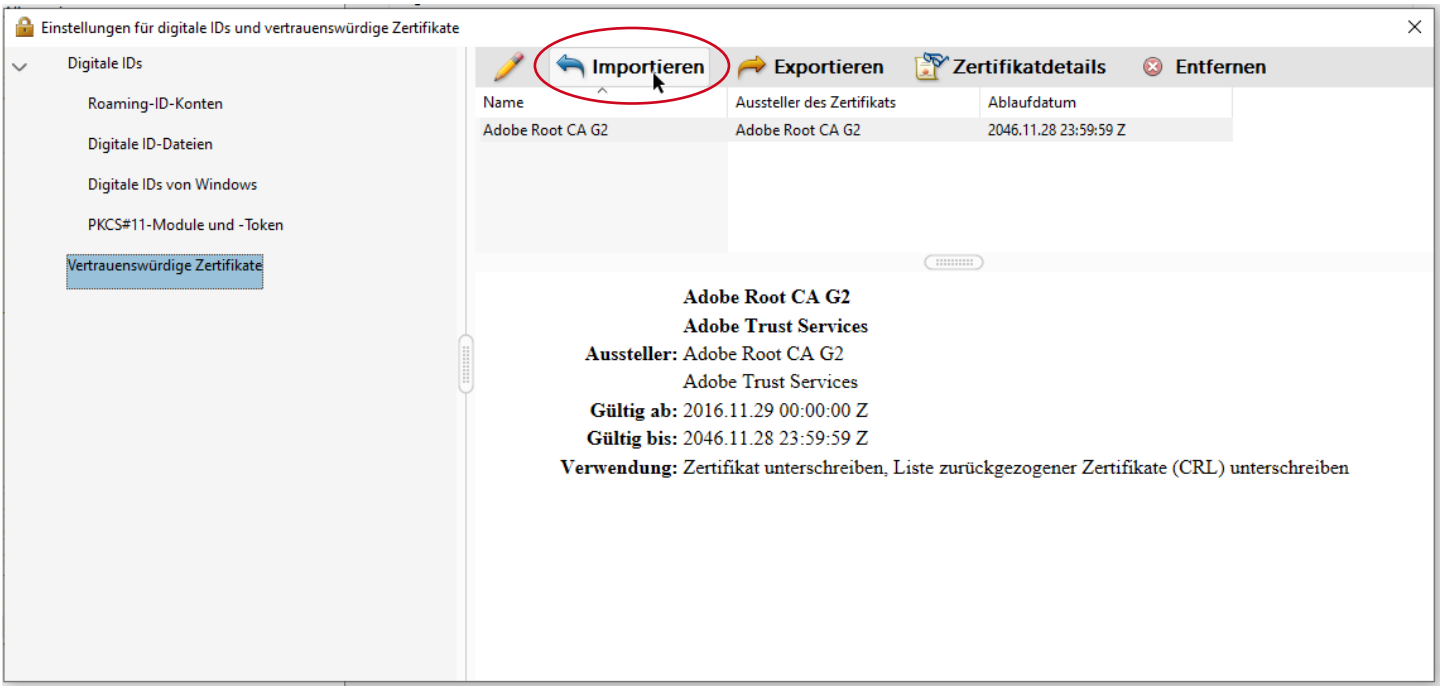


Abbildung 24: Zertifikate in Adobe importieren

Es öffnet sich das Dialogmenü „Zu importierende Kontakte auswählen“. Bitte klicken Sie hier auf „Durchsuchen“.

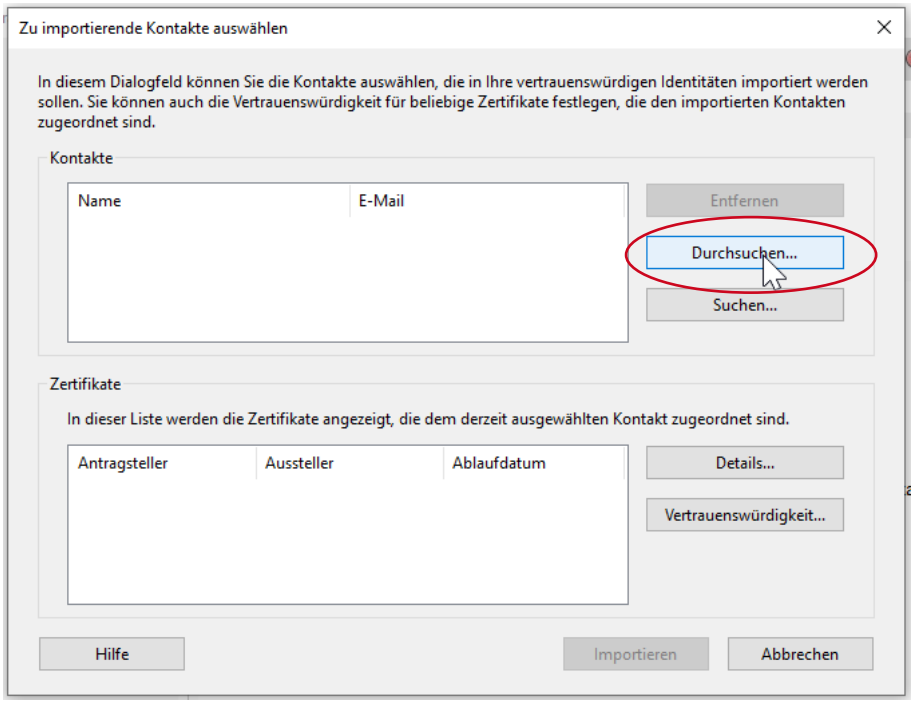
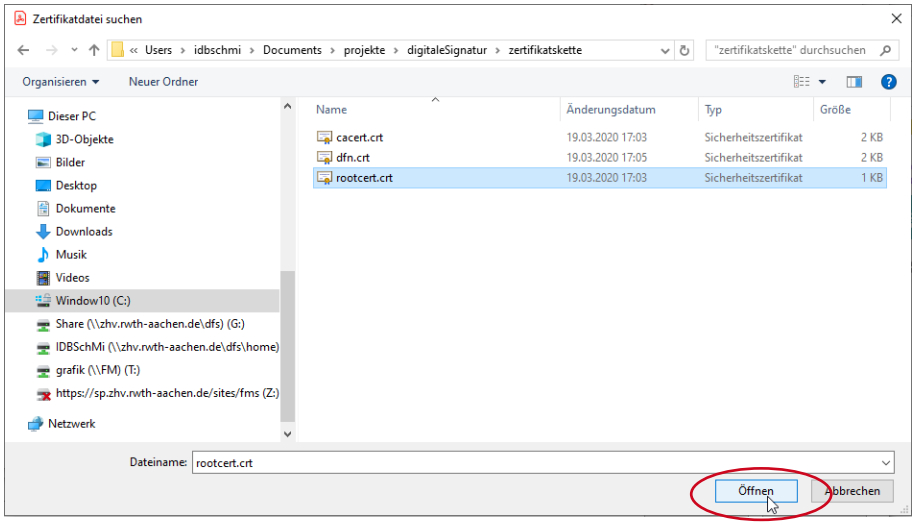


Abbildung 25: Zwischengespeichertes Stammzertifikat wählen

Wählen Sie die Datei mit dem zuvor zwischengespeicherten T-TeleSec GlobalRoot G 2 Zertifikat aus und klicken Sie auf „Öffnen“



Im Bereich „Kontakte“ wird der jeweilige Name des importierten Zertifikats angezeigt. Hier: T-TeleSec GlobalRoot Class 2. Wählen Sie dieses im Bereich „Kontakte“ im Feld „Name“ durch Anklicken aus.

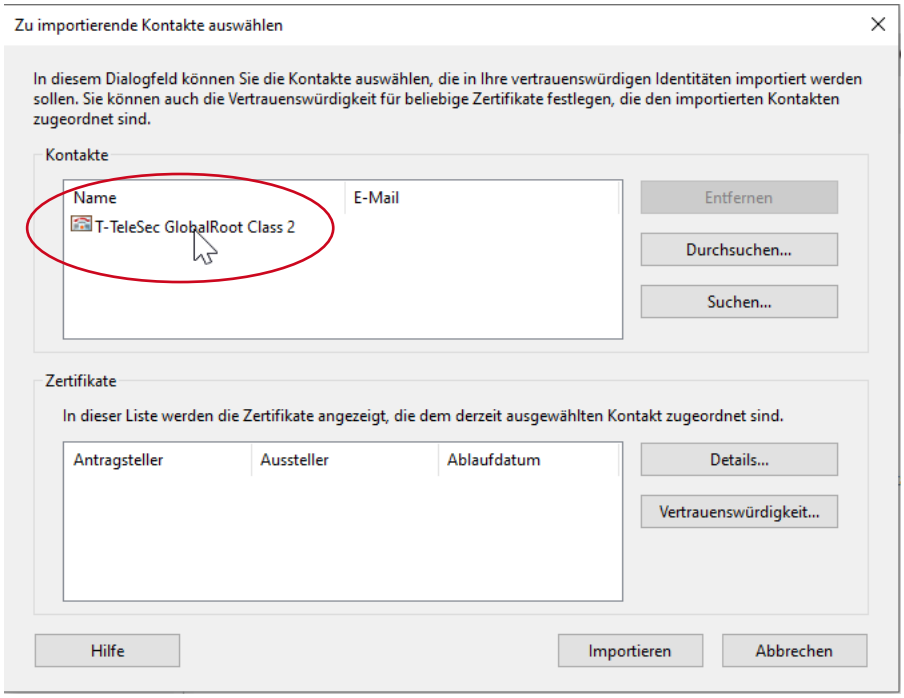


Abbildung 26: T-TeleSec Zertifikat als Kontakt wählen

Im Bereich „Zertifikate“ wird im Anschluss das zugehörige Zertifikat angezeigt.

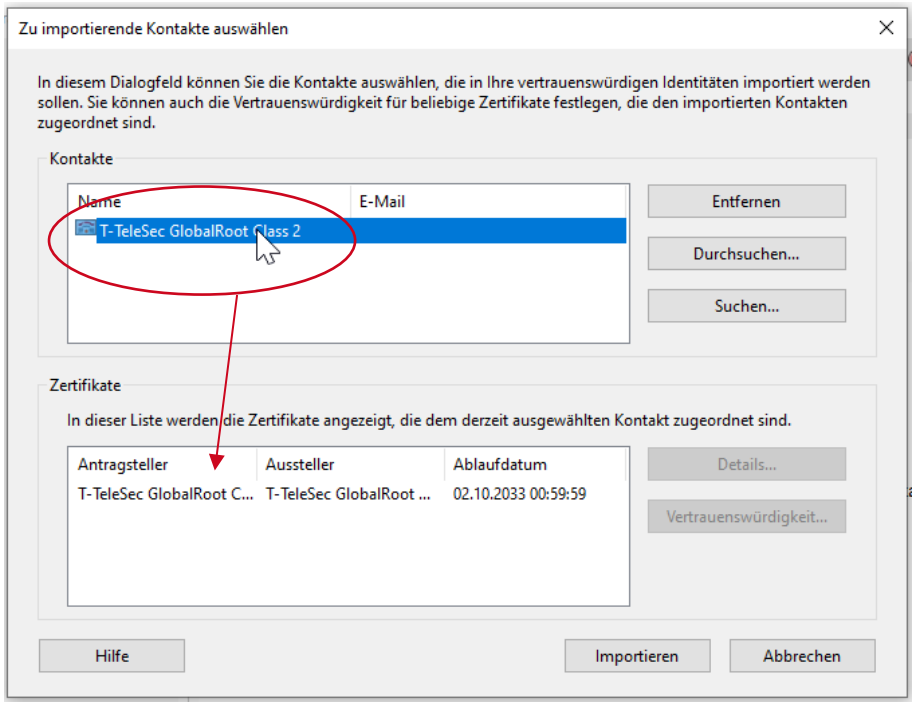


Abbildung 27: T-Telesec Zertifikat wird angezeigt

Wählen Sie jetzt wiederum im Bereich „Zertifikate“ das Zertifikat durch Klick aus.

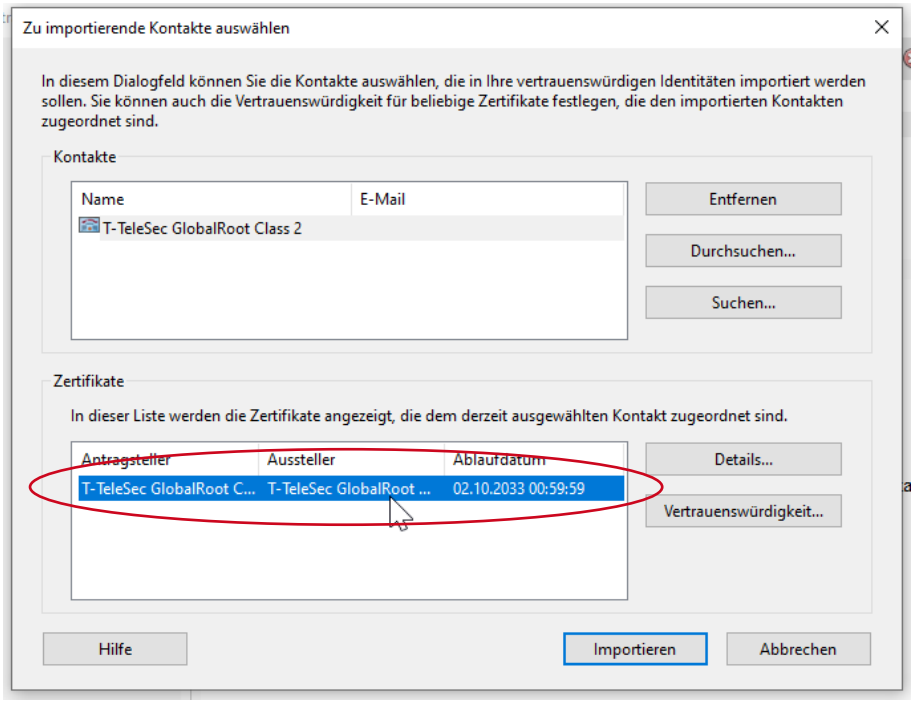


Abbildung 28: Zertifikat auswählen

Im Anschluss betätigen Sie bitte den Button „Vertrauenswürdigkeit“.

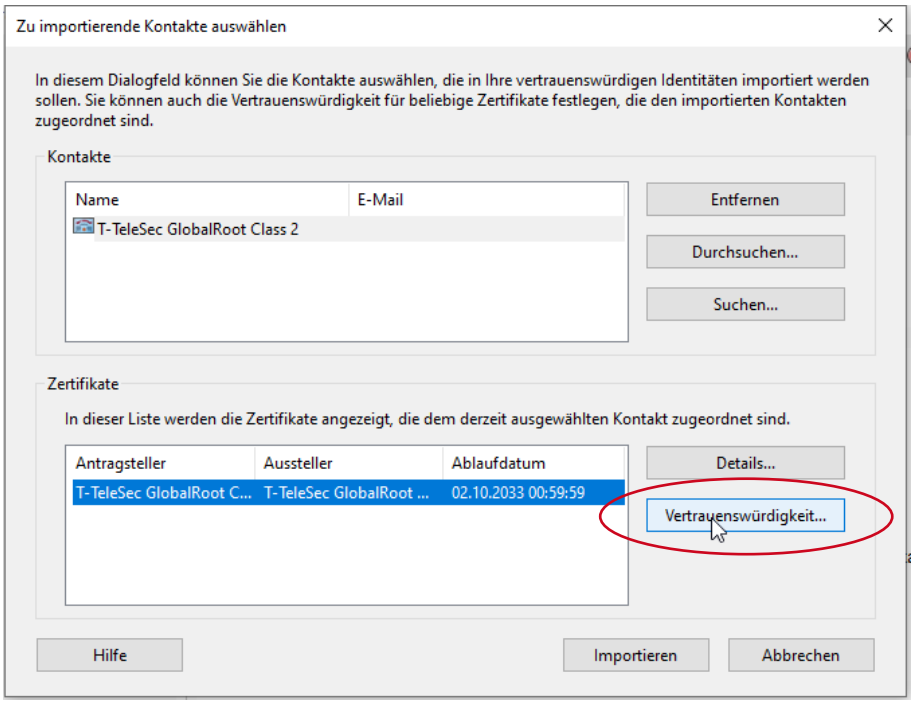


Abbildung 29: Vertrauenswürdigkeitsdialog öffnen

Es öffnet sich ein weiteres Dialogfenster „Kontakteinstellungen importieren“.

In diesem Dialogfenster haken Sie bitte für die Vertrauenswürdigkeit des Zertifikats die zwei Optionen „Dieses Zertifikat als vertrauenswürdigen Stamm verwenden“ und „Zertifizierte Dokumente“ an. Bitte schließen Sie das Dialogfenster anschließend mit OK.

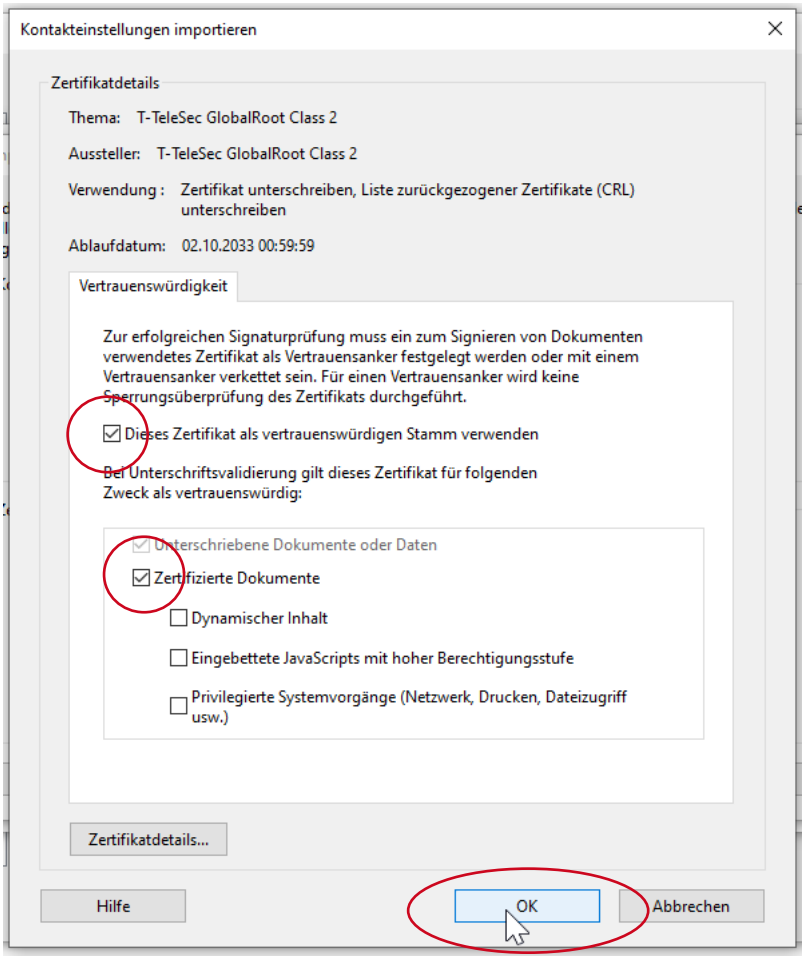


Abbildung 30: Kontakteinstellungen importieren

Bitte bestätigen Sie den Import des Stammzertifikats im Dialogfenster mit Button „Importieren“.

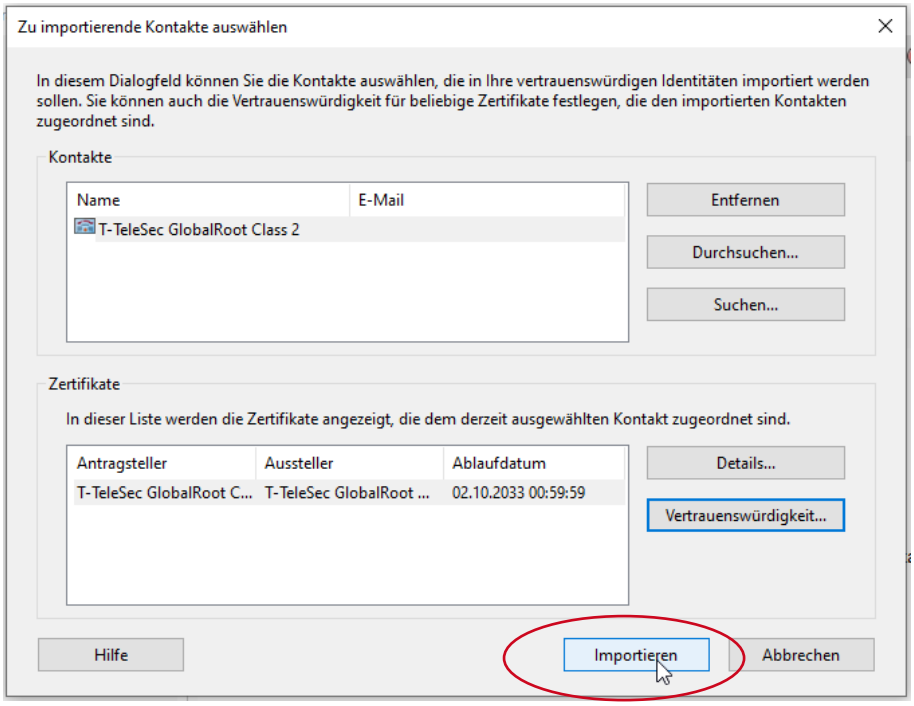


Abbildung 31: Stammzertifikat importieren

Bestätigen Sie den Import mit OK.

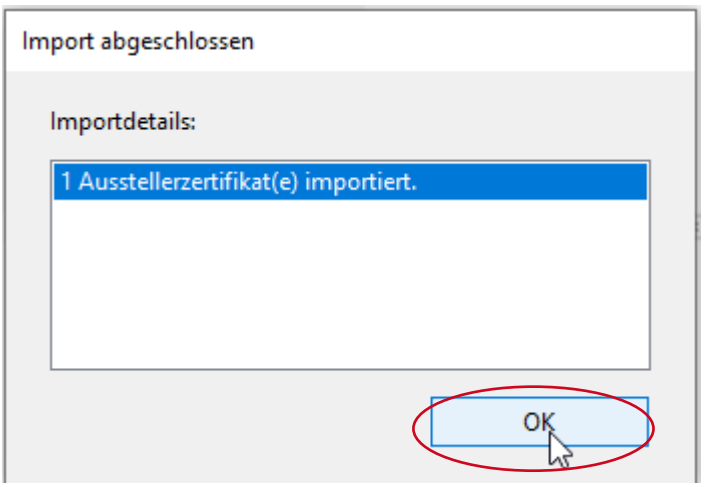


Abbildung 32: Zertifikatsimport abgeschlossen

Die Konfiguration der Zertifikatskette ist nun abgeschlossen und Sie können das Dialogfenster „Einstellungen für digitale IDs und vertrauenswürdige Zertifikate“ schließen.

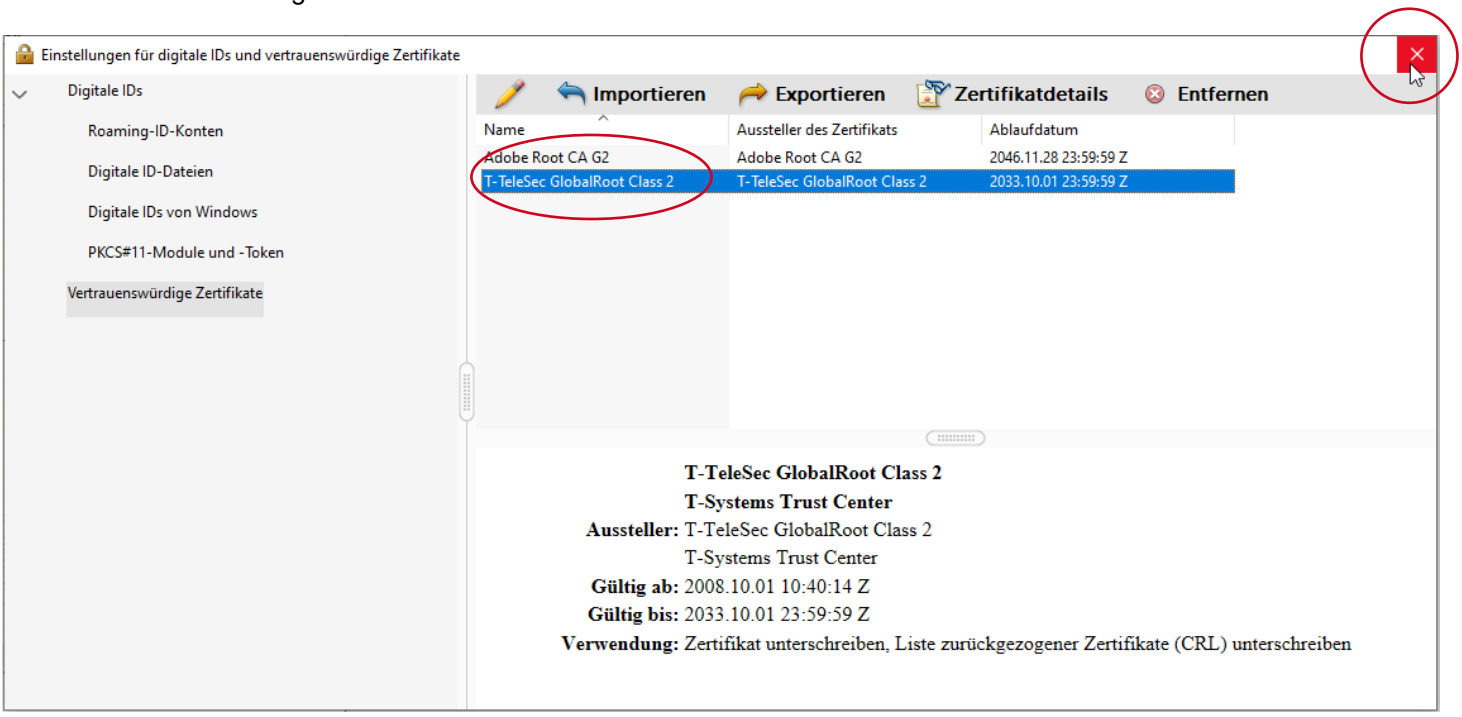


Abbildung 33: Einstellungen Vertrauenswürdige Zertifikate abgeschlossen

5 Elektronische Unterschrift konfigurieren

Bei der Erstkonfiguration Ihrer elektronischen Unterschrift legen Sie fest welche digitale ID Sie zur elektronischen Unterschrift verwenden möchten. Adobe bietet die Möglichkeit die Zertifikate aus dem Windows Zertifikatsspeicher zu verwenden („Eigene Zertifikate“).

Dazu öffnen Sie bitte im Acrobat Reader DC über „Bearbeiten“ das Dialogfenster „Einstellungen“. Dort Klicken Sie unter dem Navigationspunkt „Unterschriften“ im Bereich „Identitäten und vertrauenswürdige Zertifikate“ den Button „Weitere“.

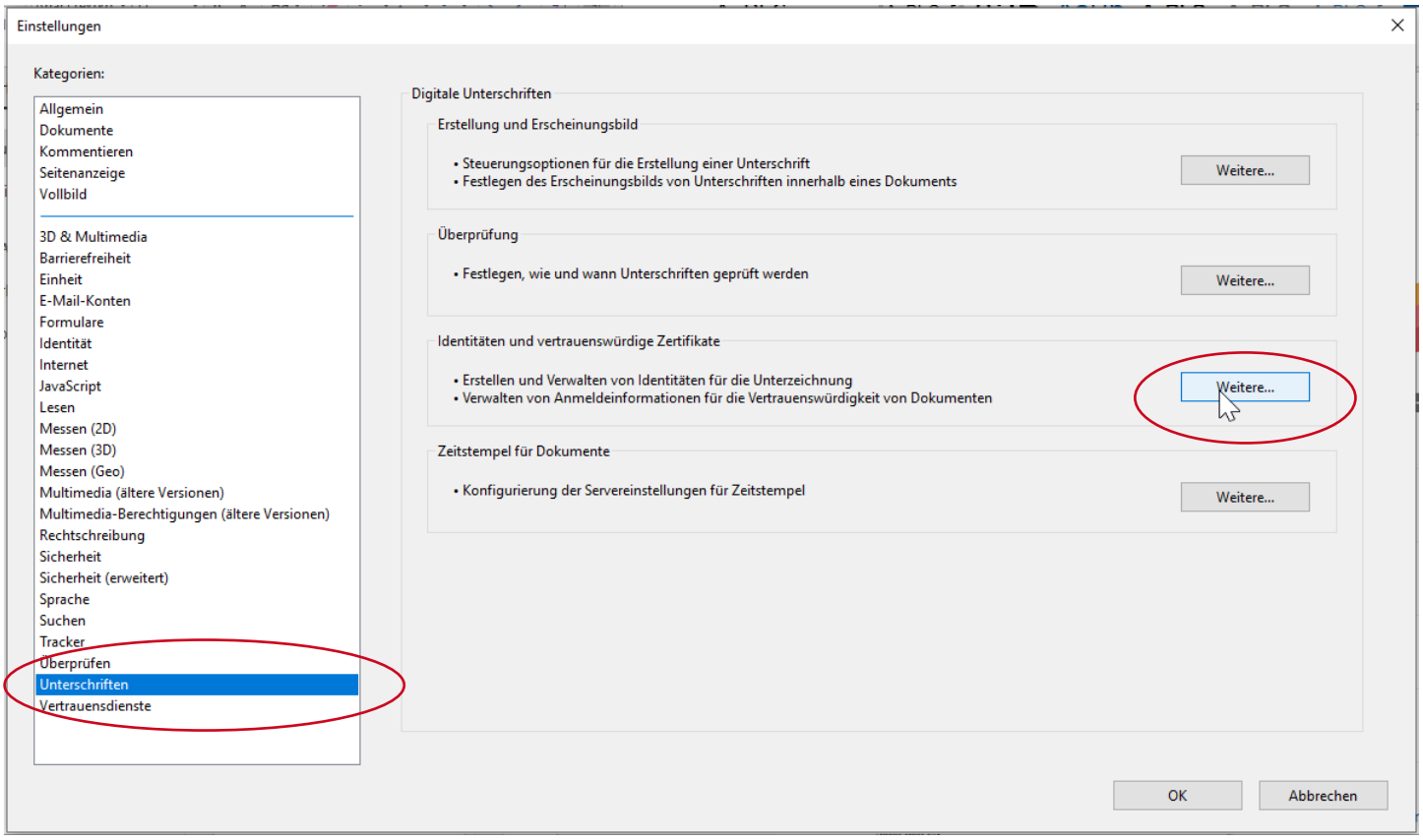


Abbildung 34: Identitäten verwalten

Es öffnet sich das Dialogfenster „Einstellungen für digitale IDs und vertrauenswürdige Zertifikate“. Hier navigieren Sie bitte zum Menüpunkt „Digitale IDs von Windows“, um die Zertifikate aus dem Windows Zertifikatsspeicher zu verwenden.

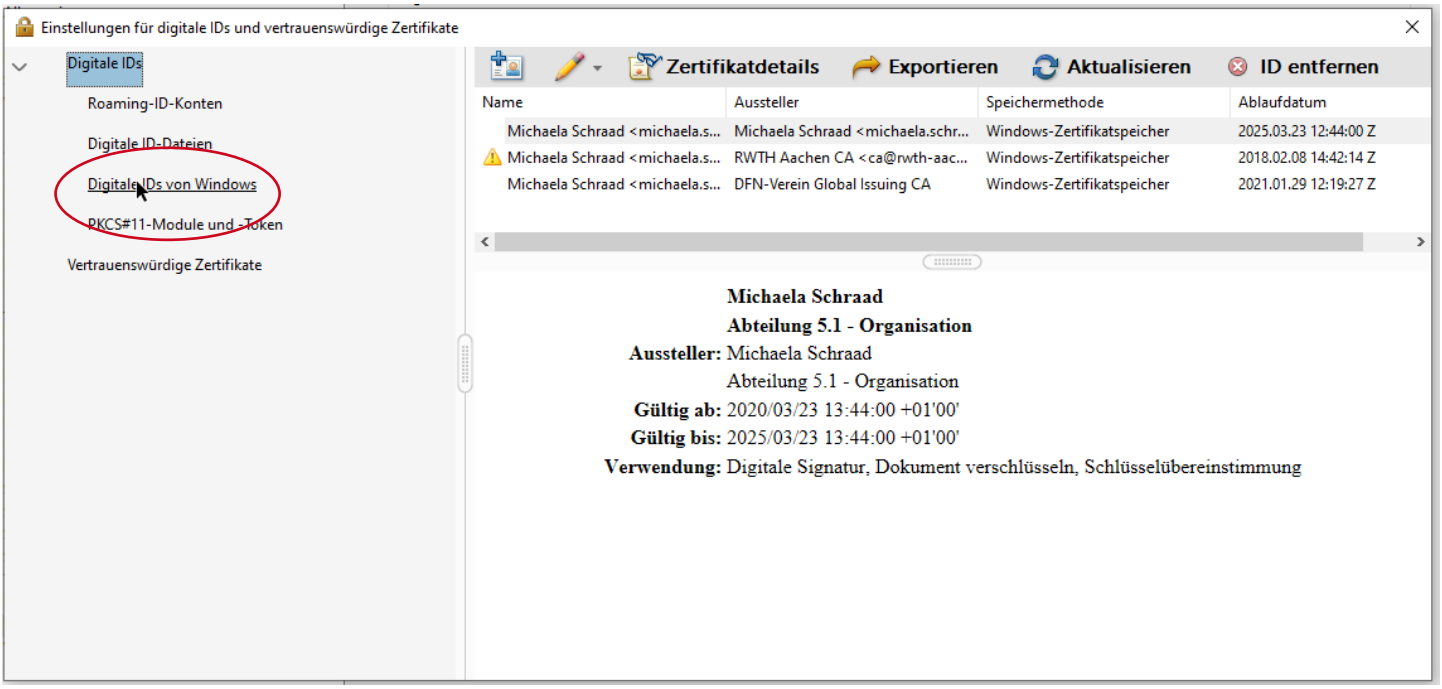


Abbildung 35: Digitale ID von Windows konfigurieren

Wird in dieser Listendarstellung keine digitale ID angezeigt, verfügen Sie entweder noch nicht über ein persönliches Nutzerzertifikat oder Sie haben dies bzw. den privaten Schlüssel Ihres Nutzerzertifikates noch nicht in den Windows-Zertifikatsstore (Meine Zertifikate) importiert. (vgl. Kapitel **2 Persönliches Nutzerzertifikat**, S.**2**)

Verfügen Sie über mehrere noch gültige digitale IDs (weil Sie bspw. E-Mails für unterschiedliche E-Mail-Adressen signieren wollen) wählen Sie bitte per Klick die zu Ihrem persönlichen Nutzerzertifikat gehörende digitale ID aus, mit der Sie standardmäßig elektronisch unterschreiben wollen. Wählen Sie dabei die digitale ID aus mit der Ihr Name und Ihre persönliche E-Mail-Adresse verbunden sind.

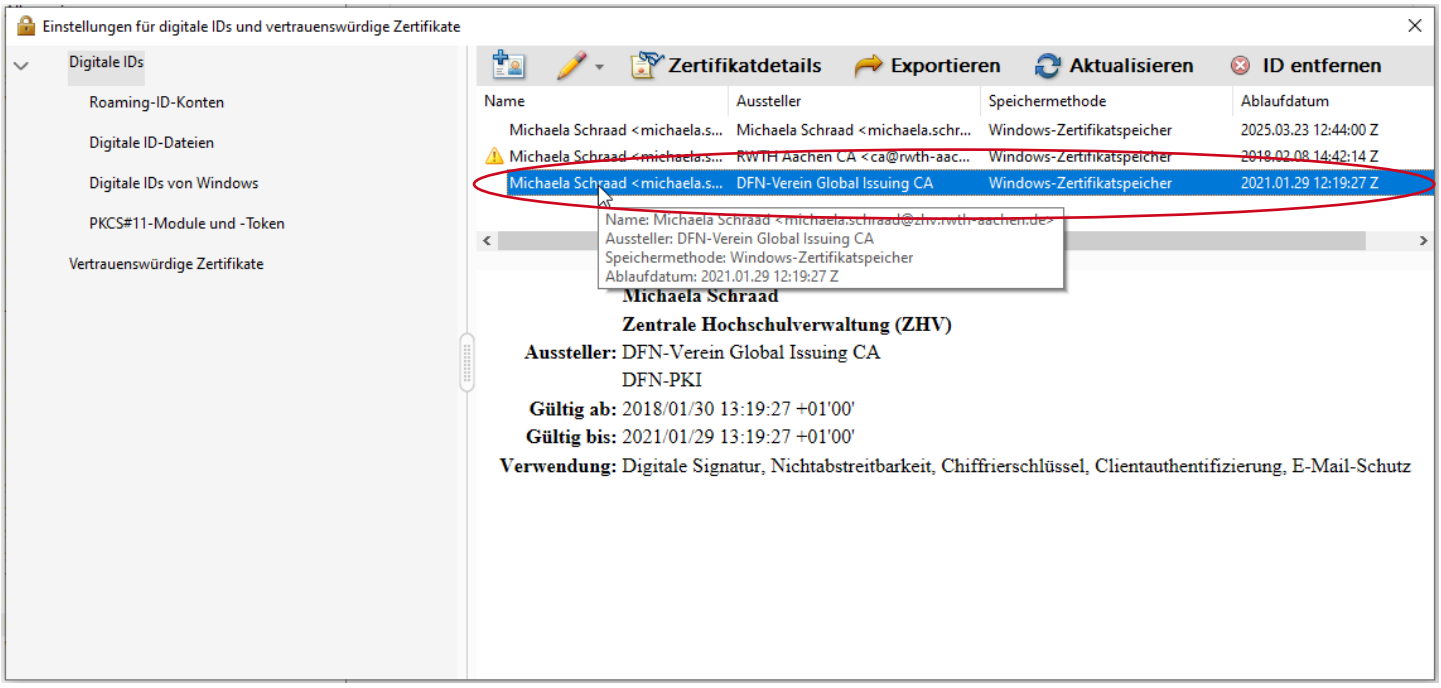


Abbildung 36: Digitale ID wählen

Digitale IDs zu bereits abgelaufenen Zertifikaten werden wie im obigen Beispiel mit einem gelben Ausrufungszeichen gekennzeichnet und können an dieser Stelle nicht ausgewählt werden.

Bitte beachten Sie, dass digitale IDs zu Gruppenzertifikaten, die Sie ggf. für die Signierung von funktionalen E-Mail-Adressen verwenden, an dieser Stelle nicht ausgewählt werden dürfen. Gruppenzertifikate erkennen Sie am vorangestellten Kürzel „GRP“.

Öffnen Sie nun in der Top-Navigation über Klick auf den Button „Verwendungsoptionen“ (Stift-Button) das Drop-Down-Menü.

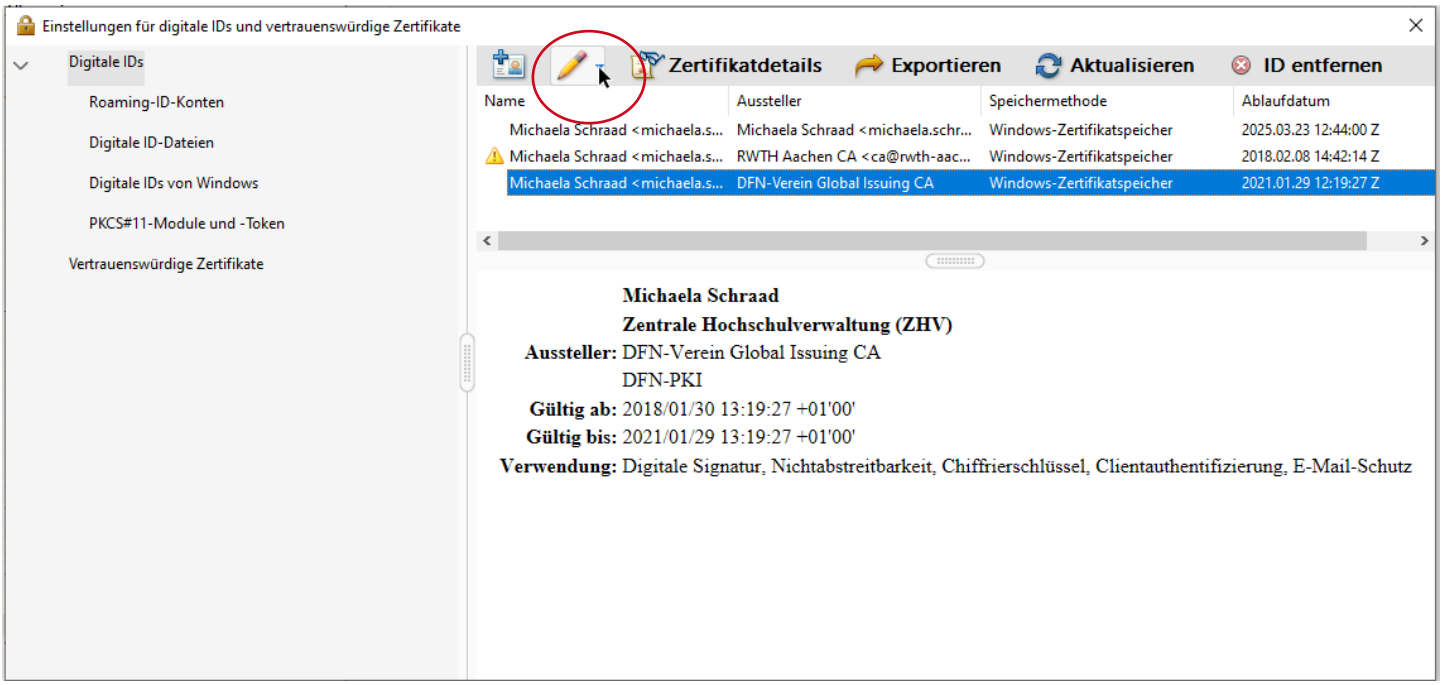


Abbildung 37: Digitale ID zum Unterschreiben wählen

Klicken Sie zur Konfiguration Ihrer elektronischen Unterschrift auf den Untermenüpunkt „Zum Unterschreiben verwenden“.

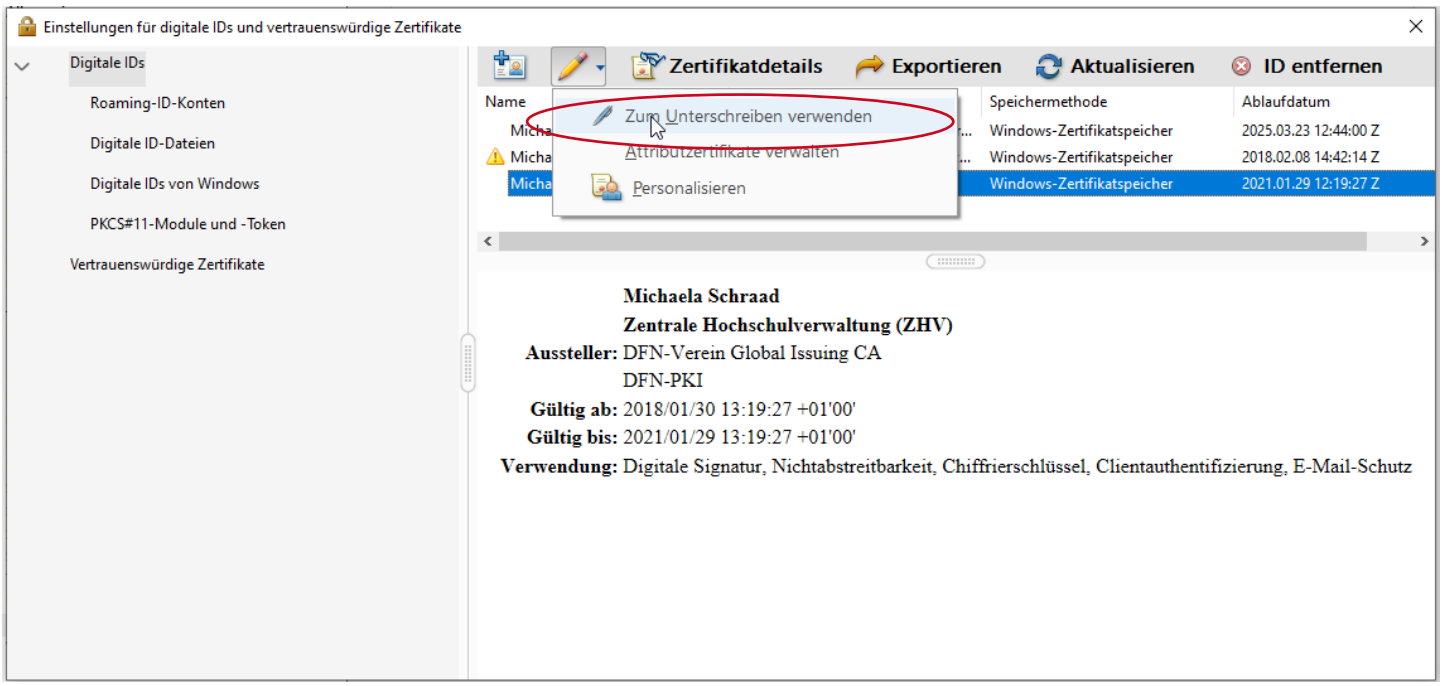


Abbildung 38: Digitale ID zum Unterschreiben verwenden

In der Listendarstellung wird das für die elektronische Unterschrift verwendete Zertifikat mit einem Stift markiert dargestellt.

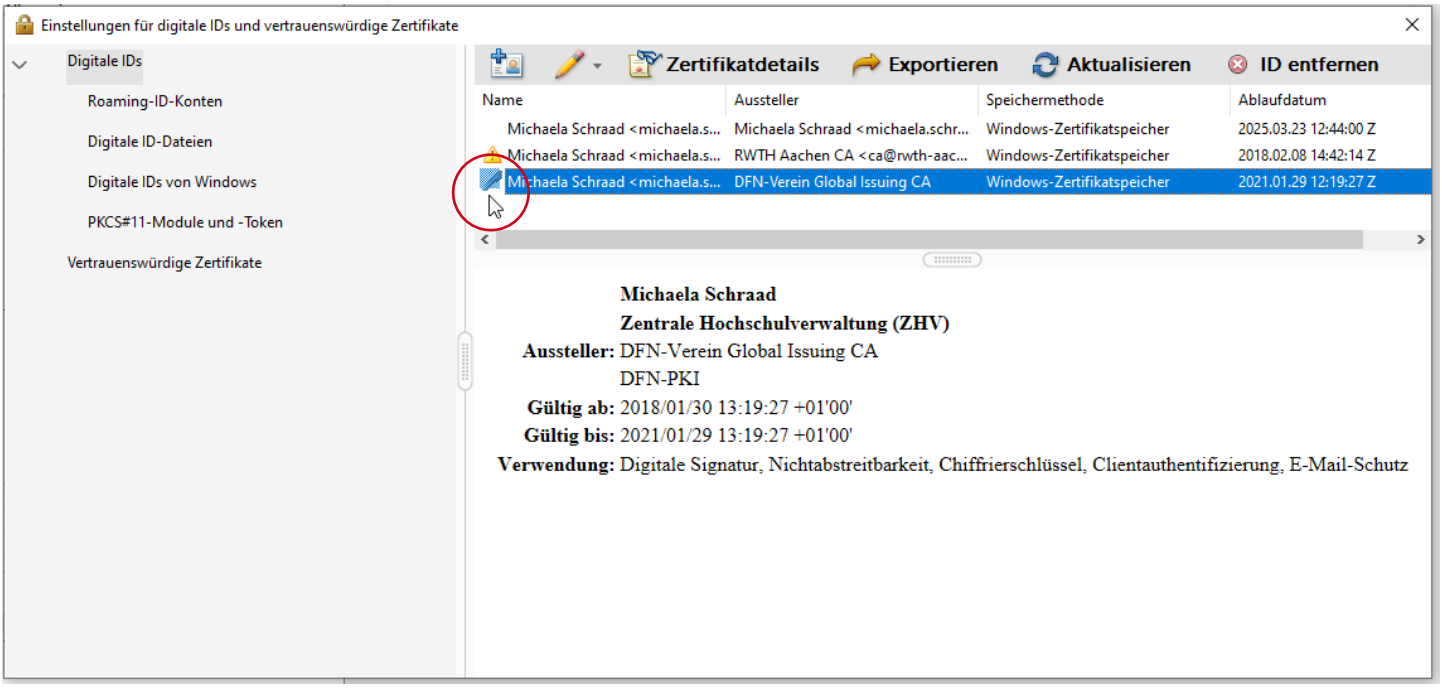


Abbildung 39: Digitale ID ist konfiguriert

Schließen Sie das Dialogfenster.

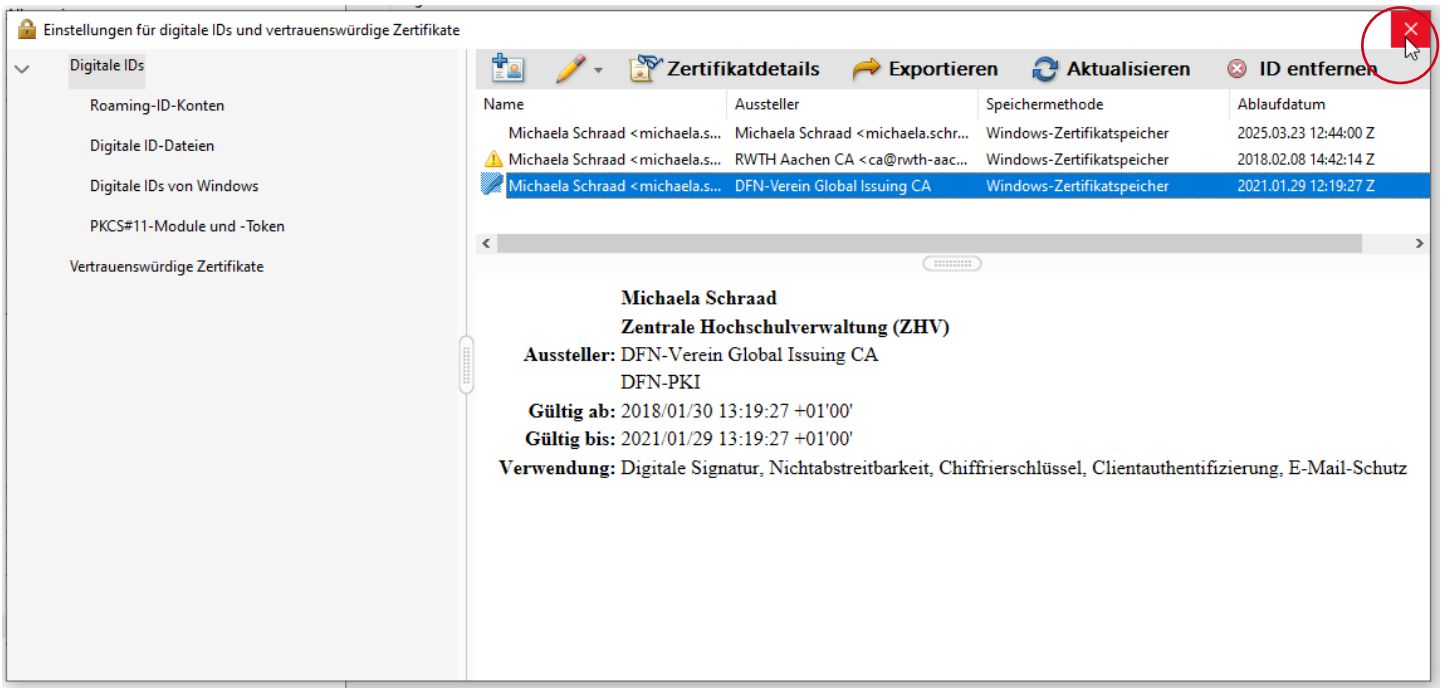


Abbildung 40: Einstellungen für digitale IDs schließen

Mit Klick auf OK wird auch das Dialogfenster geschlossen und die Konfiguration ist nun abgeschlossen und sie können ab jetzt PDF-Dokumente elektronisch unterschreiben.

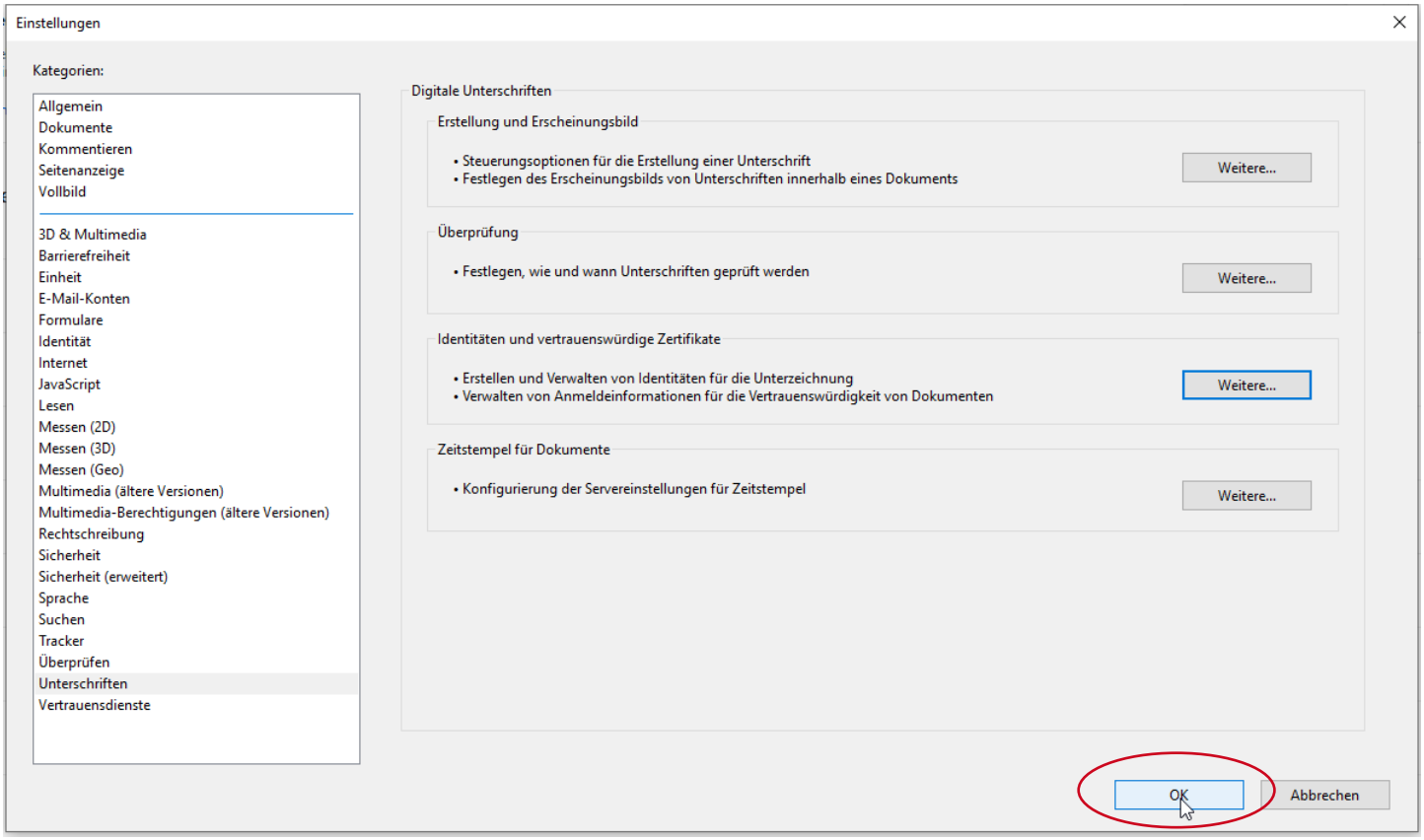


Abbildung 41: Einstellungen schließen

6 PDF-Dokument elektronisch unterschreiben

Jetzt haben Sie alle Konfigurationen des Acrobat Reader DC aus den vorangegangenen Kapiteln abgeschlossen. Um nun PDF-Dokumente elektronisch unterschreiben zu können, schließen Sie bitte nach der initialen Konfiguration einmalig den Adobe Acrobat Reader und starten ihn erneut.

6.1 PDF-Dokument öffnen

Öffnen Sie das PDF-Dokument, welches Sie unterschreiben wollen.

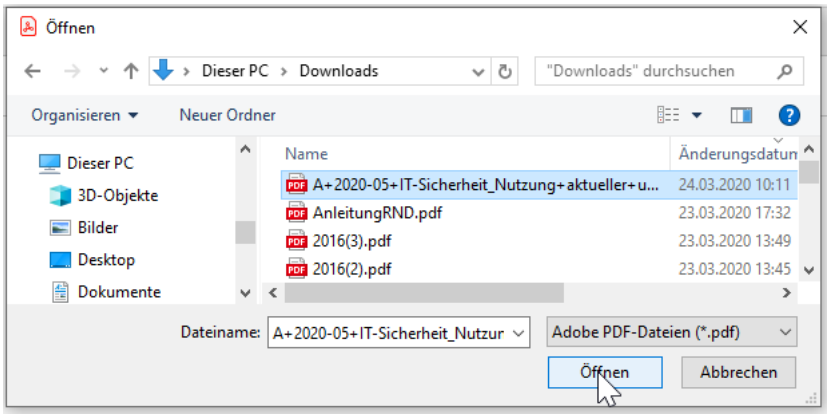


Abbildung 42: PDF-Dokument öffnen

6.2 Unterschreiben und Dokument sperren

Öffnen Sie im Acrobat Reader DC den Reiter „Werkzeuge“.

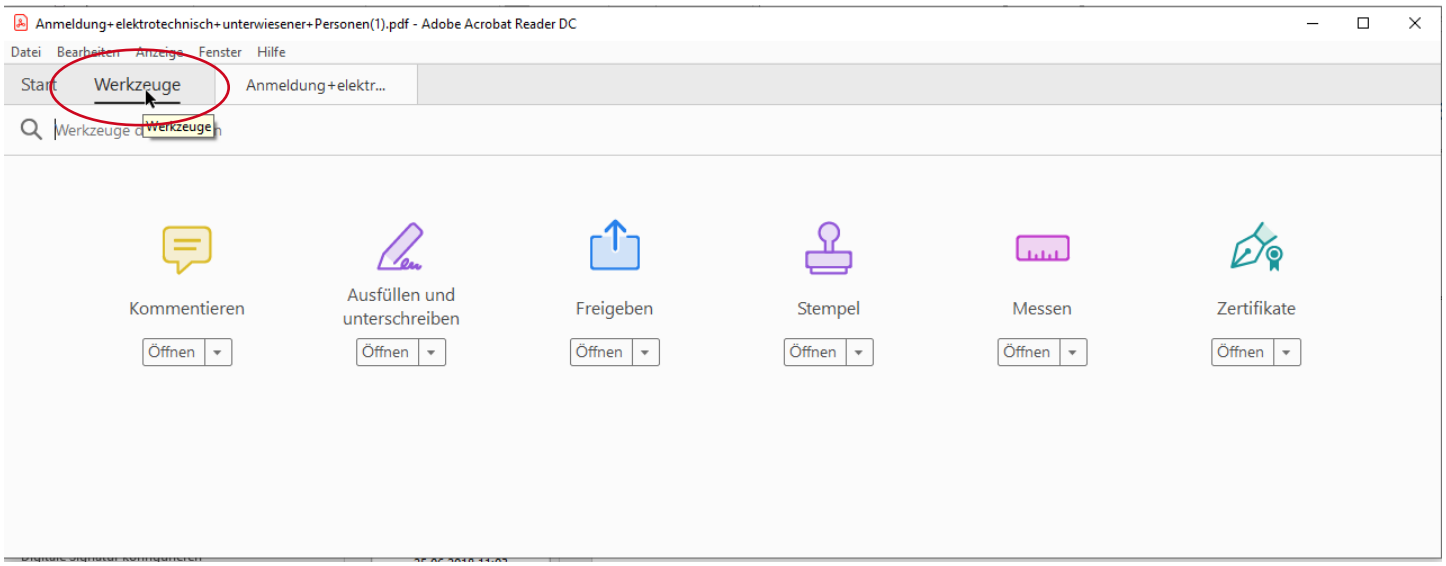


Abbildung 43: Werkzeuge wählen

Klicken Sie hier auf Zertifikate öffnen.

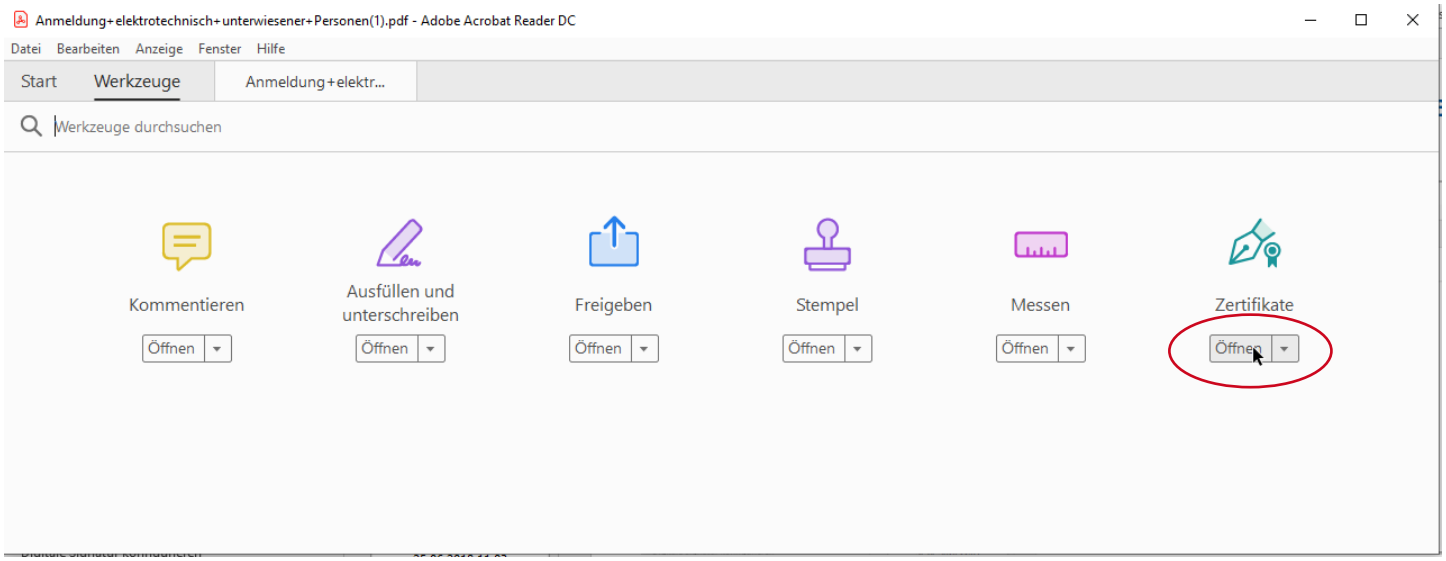


Abbildung 44: Zertifikate wählen

In der Werkzeugleiste klicken Sie dann bitte auf „Digital unterschreiben“.

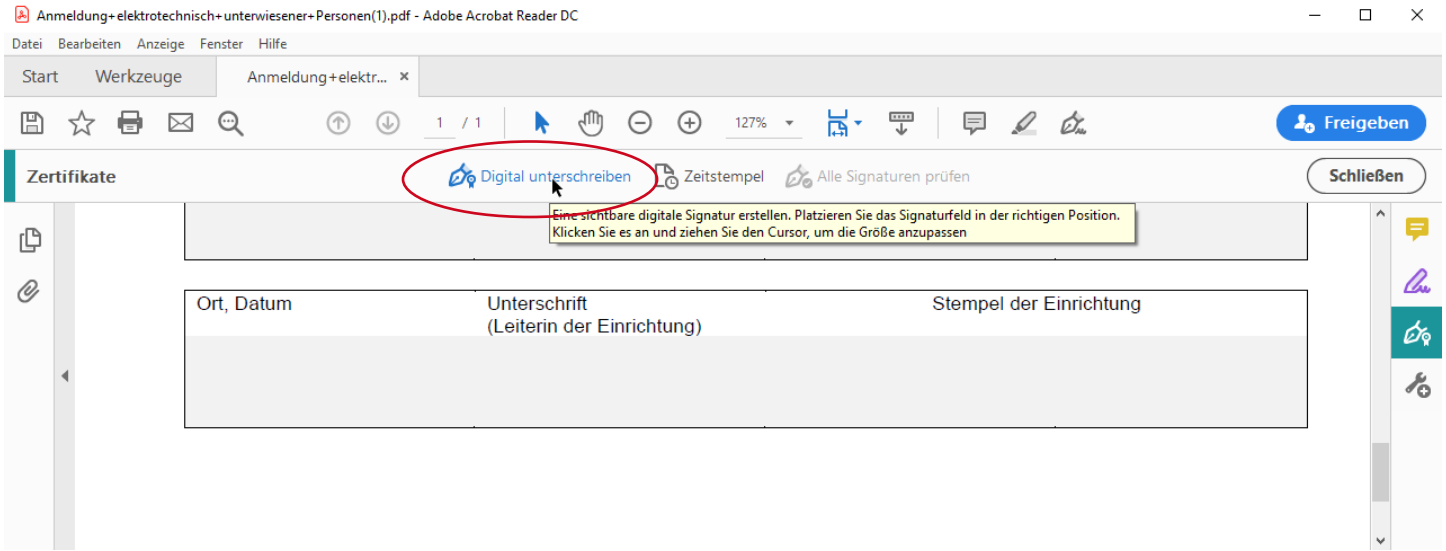


Abbildung 45: „Digital unterschreiben“ wählen

Sie können entscheiden, ob Sie das daraufhin sich öffnende Meldungsfenster weiterhin angezeigt bekommen wollen. Bitte bestätigen Sie Ihre Entscheidung mit OK.

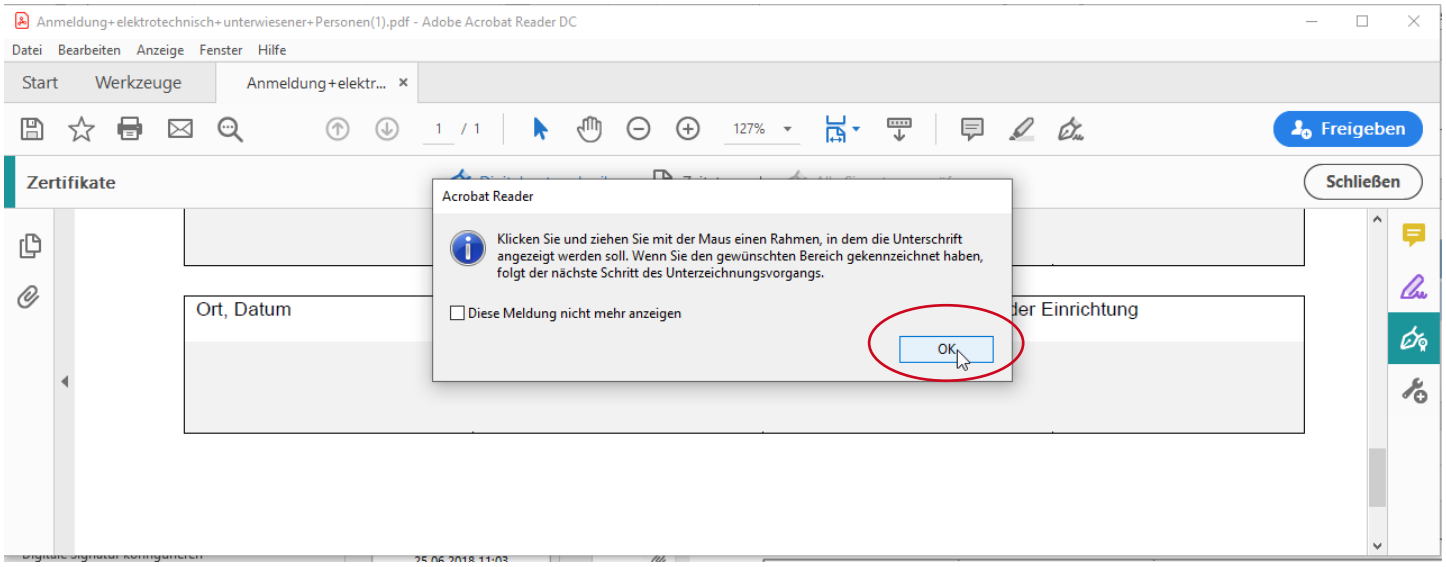


Abbildung 46: Infofenster zum Unterschriftenbereich

Abhängig von der Gestaltung des Formulars ziehen Sie bitte an der vorgesehenen Stelle im Formular mit der Maus einen Bereich für die Platzierung der elektronischen Unterschrift auf.

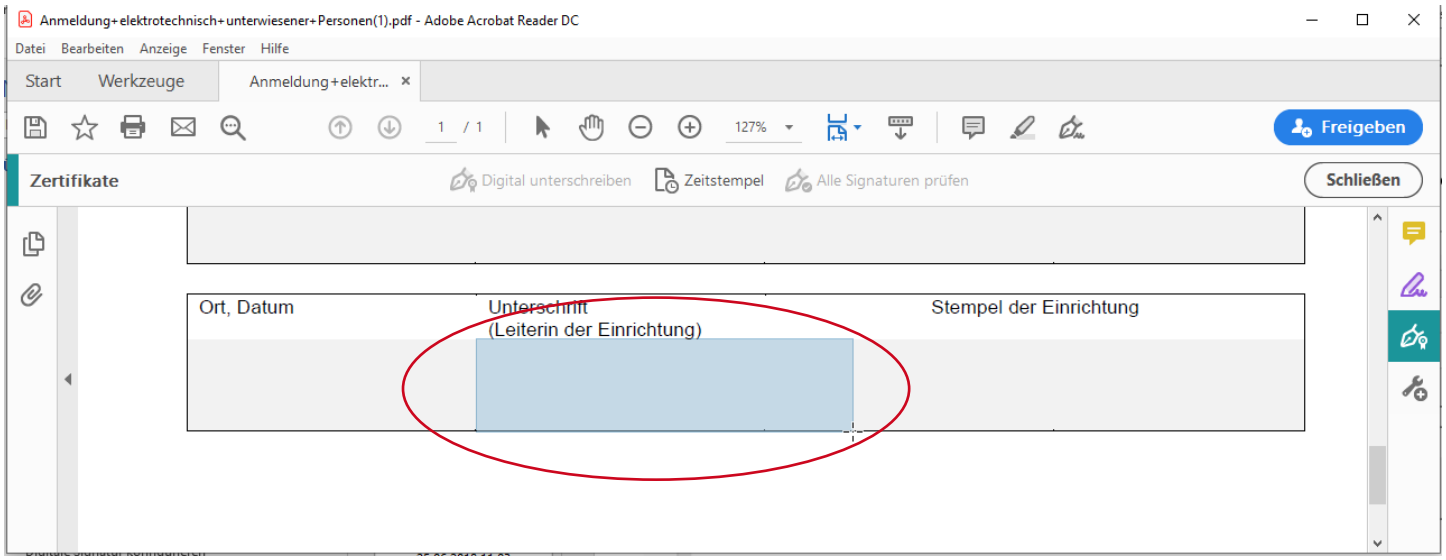


Abbildung 47: Unterschriftenbereich

Es öffnet sich ein Dialogfenster in dem Sie auswählen können, mit welcher digitalen ID das Dokument unterschrieben werden soll.

Die in Kapitel **5 Elektronische Unterschrift konfigurieren**, S. **24** vorkonfigurierte digitale ID ist dabei vorausgewählt.

Bitte beachten Sie auch an dieser Stelle, dass das Unterschreiben mit digitalen IDs zu Gruppenzertifikaten nicht zulässig ist. Gruppenzertifikate erkennen Sie an dem vorangestellten Kürzel „GRP“.

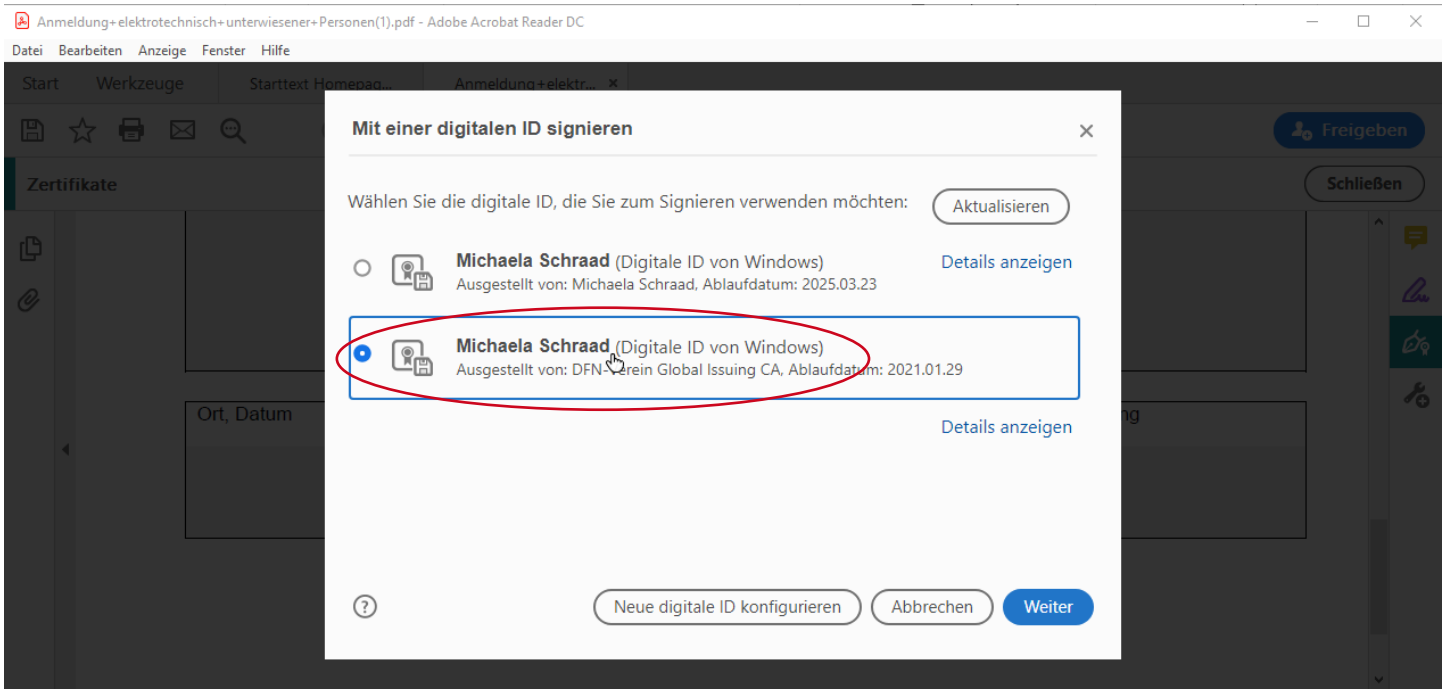


Abbildung 48: Wählen der digitalen ID

Bestätigen Sie die Auswahl über Klick auf den Button Weiter.

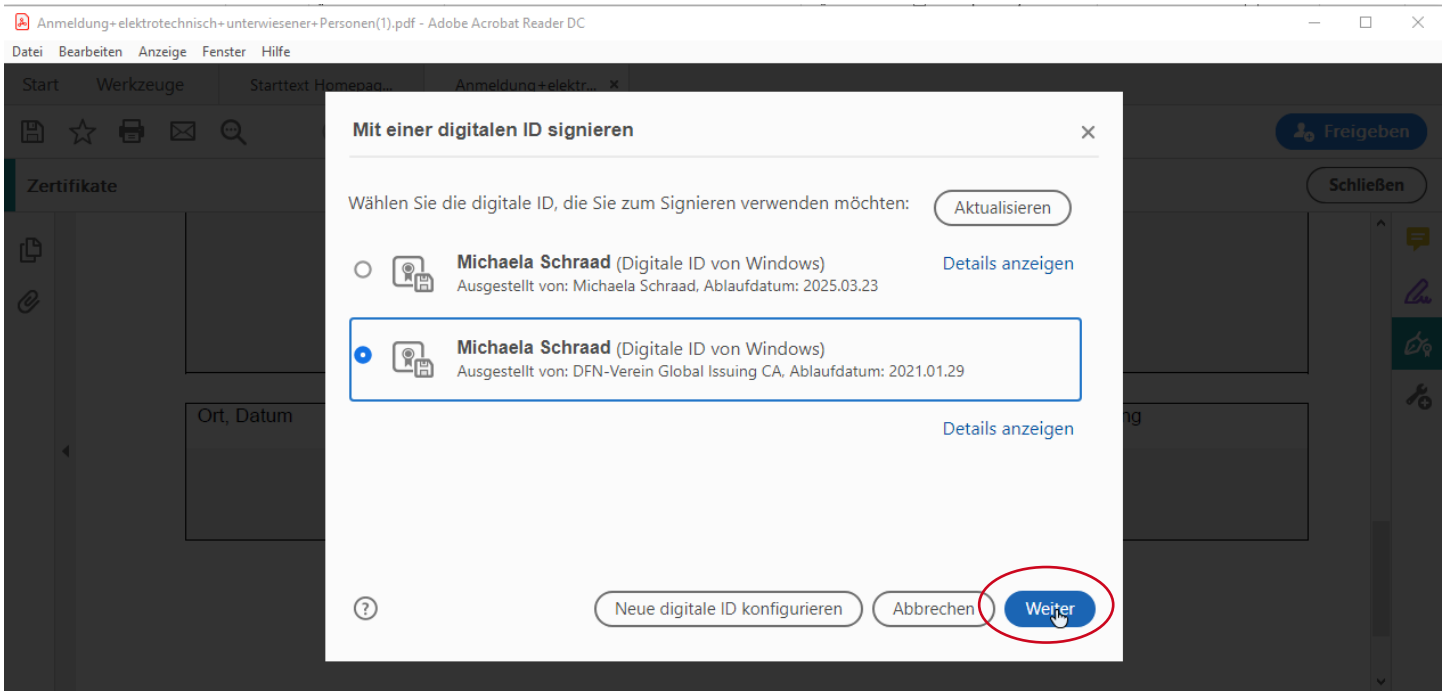


Abbildung 49: Bestätigen der digitalen ID

Nutzen Sie die elektronische Unterschrift das erste Mal, kann es sein, dass Sie abhängig von Ihren Windows-Sicherheitseinstellungen dem Acrobat Reader DC erlauben müssen auf Ihren privaten Schlüssel Ihres persönlichen Nutzerzertifikats zugreifen zu dürfen. Bitte bestätigen Sie dies über Klick auf „Zulassen“.

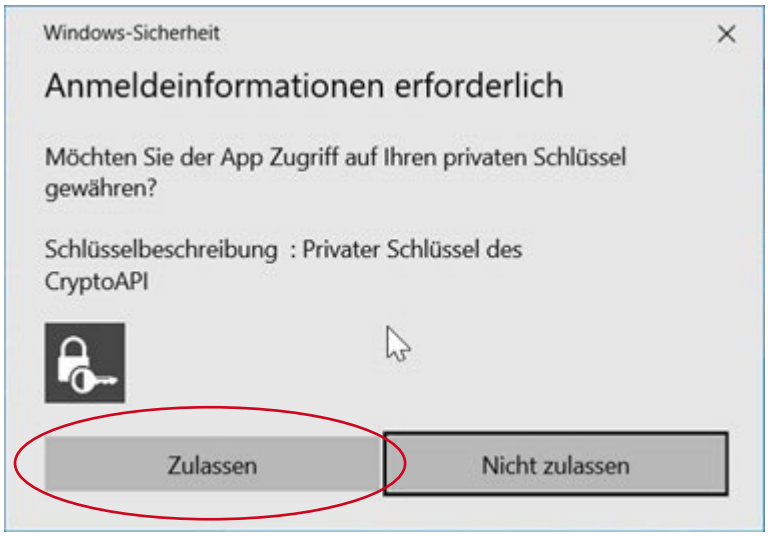


Abbildung 50: Zugriff auf privaten Schlüssel erlauben

Es öffnet sich das Vorschau-Fenster zur elektronischen Unterschrift.

Bitte wählen Sie als Erscheinungsbild die Anzeige als „Standardtext“ aus.

Bitte wählen Sie die Option „Dokument nach dem Signieren sperren“ nur an, wenn Sie die letzte Person sind, die das Dokument unterschreiben muss. Das Dokument kann danach nicht mehr verändert werden.

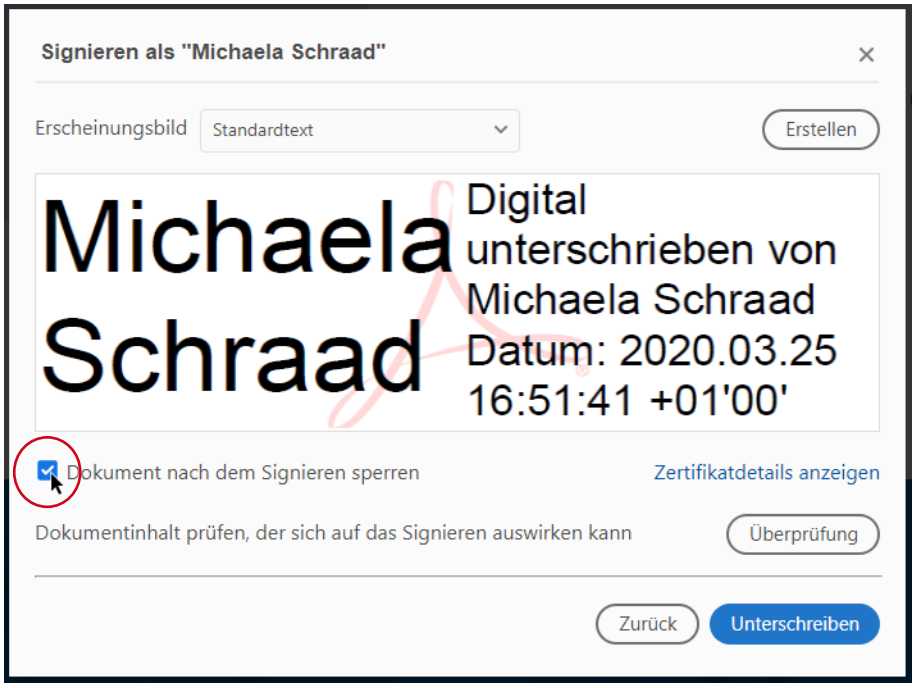


Abbildung 51: Dokument sperren

Mit Klick auf „Unterschreiben“ wird die Signierung des Dokumentes gestartet.

Abbildung 52: Endgültig unterschreiben

Im Normalfall öffnet sich beim Klick auf „Unterschreiben“ ein Dialogfenster und Sie werden aufgefordert das Dokument unter einem neuen Namen zu speichern. Erst nach dem Speichern wird die elektronische Unterschrift auf dem Dokument angezeigt.

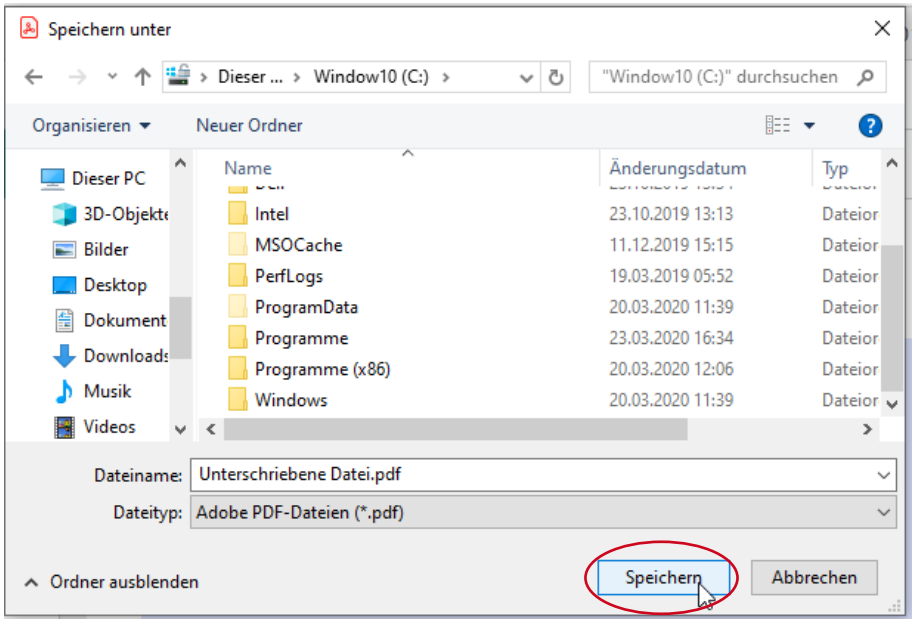


Abbildung 53: Unterschriebenes Dokument speichern

Wird Ihnen vor oder nach Öffnen des „Speichern-unter“-Dialogs eine Sicherheitswarnung bezüglich des Zeitstempelservers des DFN präsentiert, können Sie das Häkchen „Gewählte Aktion für diese Webseite für alle PDF-Dokumente speichern“ aktivieren, so dass Sie diese Meldung nur beim ersten Mal über Klick auf den Button „Zulassen“ bestätigen müssen.

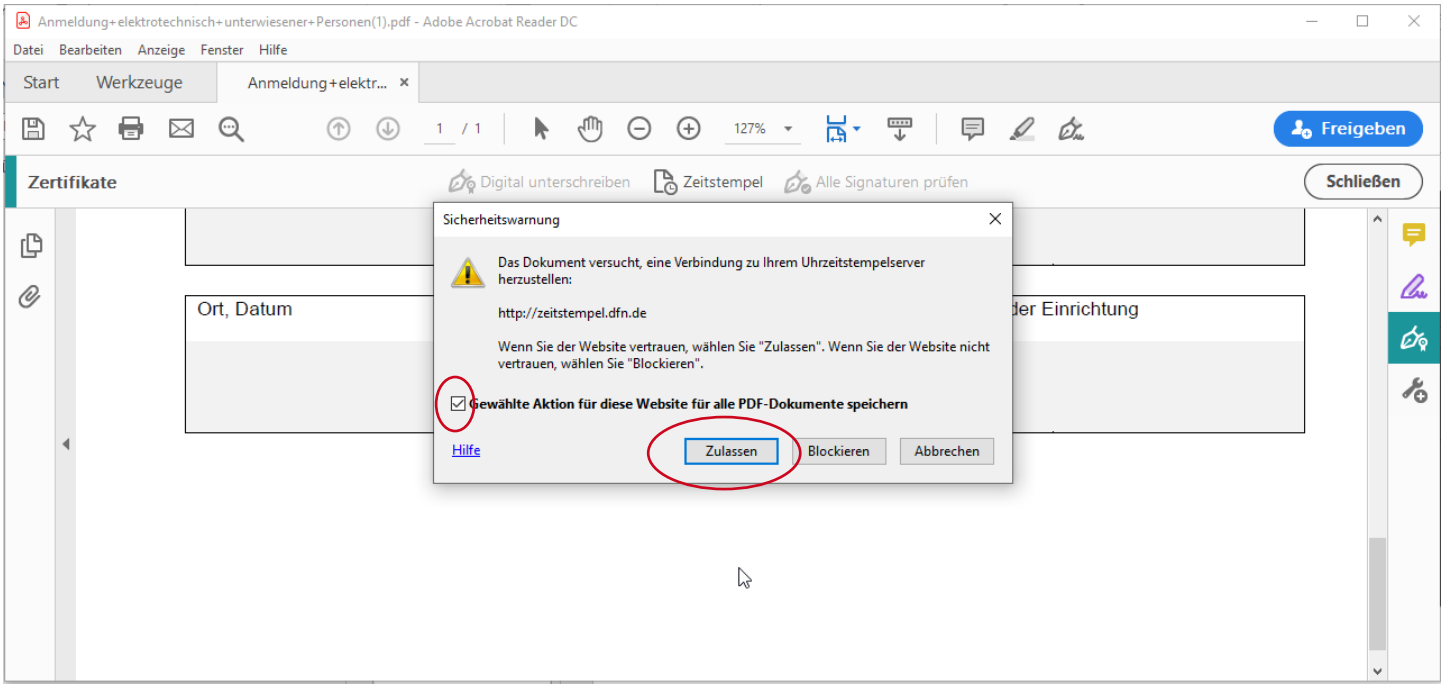


Abbildung 54: DFN Zeitstempeldienst bestätigen

Sollten Sie während des Unterschriftsvorgangs keinen Zugriff auf das Internet haben oder kann der Zeitstempelserver des DFN aus anderen Gründen nicht erreicht werden, bekommen Sie eine Fehlermeldung angezeigt.

In einem solchen Fall, wird anstelle des Zeitstempels des DFN-Zeitstempelservers die lokale Uhrzeit des jeweiligen Rechners zum Unterschreiben verwendet. Dies ist nicht zulässig für alle Dokumente bei denen Fristen für die Unterzeichnung gelten, da die Uhrzeit auf dem lokalen Rechner manipulierbar ist. Bitte stellen Sie in dem Fall sicher, dass die Verbindung zum DFN-Zeitstempelserver möglich ist und unterschreiben Sie das Dokument erneut.

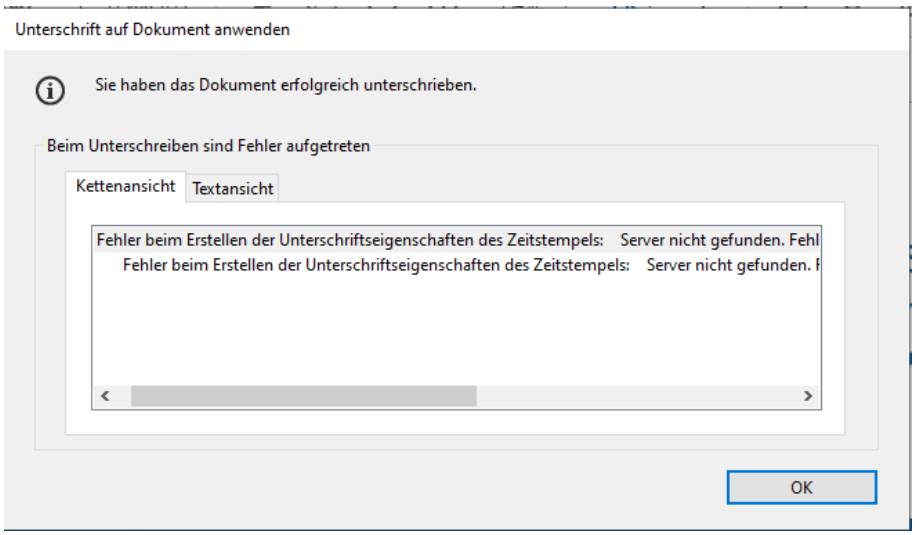


Abbildung 55: Fehlermeldung Zeitstempelserver

Wird Ihnen nach dem Speichern in der Statusleiste des Dokumentes die Meldung „Unterschrieben und alle Unterschriften sind gültig“ angezeigt, haben Sie das Dokument verbindlich mit einer elektronischen Unterschrift unterschrieben.

Es kann danach nicht mehr verändert werden, falls Sie wie in **Abbildung 51: Dokument sperren** beschrieben, die Checkbox „Dokument nach dem Signieren sperren“ angeklickt haben.

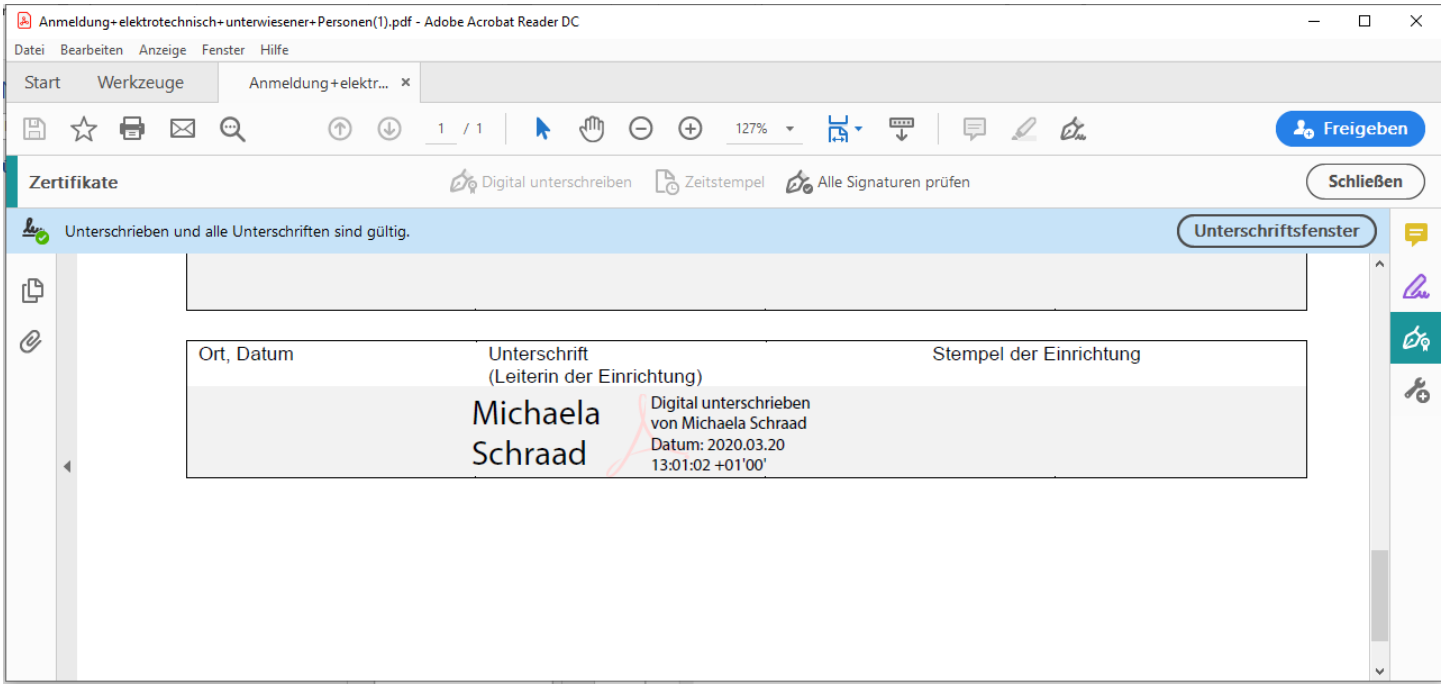


Abbildung 56: Abbildung der Adobe elektronischen Unterschrift

6.3 Mehrstufige Unterschriften

Die Vorgehensweise für Dokumente, die von mehreren Personen unterzeichnet werden müssen, entspricht für die Person, die das Dokument als letztes unterschreibt, in jedem Schritt der Anleitung aus Kapitel **6.2 Unterschreiben und Dokument sperren**, S. **30**.

Für alle Personen, die das Dokument im Vorfeld unterzeichnen, unterscheidet sich die Anleitung aus Kapitel **6.2 Unterschreiben und Dokument sperren**, S. **30**. nur in einem Punkt. Anstelle der in **Abbildung 51: Dokument sperren** aktivierten Checkbox „Dokument nach dem Signieren sperren“, bleibt die Checkbox in diesem Fall deaktiviert.

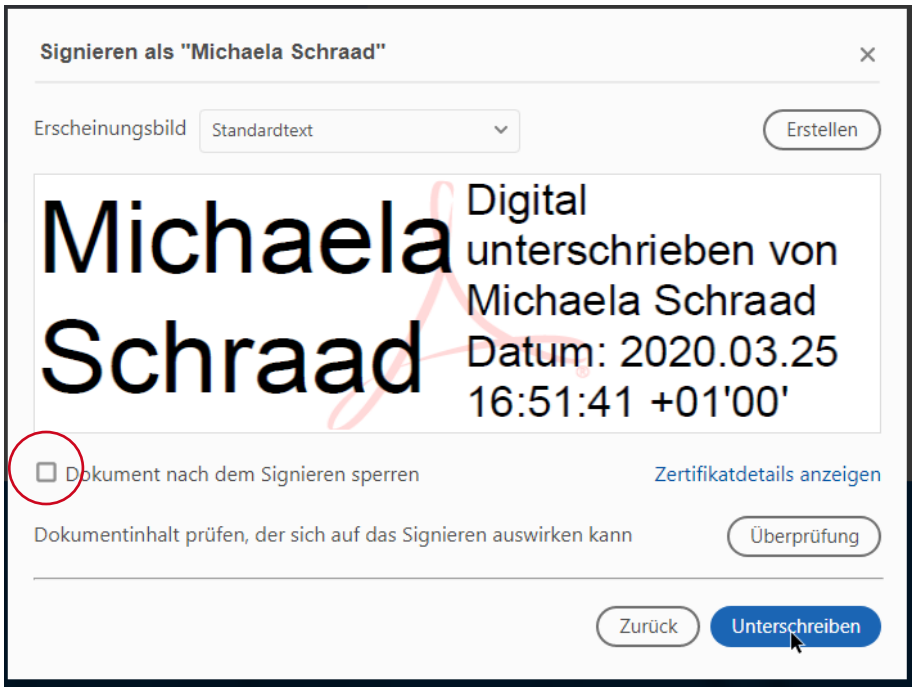


Abbildung 57: Dokument nicht sperren

7 Elektronische Unterschrift prüfen

Haben Sie die Konfiguration für die Prüfung von elektronischen Unterschriften bereits vorgenommen, können Sie direkt zu Kapitel **7.3 Unterschrift prüfen**, S. **43** springen.

7.1 Voraussetzungen

Um eine durch die DFN-PKI ausgestellte fortgeschrittene elektronischen Signatur eines PDF-Dokumentes validieren zu können, müssen folgende Voraussetzungen erfüllt sein:

a. Die Sicherheitseinstellungen im Adobe Reader DC wurden vorgenommen. (Kapitel **3 Sicherheitseinstellungen**, S. **6**)
b. Das verwendete Zertifikatskette der DFN-PKI ist konfiguriert. (Kapitel **4 Stammzertifikat konfigurieren**, S. **14**)

7.2 Konfiguration

Bitte konfigurieren Sie zur Prüfung von elektronischen Unterschriften Ihren Acrobat Reader DC sorgfältig. Dazu Klicken Sie bitte im Dialogfenster „Einstellungen“ unter dem Navigationspunkt „Unterschriften“ im Bereich „Überprüfung“ auf den Button „Weitere“.

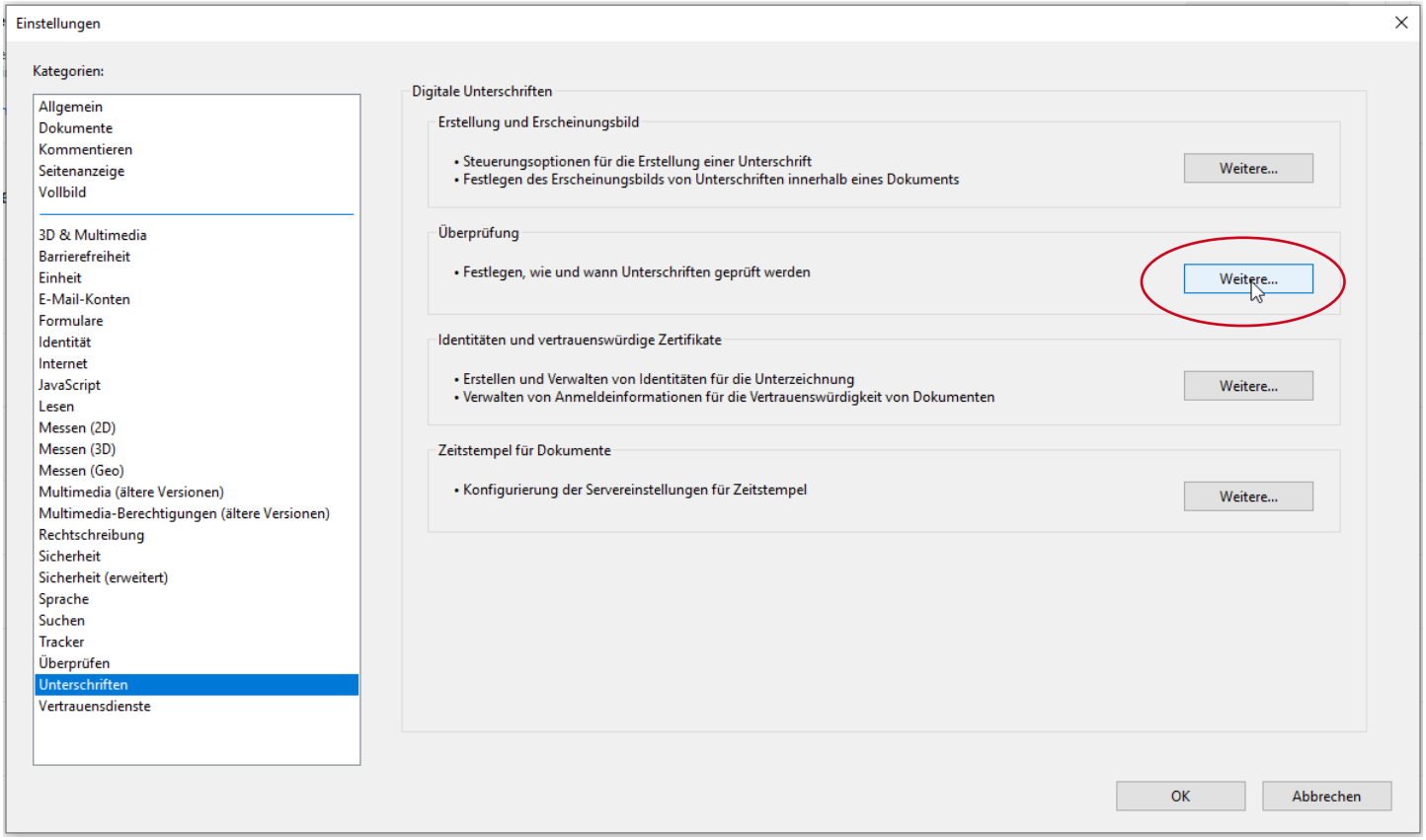


Abbildung 58: Konfiguration zur Überprüfung von Unterschriften

Es öffnet sich das Dialogmenü „Voreinstellungen für das Prüfen von Unterschriften“. Bitte ändern Sie im Bereich „Zeitpunkt der Überprüfung“ die Prüfkriterien um in „In Signatur eingebettete Zeit (Zeitstempel) sichern“.

Es wird nicht empfohlen Zertifikate aus dem Windows-Zertifikatsspeicher zu verwenden. Deaktivieren Sie daher im Bereich „Windows-Integration“ das Überprüfen von zertifizierten Dokumenten“.

Bestätigen Sie die Konfiguration mit „OK“.

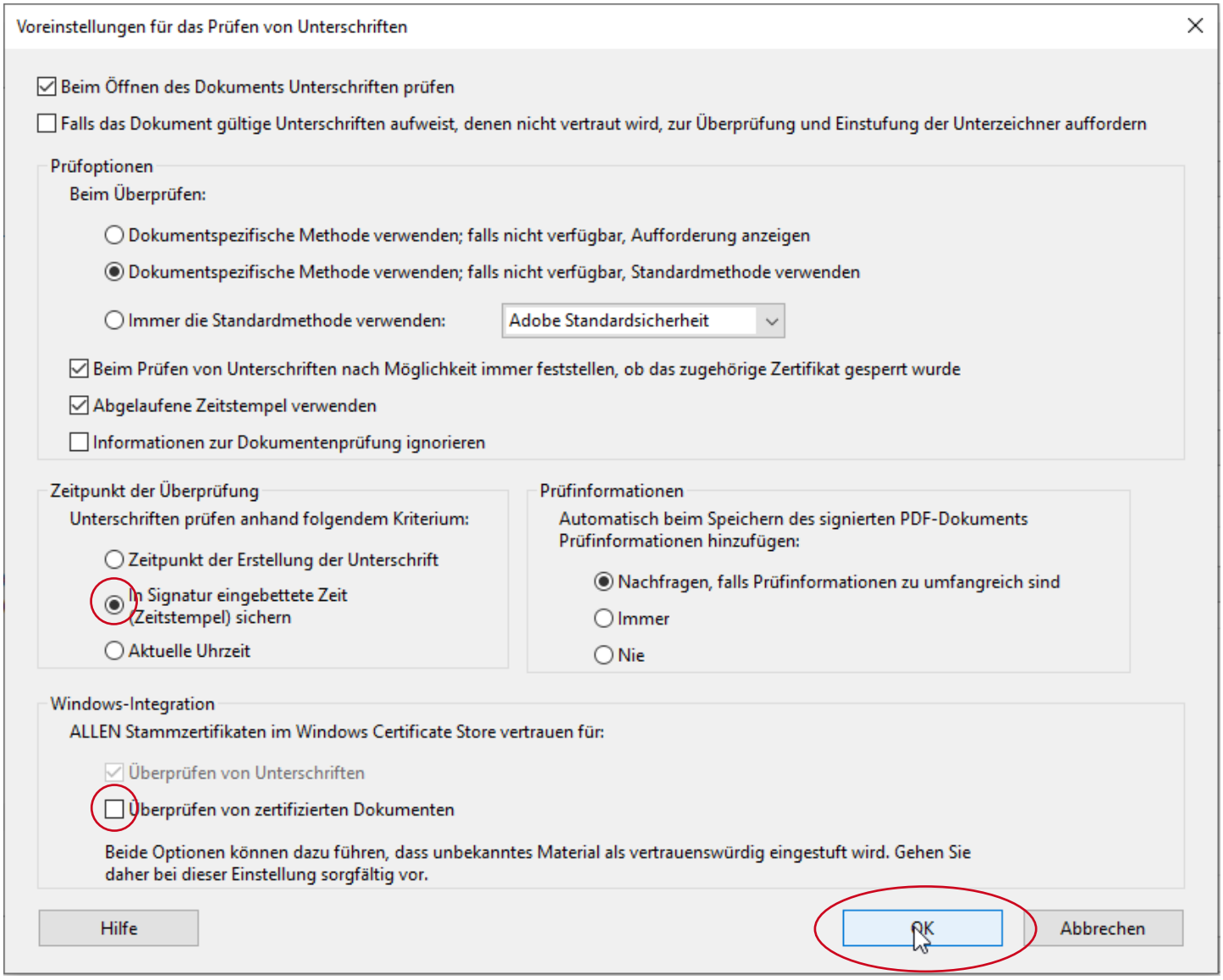


Abbildung 59: Windows-Integration deaktivieren (i)

Da die Deaktivierung beider Checkboxen nicht gleichzeitig möglich ist, öffnen Sie bitte das Dialogfenster für die Voreinstellungen zur Unterschriftenüberprüfung erneut über Klick auf „Weitere“ im Bereich „Überprüfung“ unter dem Navigationspunkt „Unterschriften“.

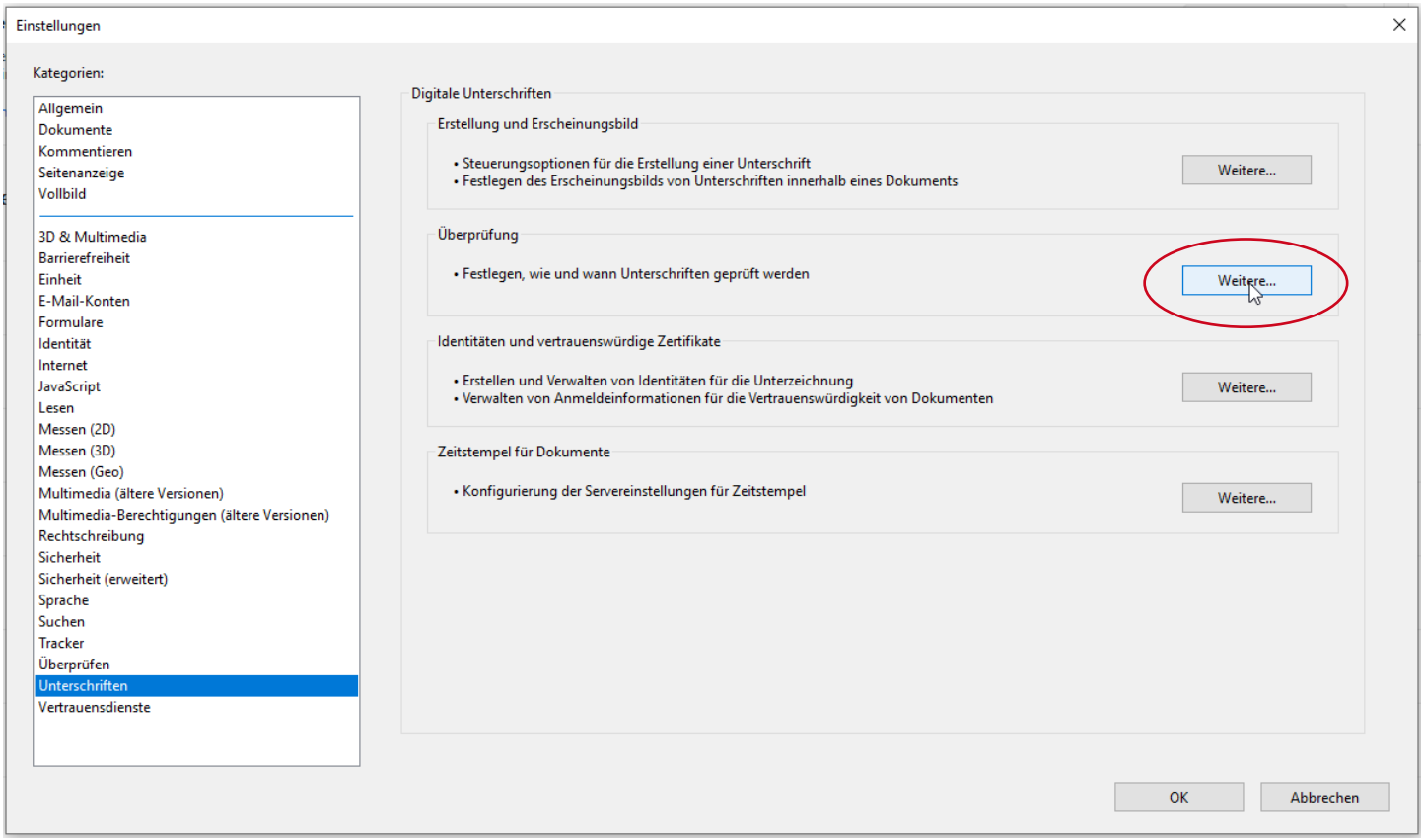


Abbildung 60: Menü zur Unterschriftenüberprüfung erneut öffnen

Bitte stellen Sie sicher, dass beide Checkboxen im Bereich „Windows-Integration“ deaktiviert sind und bestätigen Sie die Konfiguration mit OK.

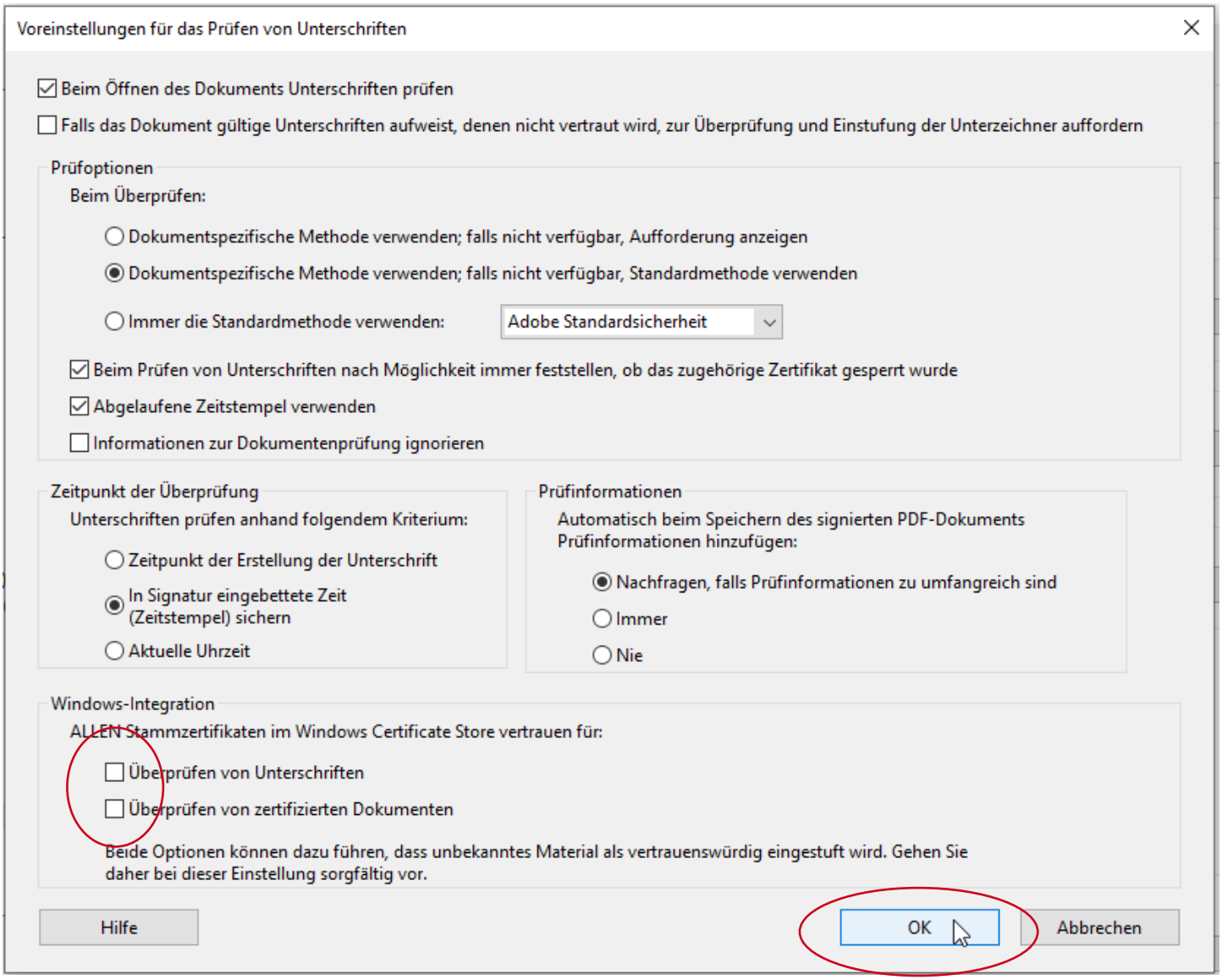


Abbildung 61: Windows-Integration deaktivieren (ii)

Sollten Sie dennoch vertrauenswürdige Zertifikate aus Ihrem Windowszertifikatspeicher verwenden wollen, exportieren Sie diese und importieren sie vergleichbar dem T-TeleSec Global Root2-Zertifikat. (vgl. Kapitel **4 Stammzertifikat konfigurieren**, S. **14**).

7.3 Unterschrift prüfen

Öffnen Sie ein elektronisch unterschriebenes PDF-Dokument im Acrobat Reader DC. Wird Ihnen in der Statusleiste die Meldung „Unterschrieben und alle Unterschriften sind gültig“ angezeigt, sind alle elektronischen Unterschriften im Dokument gültig.

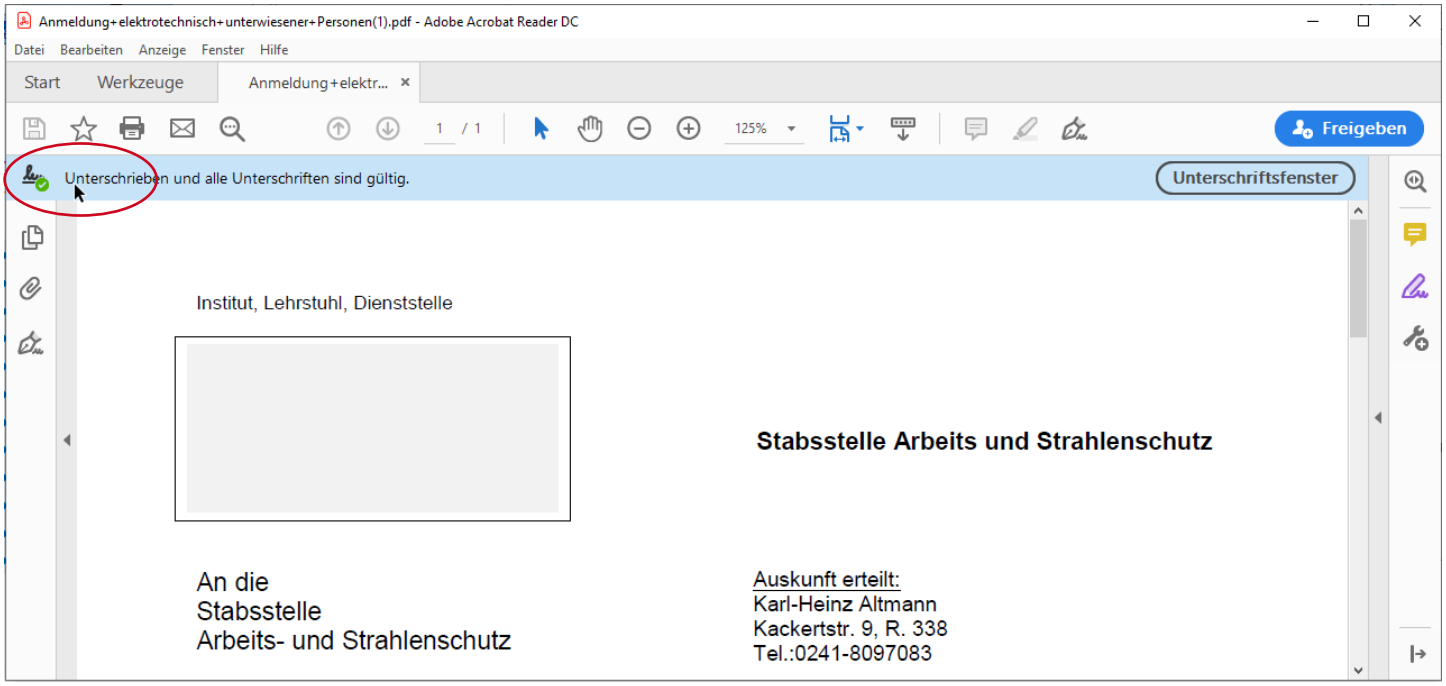


Abbildung 62: Elektronische Unterschrift in Adobe prüfen

Wenn Sie die Details der elektronischen Unterschriften prüfen möchten, haben Sie verschiedene Möglichkeiten. Sie können durch Klick auf den Button „Unterschriftenfenster“ die Listenansicht aller elektronischen Unterschriften des Dokumentes öffnen.

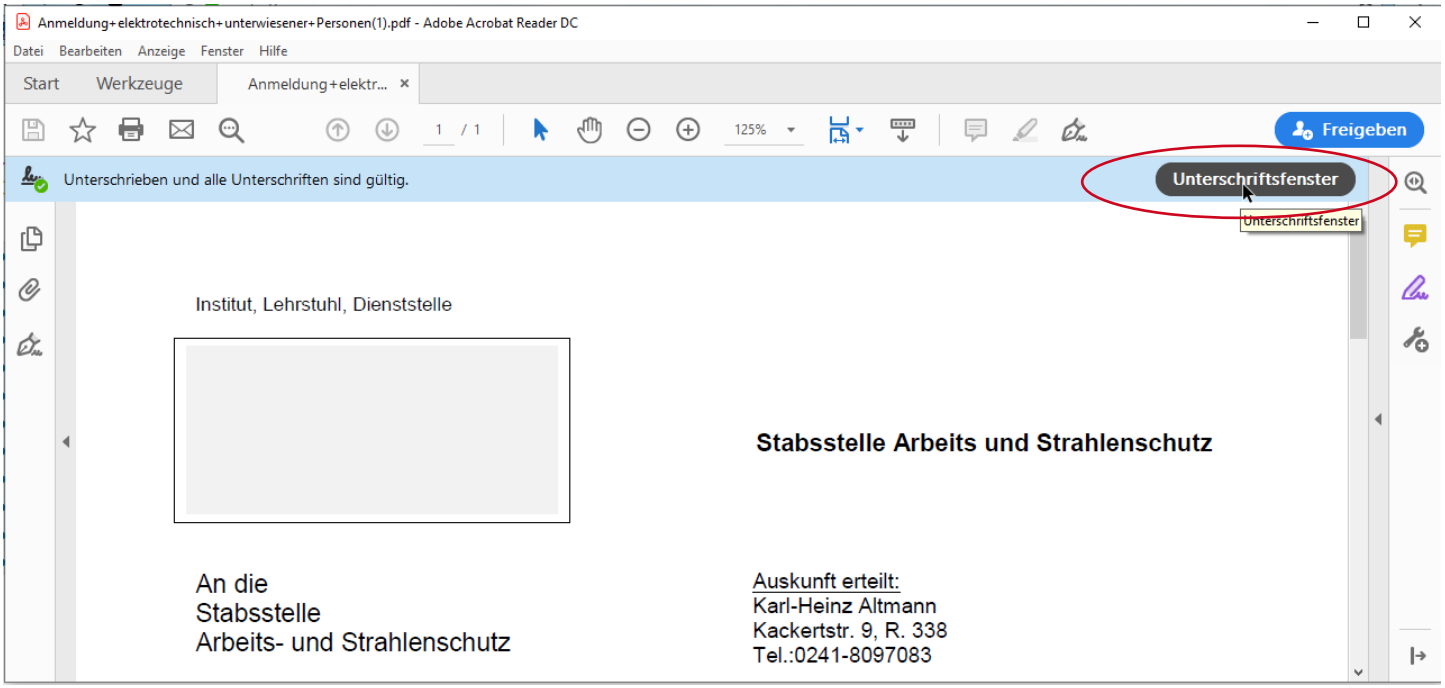


Abbildung 63: Unterschriftsfenster öffnen

Klicken Sie auf eine elektronische Unterschrift, springt die Dokumentenanzeige an die entsprechende Stelle im Dokument.

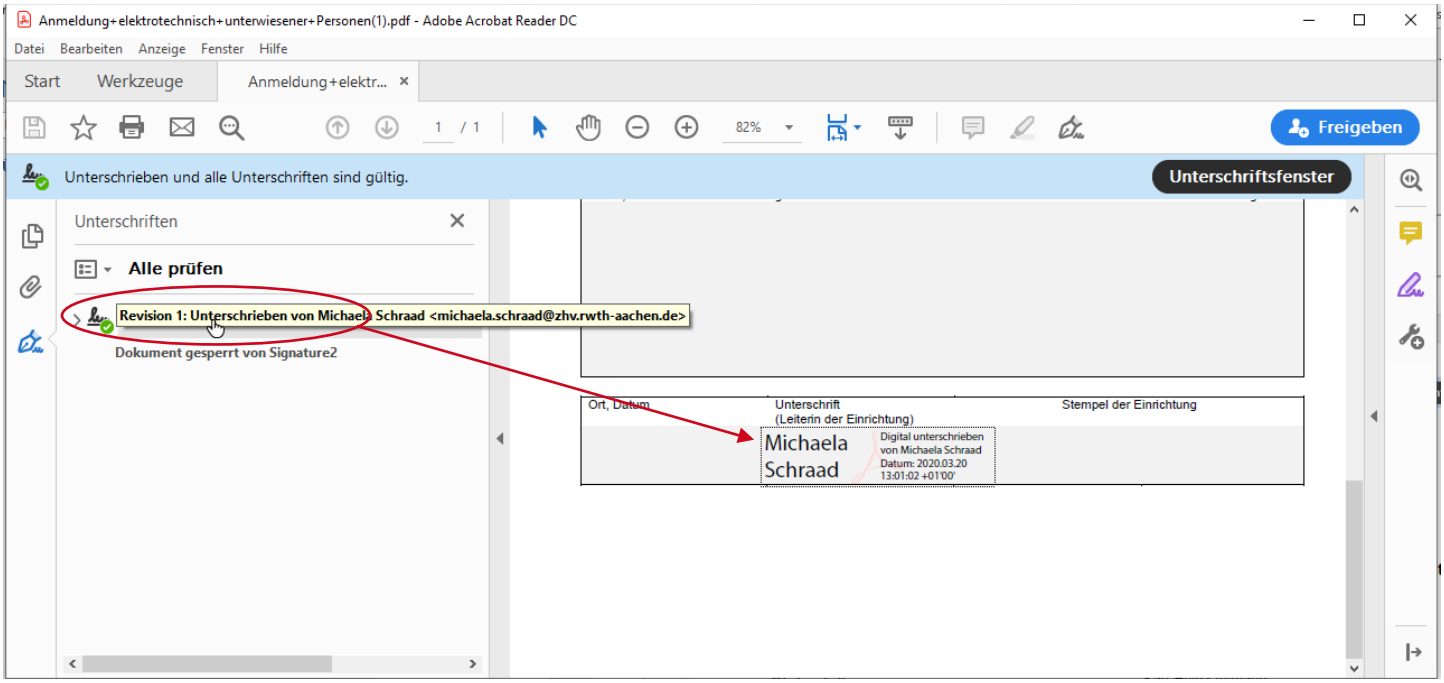


Abbildung 64: Elektronische Unterschrift prüfen

Im Dokument selber können Sie auf die elektronische Unterschrift klicken um die Gültigkeit der Unterschrift zu prüfen.

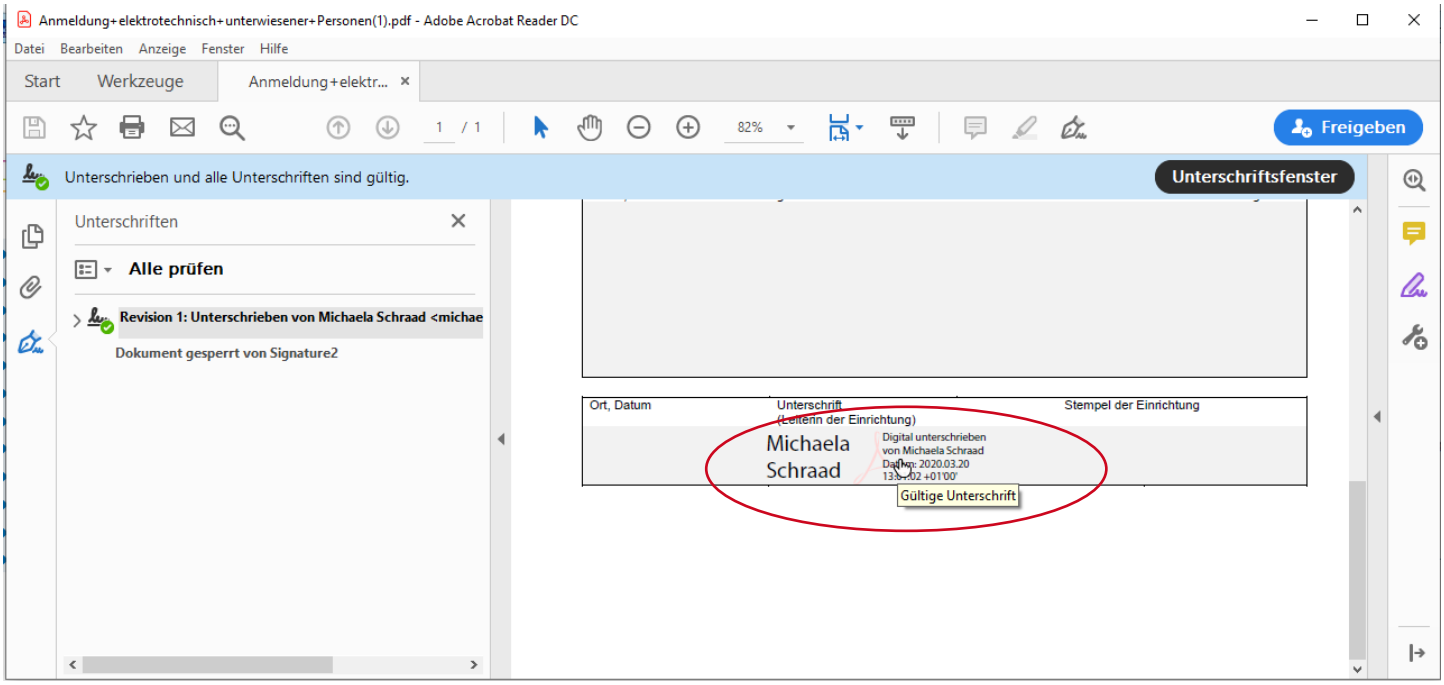


Abbildung 65: Elektronische Unterschrift anzeigen

Beim Klick auf die Unterschrift öffnet sich das Dialogfenster „Unterschriftenvalidierungsstatus“. Mit einem Klick auf den Button „Unterschrifteneigenschaften“, können Sie weitere Prüfdetails zum unterschriebenen Dokument einsehen.

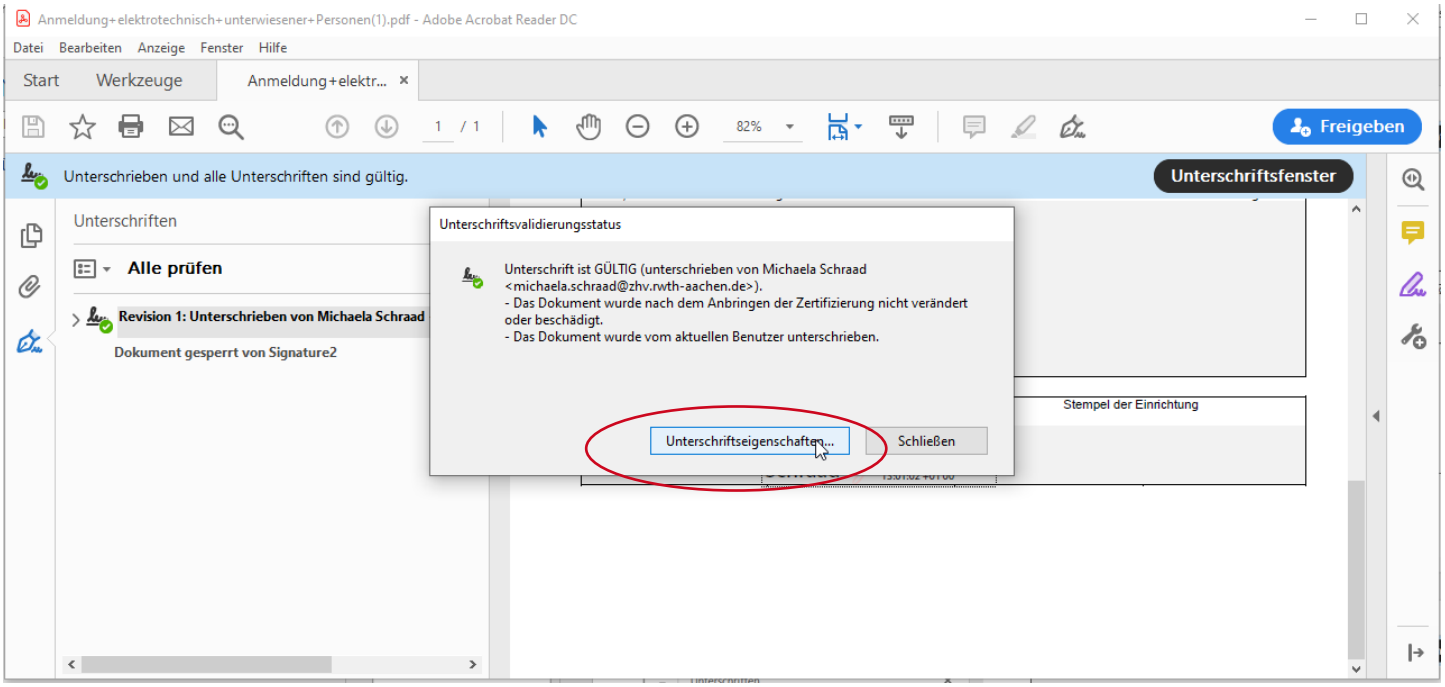


Abbildung 66: Statusanzeige elektronische Unterschrift

Es werden Ihnen in einem weiteren Dialogfenster Informationen zur Gültigkeit und Validierung angezeigt. Sie können durch Klick auf „Zertifikat des Ausstellers anzeigen“ auch die Zertifikatseigenschaften wie z. B. Gültigkeitszeitraum oder auch den Zeitstempel prüfen.

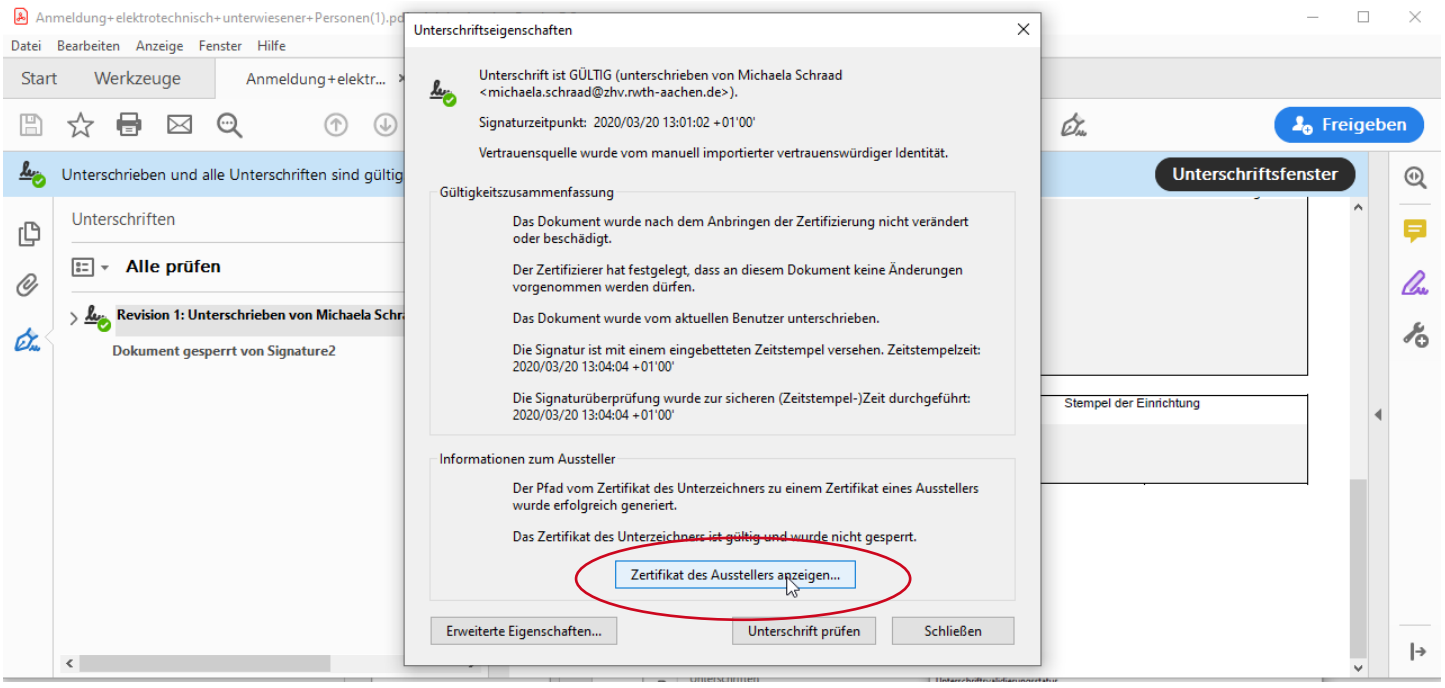


Abbildung 67: Nutzerzertifikat des Unterschreibendens anzeigen

Die Zertifikatsanzeige enthält verschiedene Module. Es gibt die Möglichkeit sich über die verschiedenen Reiter weitere Details für das Nutzerzertifikat und alle weiteren Zertifikate aus der Zertifikatskette anzeigen zu lassen.

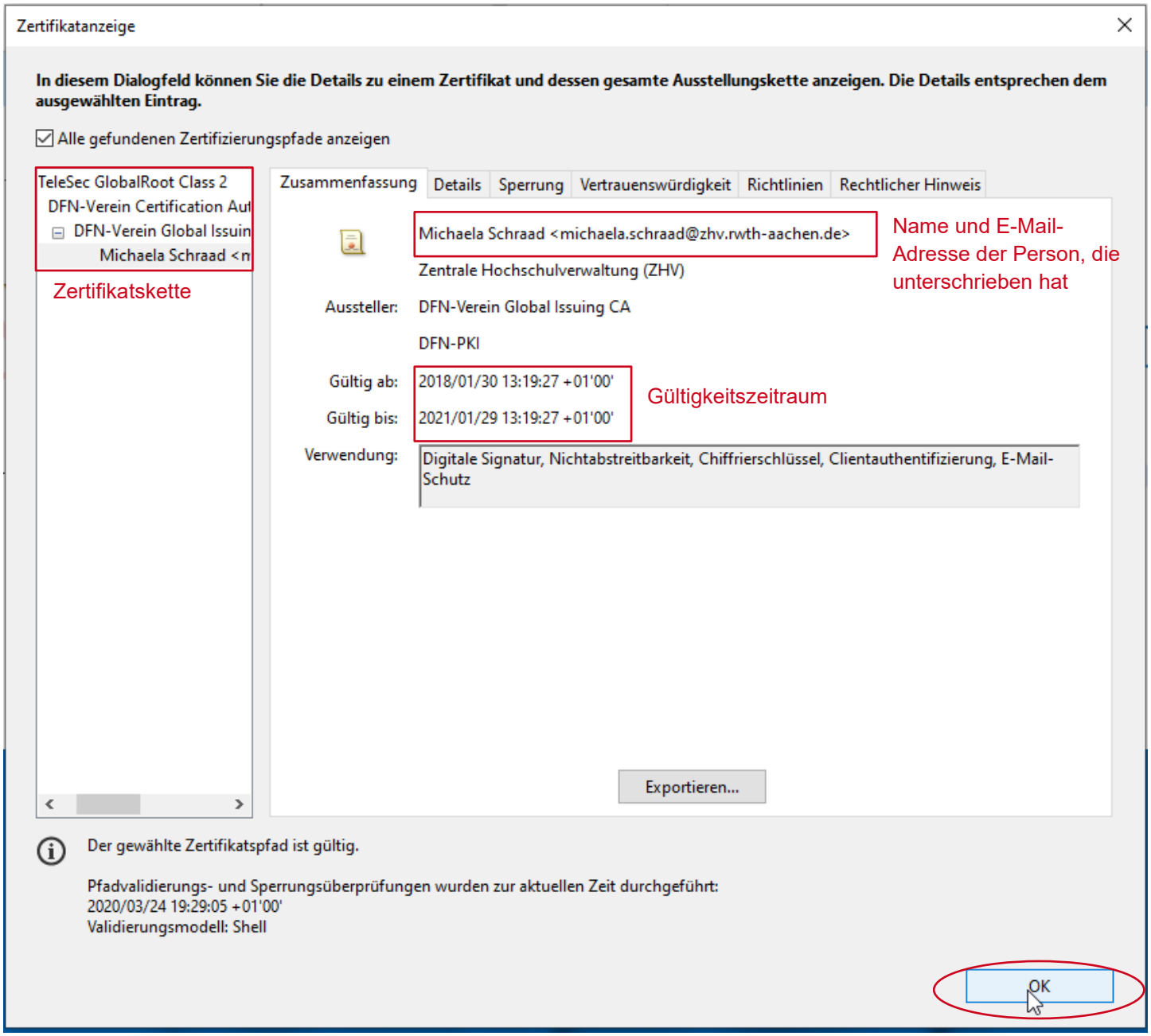


Abbildung 68: Zusammenfassung der Nutzerzertifikatdaten

Öffnen Sie das Unterschriftenfenster über Klick auf das Unterschriften-Icon in der Werkzeugleiste.

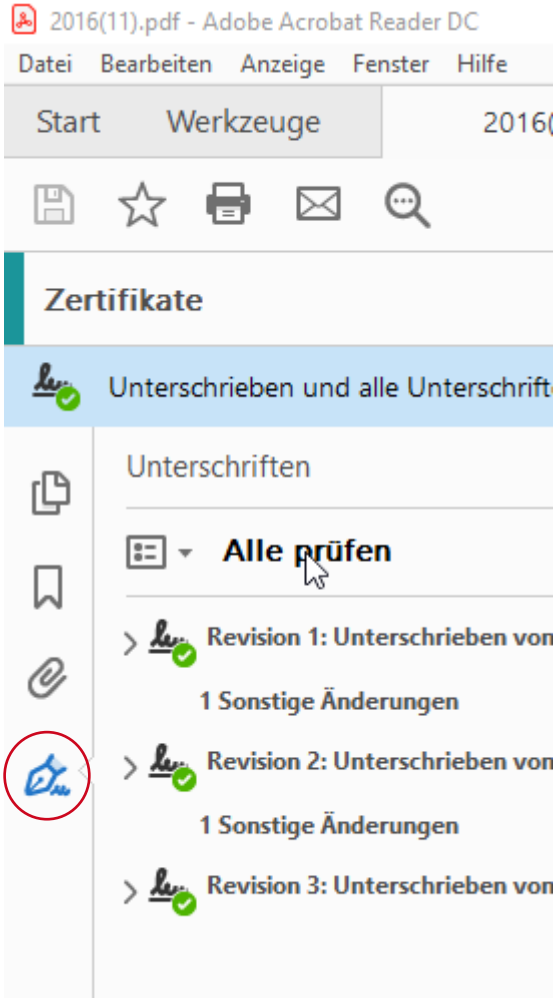


Abbildung 69: Unterschriftenfenster öffnen

Bei mehreren elektronischen Unterschriften im Dokument können Sie den Validierungsprozess auch für alle elektronischen Unterschriften gleichzeitig starten, indem Sie auf den Button „Alle prüfen“ klicken.

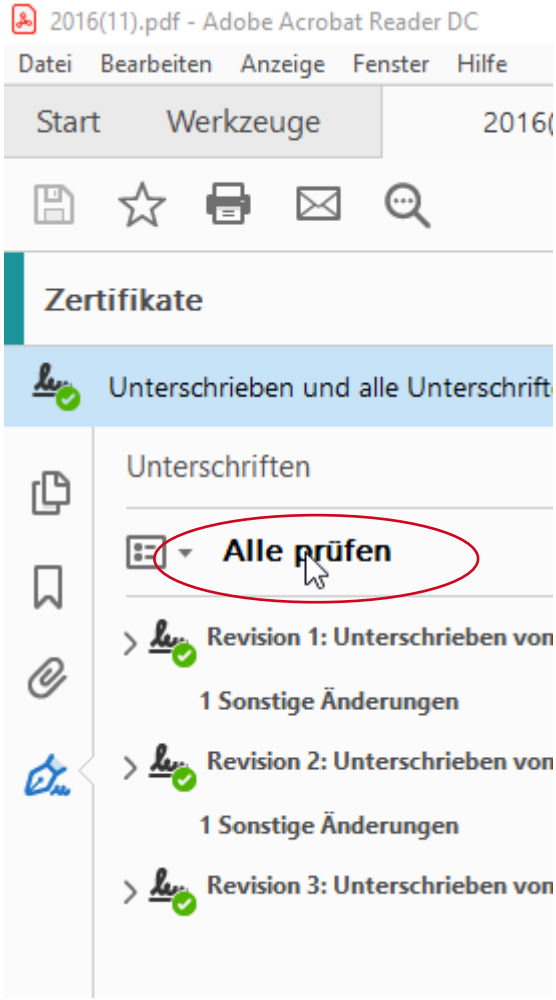


Abbildung 70: Beispiel für mehrere elektronische Unterschriften in einem Dokument

Bei der gleichzeitigen Prüfung aller Unterschriften bekommen Sie ein Meldungsfenster angezeigt. Über die Checkbox können Sie dieses für zukünftige Prüfungen deaktivieren.

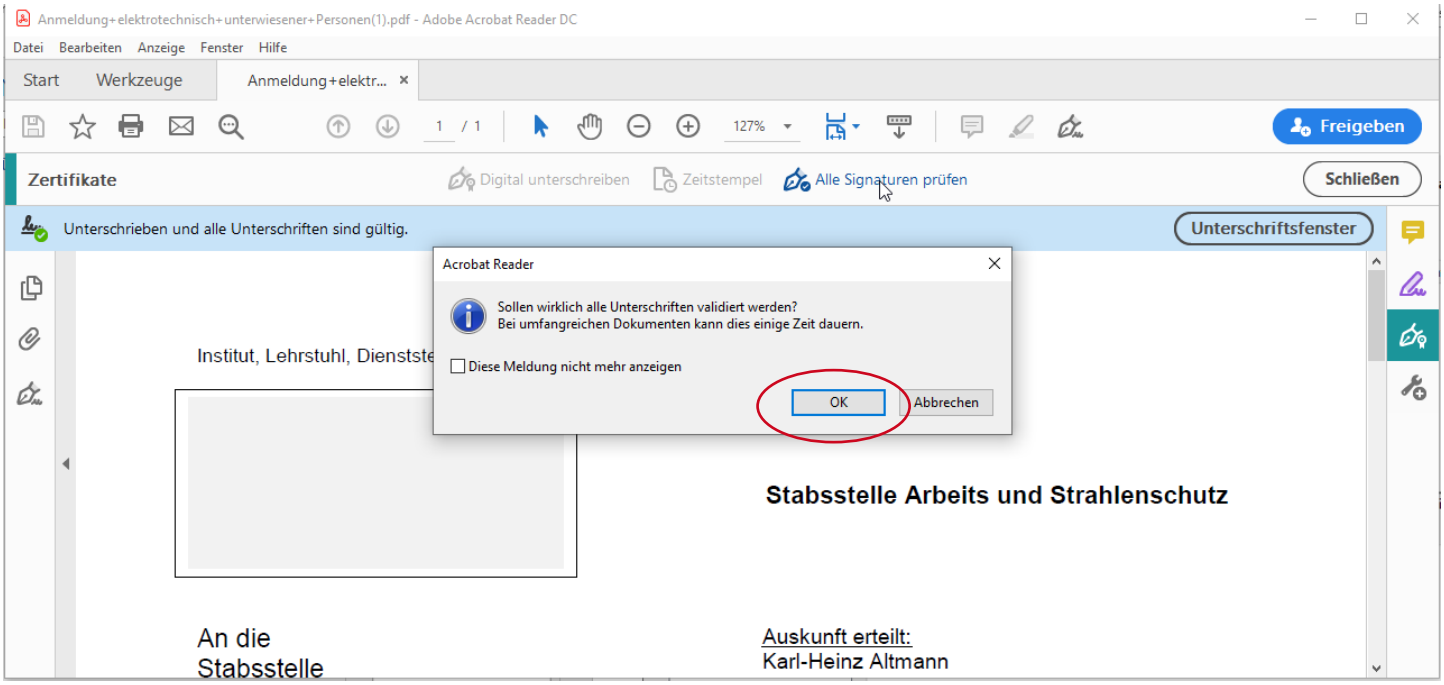


Abbildung 71: Prüfung aller elektronischen Unterschriften durchführen

Bitte bestätigen Sie die durchgeführte Validierung mit OK.

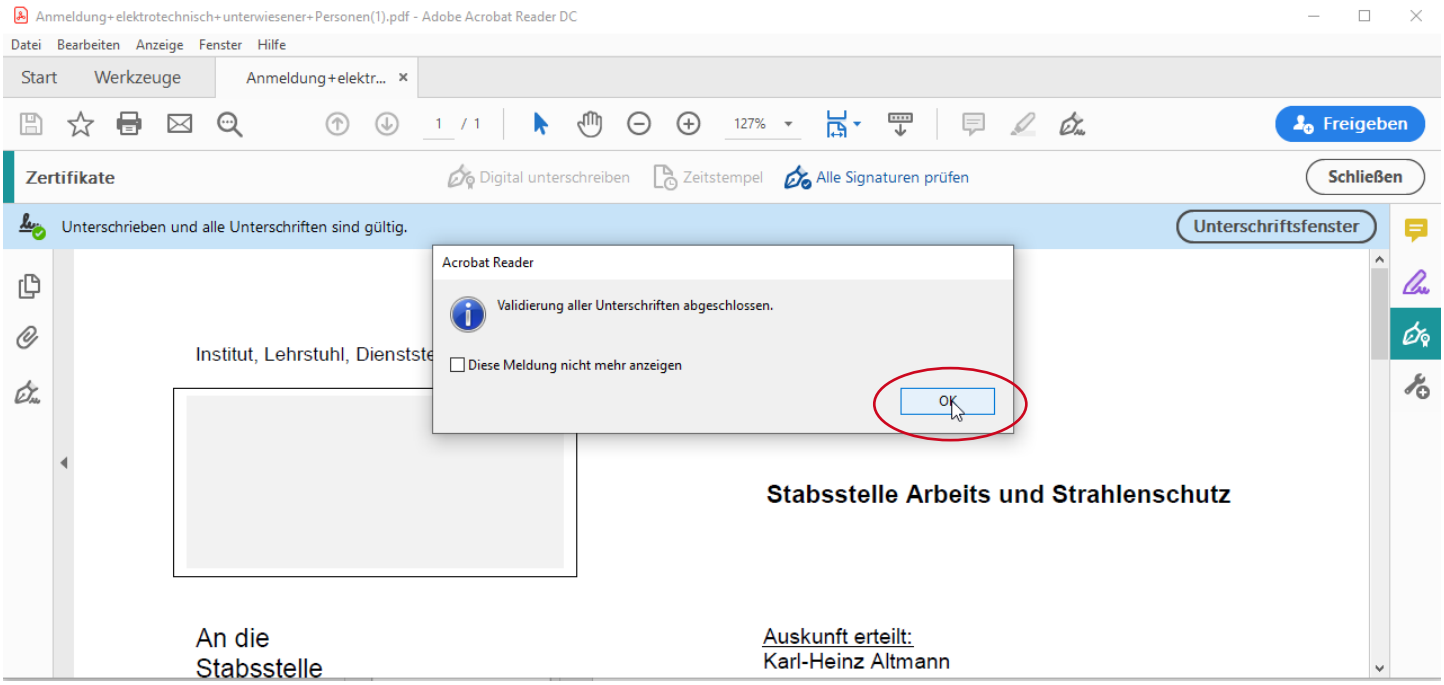


Abbildung 72: Prüfung aller elektronischen Unterschriften abgeschlossen

Wird bei der Überprüfung der Unterschriften die Meldung „Es gibt bei mindestens einer Unterschrift Probleme“, kann es bspw. daran liegen, dass das Zertifikat der digitalen ID mit der unterschrieben bzw. signiert wurde inzwischen abgelaufen ist.

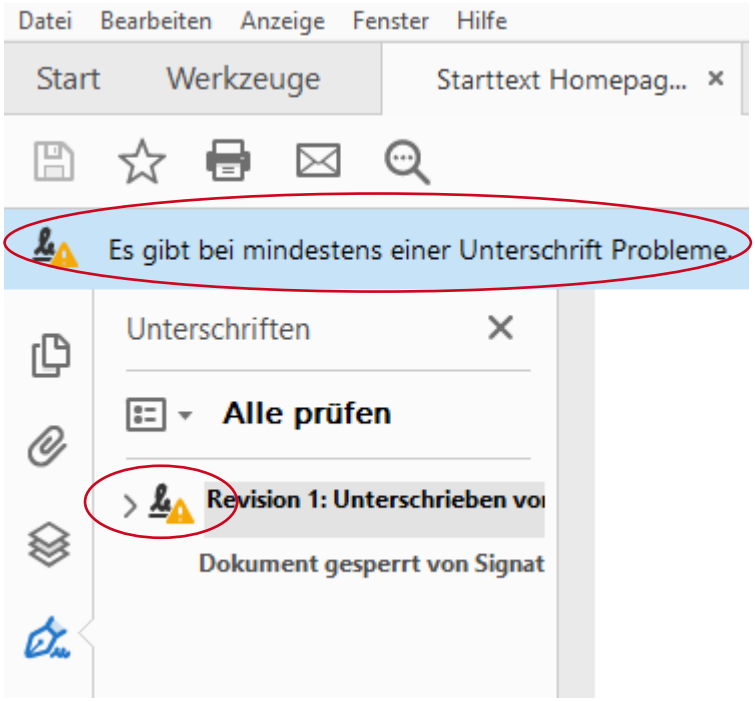


Abbildung 73: Anzeige eines abgelaufenen Zertifikats

7.4 Prüfergebnis

Abhängig von den beim Unterschreiben des Dokumentes vorgenommenen Einstellungen, bestätigt die gültige Unterschrift folgende Sachverhalte. (vgl. Schritt aus **Abbildung 67: Nutzerzertifikat des Unterschreibendens anzeigen**)

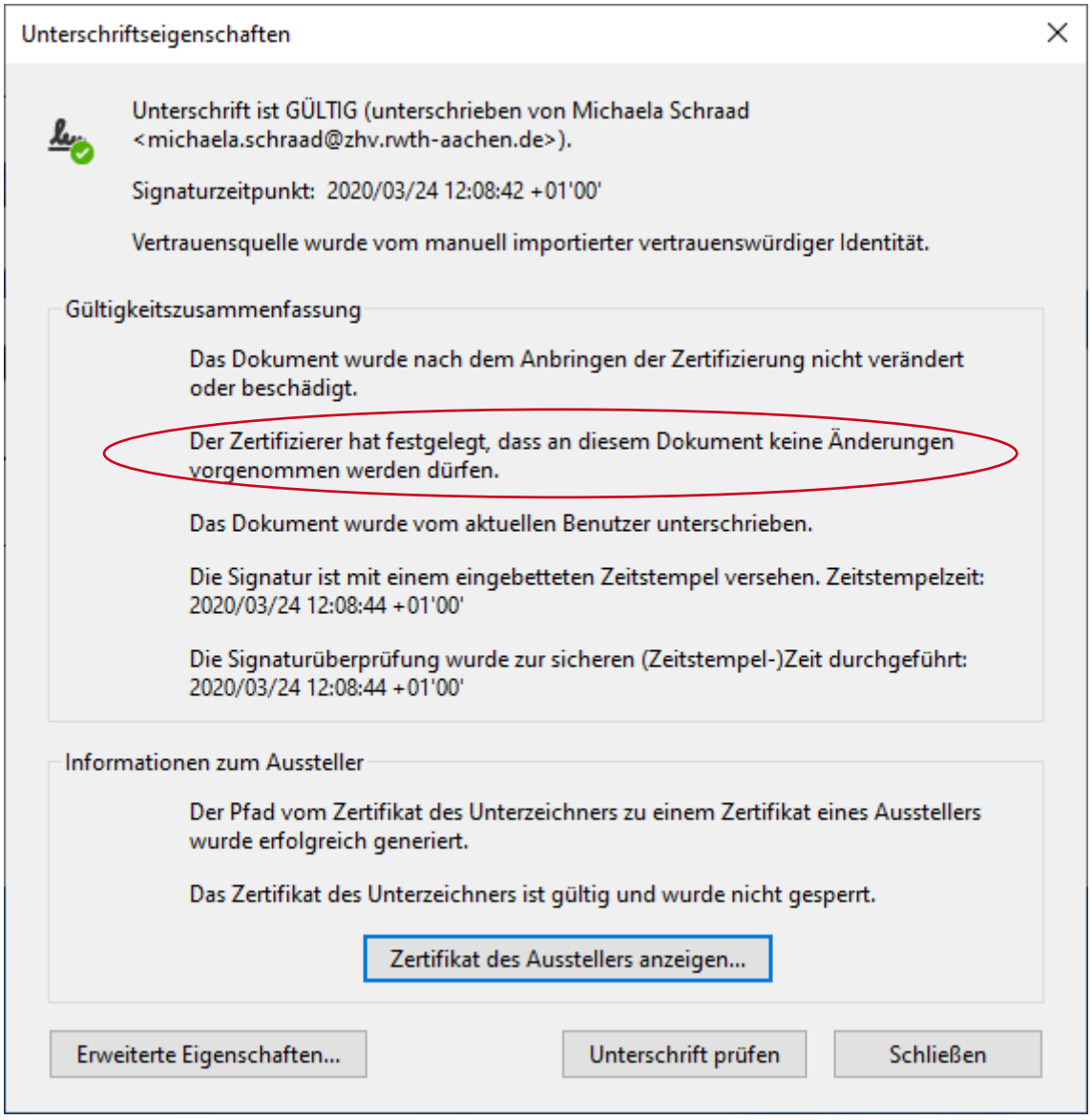


Abbildung 74: Unterschriftseigenschaften bei nach der Unterschrift gesperrten Dokumenten

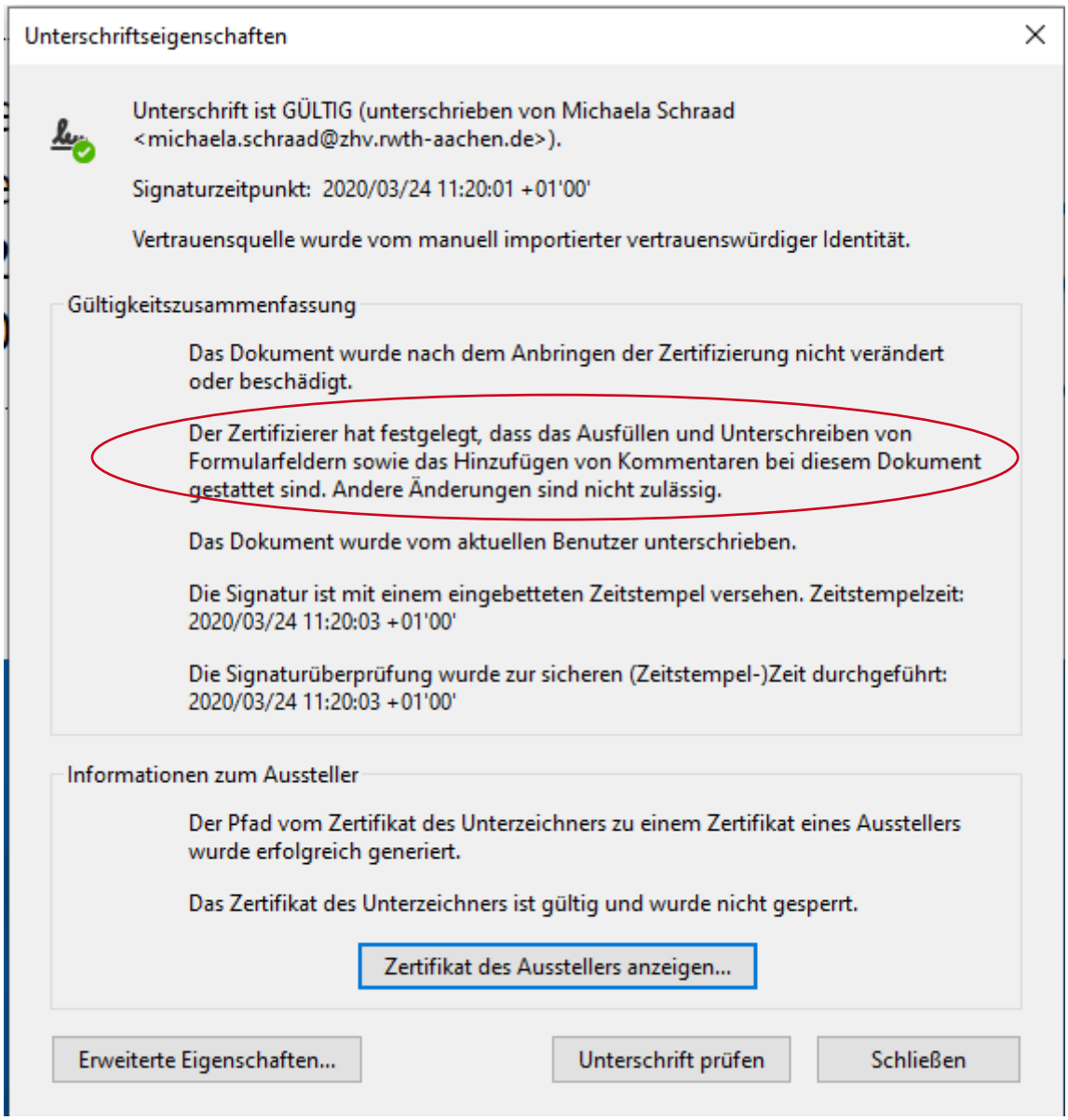


Abbildung 75: Unterschrifteneigenschaften bei unterschriebenen nicht gesperrten Dokumenten

Die Authentizität des eingebundenen Zeitstempeldienstes, können Sie durch Klick auf „Erweiterte Eigenschaften“ im vorangegangenen Fenster prüfen. Erfolgte die elektronische Unterschrift unter Nutzung des DFN-Zeitstempeldienstes, wird Ihnen die Zusammenfassung des zugehörigen Zertifikates angezeigt.

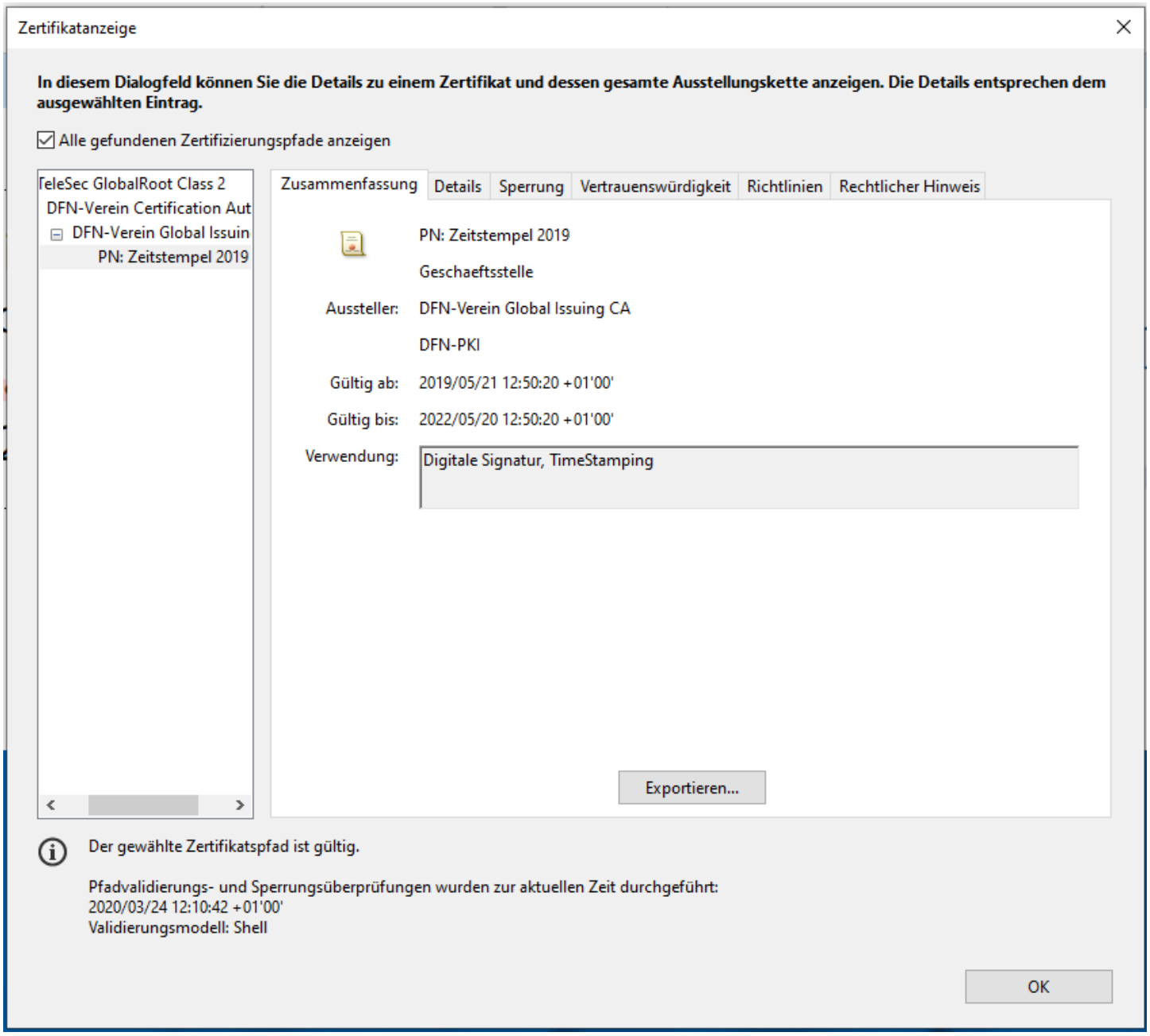


Abbildung 76: Zertifikatsanzeige Zeitstempel

7.5 Prüfbeispiel

An Hand der folgenden elektronischen Unterschrift können Sie den Prüfvorgang an diesem Dokument ausprobieren:

Michaela Schraad

Digital unterschrieben von Michaela Schraad
Datum: 2023.04.27 13:51:51 +02'00'

8 Weitere Informationen

Weitere Informationen zum RWTH-DFN-Zertifizierungsportal finden Sie im Dokumentationsportal des IT Centers unter **https://www.rwth-aachen.de/zertifikate**.

Erläuterungen und Informationen zur Konfiguration finden Sie auf den Hilfe-Webseiten von Adobe unter **https://helpx.adobe.com/de/acrobat/user-guide.html**

Informationen zur Nutzung der elektronischen Unterschrift im RWTH-internen Geschäftsverkehr finden Sie im Intranet unter **https://www.rwth-aachen.de/eUnterschrift** .

9 Abbildungsverzeichnis

Impressum
RWTH | Konfiguration einer elektronischen Unterschrift | 27.04.2023

RWTH Aachen University, Dezernat 5.0 – Organisation und IT

Autorin: Michaela Schraad

Mitwirkende:
Ekaterini Papachristou
Katrin Zeumann

Deckblattfoto: Martin Braun