WWU
MÜNSTER

Wirtschafts-
wissenschaftliche
Fakultät

Informationsverarbeitungs-
Versorgungseinheit (IVV)
Wirtschaftswissenschaften

Zertifizierung von PDF-Dokumenten: Digitales Unterschreiben

Alina Zimmer, Walter Schmitting
IVV2
Universitätsstr. 14-16
D-48143 Münster

Version: 2.0
Datum: 25.03.2020

Inhalt

Dokumentenhistorie

Version	Datum	Änderung	Autor
1.0	2017-03-08	Ersterstellung	Zimmer, Alina
2.0	2020-03-25	Vollständige Überarbeitung	Schmitting, Walter

Es sei darauf hingewiesen, dass auch die WWU IT (ehemals ZIV) eine Dokumentation zu diesem Thema vorhält: https://www.uni-muenster.de/WWUCA/de/howto-setup-acroread.html

1. Einleitung

Zuweilen ist es für den Empfänger einer PDF-Datei wünschenswert, sich der Tatsache zu versichern, dass die Datei genauso vorliegt, wie sie vom Autor erstellt wurde und keinerlei nachträgliche Änderungen durch Dritte vorgenommen wurden. Gleichzeitig soll der Autor nachvollziehbar identifiziert werden. Erforderlich ist mithin eine „digitale Unterschrift".

Zu diesem Zweck kann die PDF-Datei elektronisch „signiert" werden: Die sichtbare Signatur (welche hier durch ein Zertifikat repräsentiert und authentifiziert wird), wird – sofern passend eingestellt - zerstört, sobald ein Dritter eine Änderung am Dokument vornimmt. Für die Signatur der PDF-Datei kann dabei das persönliche Nutzerzertifikat (siehe dazu die Dokumentation „Nutzerzertifikat beantragen und einrichten") eingesetzt werden, mit welchem an der WWU auch Mails signiert und verschlüsselt werden können.

Im Folgenden wird unterstellt, dass der Autor, welcher eine PDF-Datei entsprechend signieren möchte, über ein solches persönliches Nutzerzertifikat verfügt. In dieser Dokumentation wird das „Unterschreiben" (Signieren) einer PDF-Datei unter Verwendung der Software Adobe Acrobat Pro Dc beschrieben. Für andere Versionen der Software oder andere Softwareprodukte kann sich das Vorgehen unterscheiden.

Die Dokumentation erläutert zunächst den (einmalig vorab notwendigen) Import eines Zertifikats (Abschnitt 2), des Weiteren die einmalig unter Adobe Acrobat vorzunehmenden Einstellungen zu digitalen Unterschriften (Abschnitt 3). Sie geht dann auf den Vorgang des digitalen Unterschreibens selbst ein (Abschnitt 4) und stellt abschließend dar, wie man eine vorliegende digitale Signatur eines Dritten überprüft (Abschnitt 5).

2. Zertifikat importieren

Im ersten Schritt muss das vorhandene Zertifikat (einmalig) in die Software Adobe Acrobat importiert werden. Dies wird folgend erläutert.

In der Menüleiste der Software wird das Drop-Down Menü „Bearbeiten" ausgewählt. Man klickt den Punkt „Einstellungen" an. Es öffnet sich das Fenster mit dem Titel „Einstellungen" (siehe Abb. 1). Dort wird links die Kategorie „Unterschriften" ausgewählt.

Auf der rechten Seite kann nun über Buttons in verschiedene Unterkategorien gewechselt werden. Hier klickt man unter dem Punkt „Identitäten und vertrauenswürdige Zertifikate" auf den Button „Weitere…".

Ein neues Fenster mit dem Titel „Einstellungen für digitale IDs und vertrauenswürdige Zertifikate" öffnet sich (siehe Abb. 2). In der Baumdarstellung links sollte „Digitale IDs" schon ausgewählt sein. Sofern hier schon das zu verwendende Zertifikat des Benutzers, ausgestellt vom DFN-Verein, angezeigt wird, sind keine weiteren Aktivitäten erforderlich.

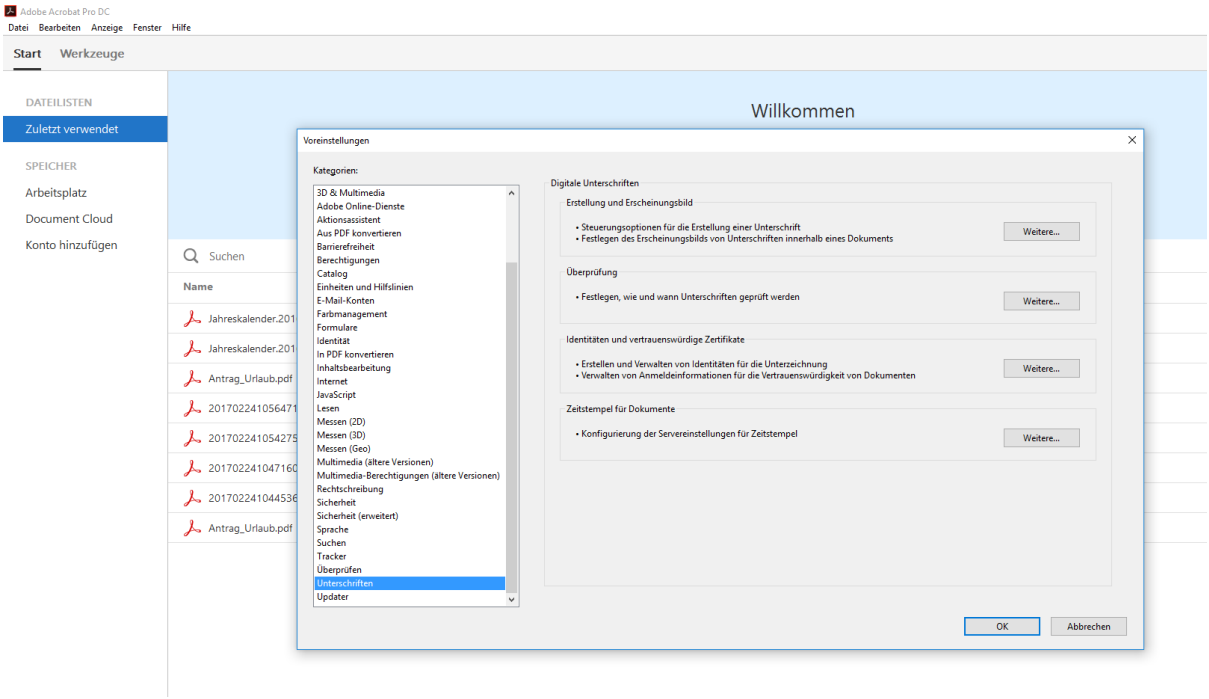

Abb. 1: Adobe Acrobat – Einstellungen für Digitale Unterschriften

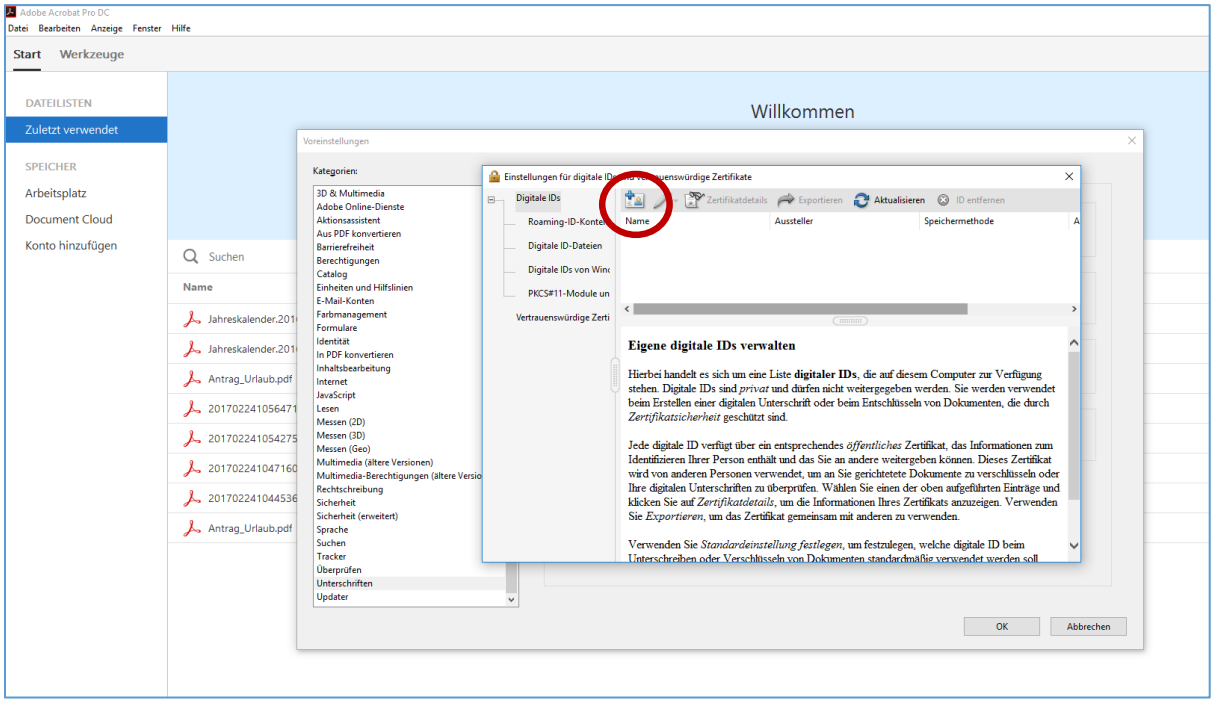

Abb. 2: Einstellungen für digitale IDs und vertrauenswürdige Zertifikate

Falls dies nicht der Fall ist, muss das Zertifikat wie nachstehend beschrieben importiert werden. Im oberen rechten Teil des Fensters ist eine Iconleiste zu sehen. Ganz links findet sich ein Icon mit einer stilisierten Visitenkarte und einem blauen Plus. Auf dieses Icon ist zu klicken.

Daraufhin öffnet sich das Fenster „Digitale ID hinzufügen“ (siehe Abb. 3). Die Voreinstellung in dem Fenster bleibt ausgewählt: Die eigene digitale ID soll aus einer Datei (*.p12 oder *.pfx) hinzugefügt werden.

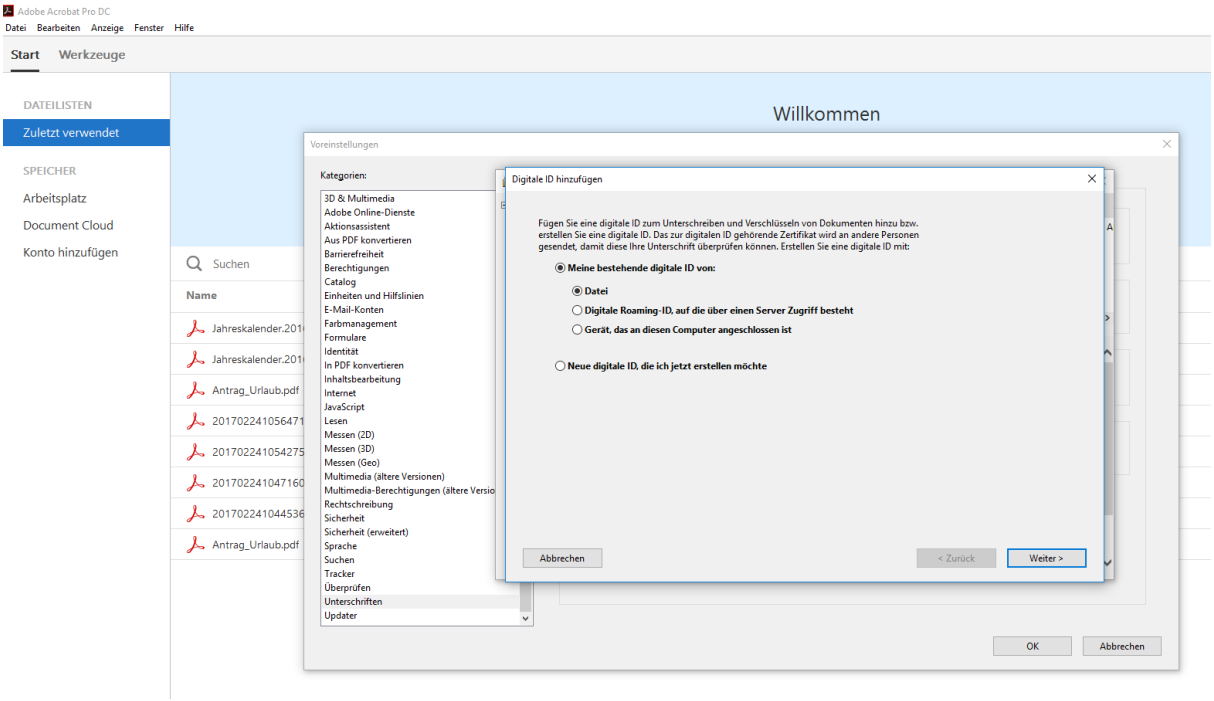

Abb. 3: Fenster „Digitale ID hinzufügen“, Auswahl Vorgehensweise

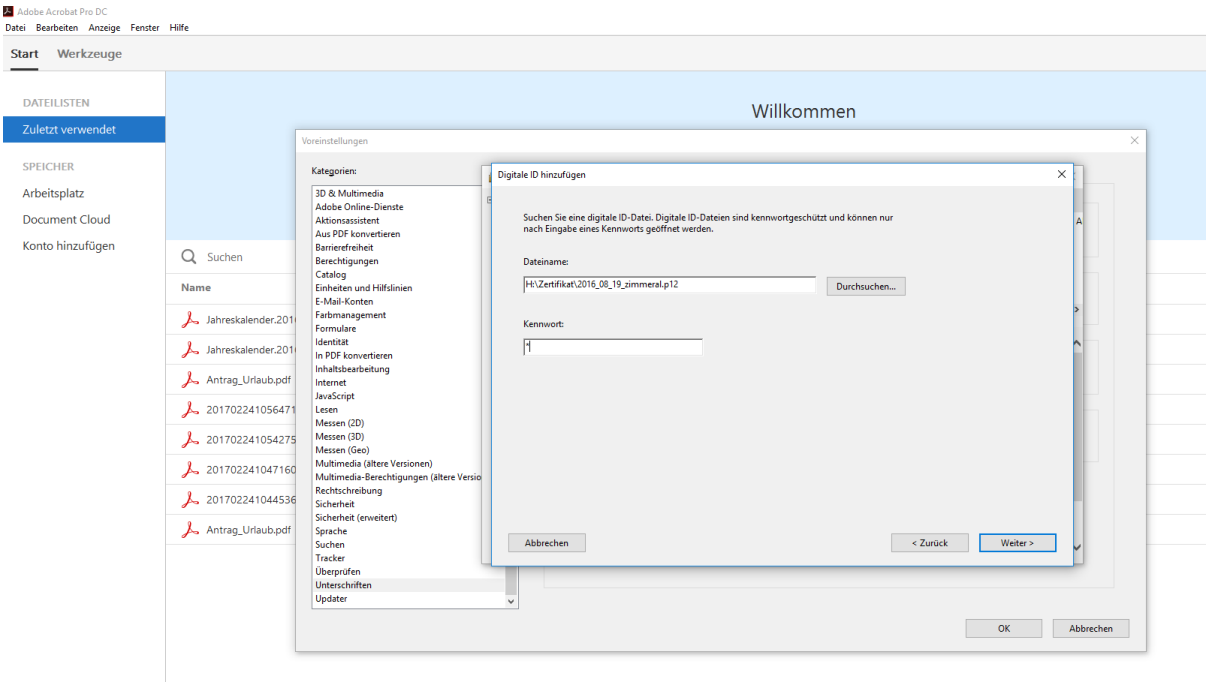

Abb. 4: Fenster „Digitale ID hinzufügen“, Eingabe Dateipfad und Passwort

Im nächsten Schritt wählt man den Dateipfad aus, unter dem man sein Zertifikat gespeichert hat, und gibt das dazugehörige Passwort für sein Zertifikat ein (siehe Abb. 4).

Danach wählt man aus der Liste der importieren digitalen IDs die gewünschte aus und klickt auf „Fertig stellen“. Nachdem der Importvorgang mit einem Klick auf „Fertig stellen“ bestätigt wurde, schließt sich das Fenster. Man gelangt wieder zu dem Fenster „Einstellungen für digitale IDs und vertrauenswürdige Zertifikate“ (siehe Abb. 5). Nun sollte in der Liste das gewünschte Zertifikat vorhanden sein.

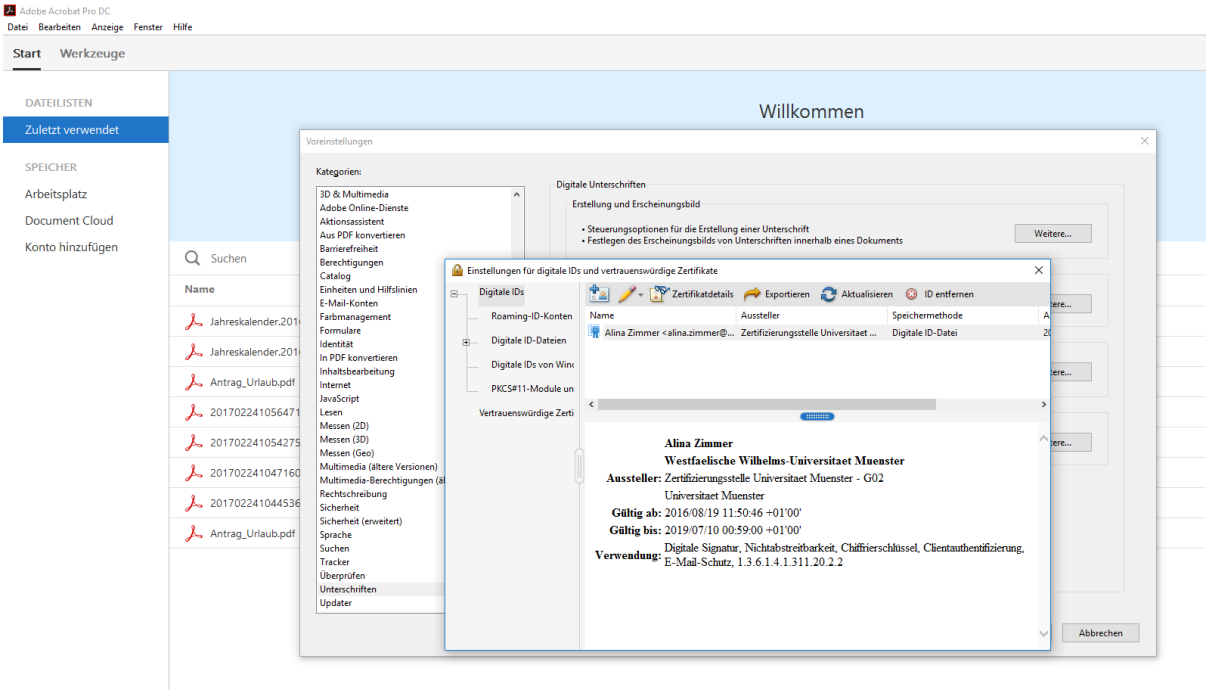

Abb. 5: Liste der eingefügten Digitalen IDs

3. Einstellungen von Adobe Acrobat anpassen

Im zweiten Schritt ist es sinnvoll, die Einstellungen von Adobe Acrobat an den hier erläuterten Zertifikatseinsatz anzupassen. Dies wird folgend beschrieben.

In der Menüleiste der Software wird das Drop-Down Menü „Bearbeiten“ ausgewählt. Man klickt den Punkt „Einstellungen“ an. Es öffnet sich das Fenster mit dem Titel „Einstellungen“. Dort wird links die Kategorie „Unterschriften“ ausgewählt. Die Einstellungen für digitale Unterschriften werden angezeigt (siehe Abb. 1).

Es werden die Einstellungen für die spätere Überprüfung von Signaturen bzw. digitalen Unterschriften angepasst. Dafür wird der Button „Weitere“ hinter dem Thema „Überprüfung“ angeklickt. Es öffnet sich das neue Fenster „Voreinstellungen für das Prüfen von Unterschriften“. Die Einstellungen sollten nun wie in Abb. 6 angegeben gewählt werden.

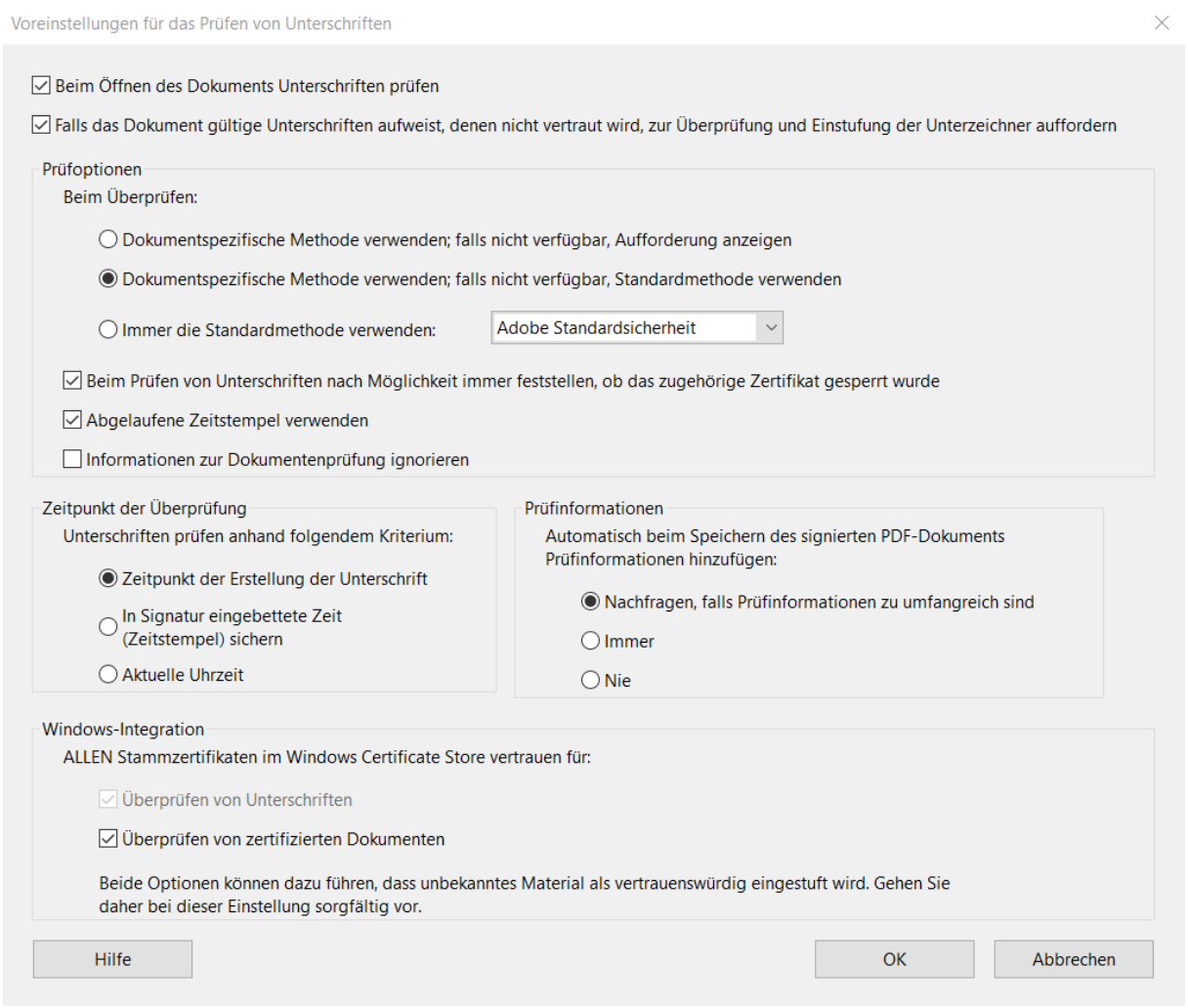

Abb. 6: Einstellungen für die Überprüfung digitaler Unterschriften

4. Ein Dokument mit dem Zertifikat unterschreiben

Man öffnet das gewünschte PDF-Dokument in Adobe Acrobat. Danach wählt man den Reiter „ Werkzeuge“ im Ribbon aus. In dem Auswahlmenü klickt man auf „Zertifikate“ (siehe Abb. 7).

Dort gibt es verschiedene Unterschriftsmöglichkeiten. Um das PDF-Dokument sichtbar zu zertifizieren, wählt man unter den in der Kopfzeile angezeigten Optionen „Digital unterschreiben“ oder „Zertifizieren (sichtbare Unterschrift)“ aus. Folgend wird „Digital unterschreiben“ gewählt. Nach der Auswahl durch Anklicken öffnet sich ein Pop-Up-Fenster, in dem verlangt wird, ein neues Unterschriftsrechteck durch Ziehen zu erstellen (siehe Abb. 8). In dem Unterschriftsrechteck wird später die zertifizierte Unterschrift platziert.

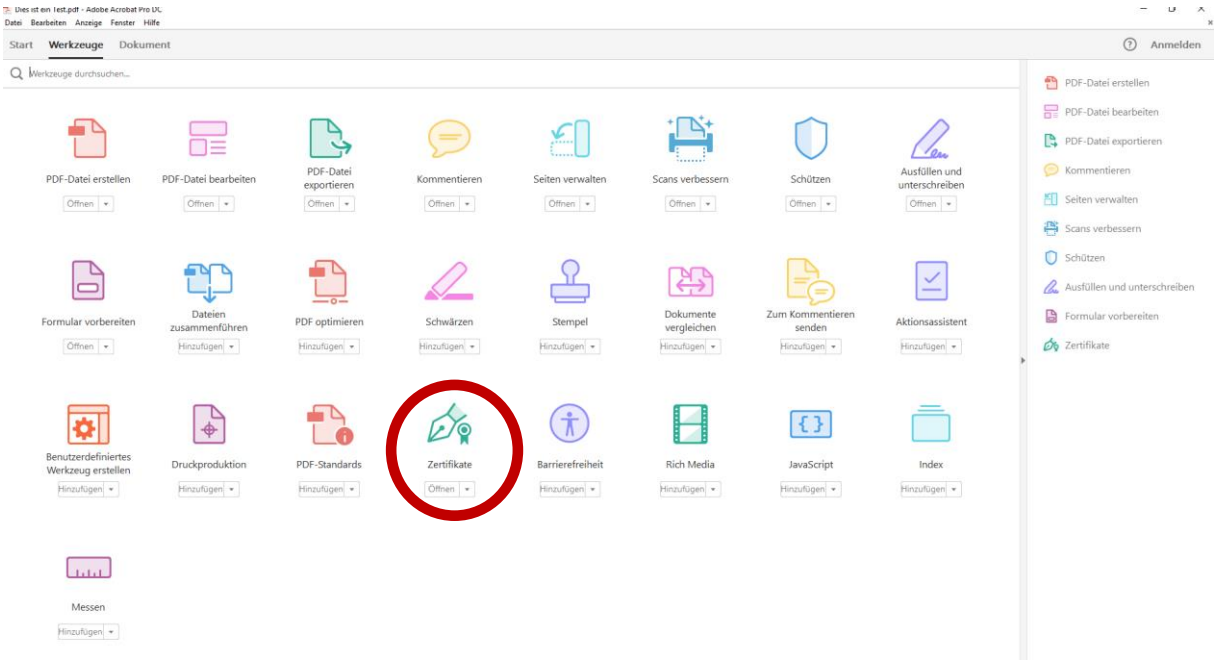

Abb. 7: Reiter Werkzeuge

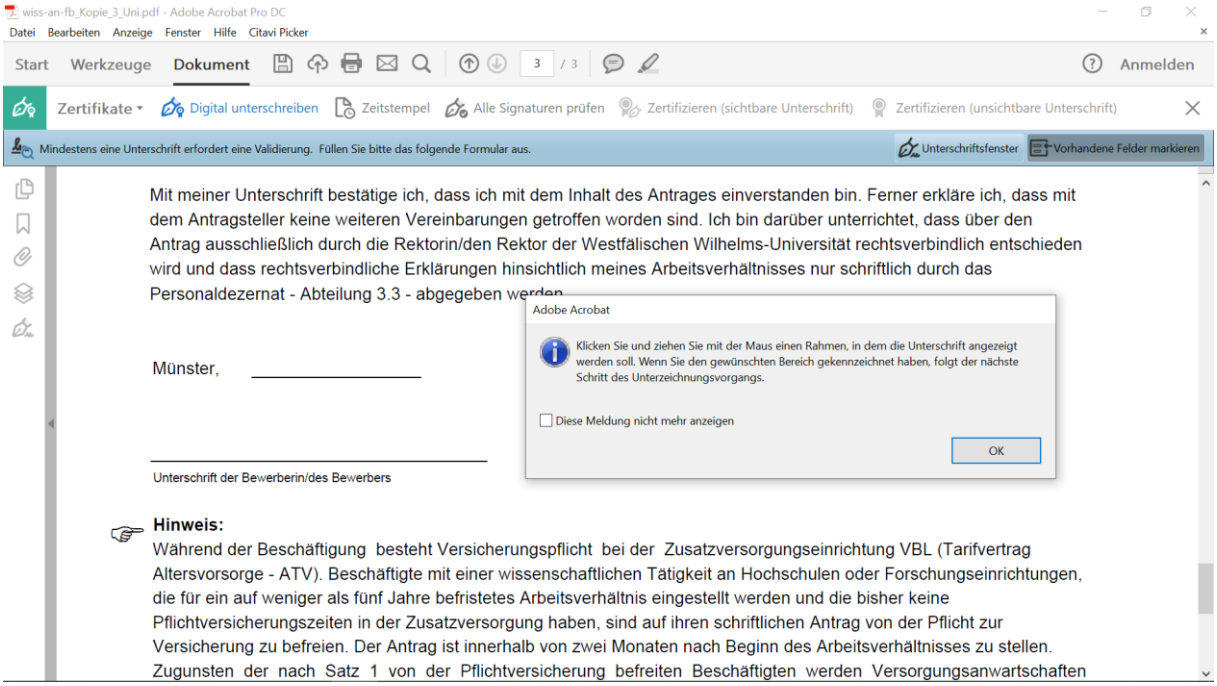

Abb. 8: Pop-Up-Fenster Unterschriftsrechteck

Nach dem Aufziehen des Rechtecks für die Unterschrift (an der richtigen Stelle im Dokument …) öffnet sich ein weiteres Pop-Up-Fenster (siehe Abb. 9). Dies bietet zum einen eine Vorschau auf die digitale Unterschrift, welche eingefügt werden soll. Über das Drop-Down-Menü hinter „Erscheinungsbild“ kann man, sofern gewünscht, auch noch die Ansicht der Signatur verändern. So ist es bei Wahl von „Neues Erscheinungsbild erstellen …“ im Drop-Down möglich, die Ansicht in einem neuen Fenster in etlichen Punkten anzupassen, z.B. ein Bild einer tatsächlichen Unterschrift zu integrieren. Des Weite-

ren kann man hier, sofern man über mehrere Zertifikate zur Signierung verfügt, aus diesen wählen. Schließlich kann man das Dokument noch für Änderungen nach der Unterschrift sperren, indem man einen Haken setzt. Ob dies sinnvoll ist, hängt vom speziellen Anwendungskontext ab. Danach sind keine Änderungen am Dokument mehr möglich; erzwingt man diese, so verliert die digitale Unterschrift automatisch ihre Gültigkeit.

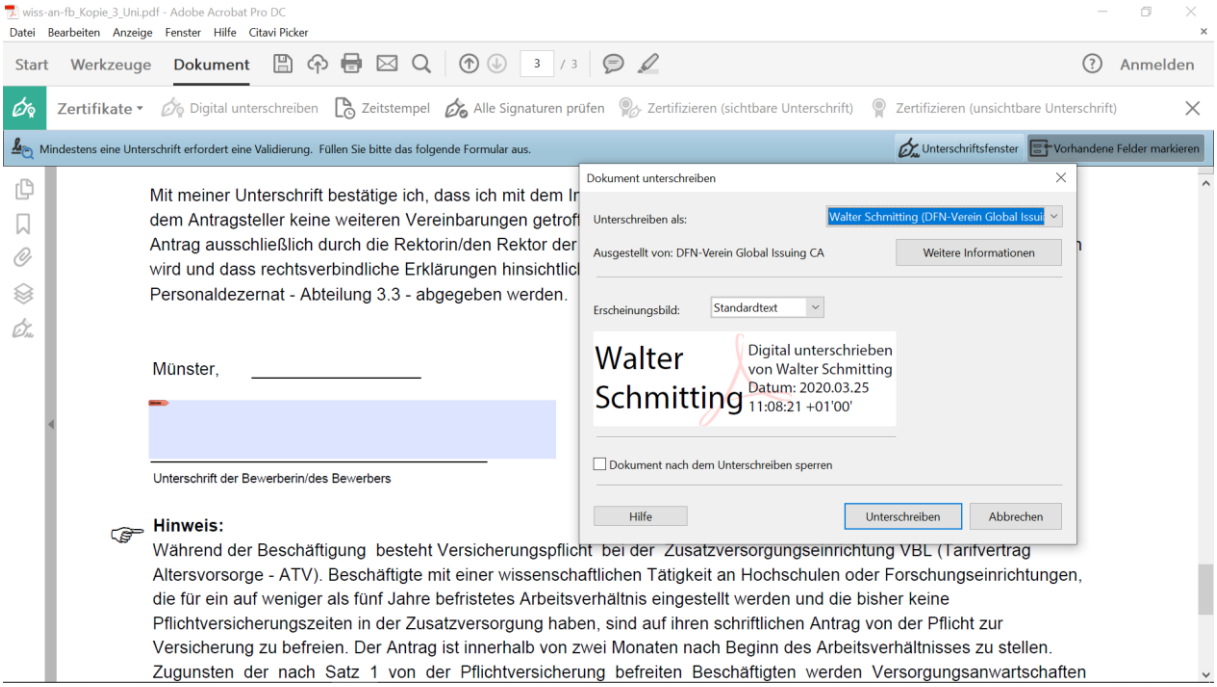

Abb. 9: Pop Up-Fenster Zertifikatsauswahl, Dokumentensperrung

Klickt man nun auf den Button „Unterschreiben“ (siehe Abb. 9), so wird die digitale Unterschrift eingefügt. Direkt danach öffnet sich eine Dateiauswahlbox: Nun muss die PDF-Datei unter einem neuen Namen gespeichert werden. Direkt danach wird man – in Abhängigkeit vom gesetzten Sicherheitsniveau – ggf. noch gefragt, ob man diese Verwendung des Zertifikats zulassen möchte. Die Abfrage ist leider etwas missverständlich – unter dem Titel „Anmeldeinformationen erforderlich“ wird gefragt, ob man der App Zugriff auf den eigenen privaten Schlüssel gewähren möchte. Um die digitale Unterschrift erfolgreich abzuschließen, ist hier auf „Zulassen“ zu klicken. Danach ist der Vorgang abgeschlossen. Die beiden Dokumente (das signierte und das nicht signierte Dokument) können nun geschlossen werden.

5. Gültigkeit einer Signierung überprüfen

Sofern ein Anwender eine signierte bzw. mit einer „digitalen Unterschrift“ versehene PDF-Datei erhält, kann (und sollte) er prüfen, ob die Unterschrift gültig ist. Man nennt dies auch eine „Validierung“. Damit wird ggf. (sofern so parametrisiert) auch ersichtlich, ob nach der „digitalen Unterschrift“ Änderungen am Dokument vorgenommen wurden.

Je nach Voreinstellung von Adobe Acrobat wird man beim Öffnen eines signierten bzw. „digital unterschriebenen“ Dokuments schon beim Öffnen dazu aufgefordert, die Unterschrift zu überprüfen (siehe Abb. 10). Man kann nun einfach auf „Unterschriftsfenster“ in der Leiste oben klicken; dann springt die Ansicht zur ersten digitalen Unterschrift. Man kann aber auch direkt im Dokument zur zu prüfenden Unterschrift scrollen.

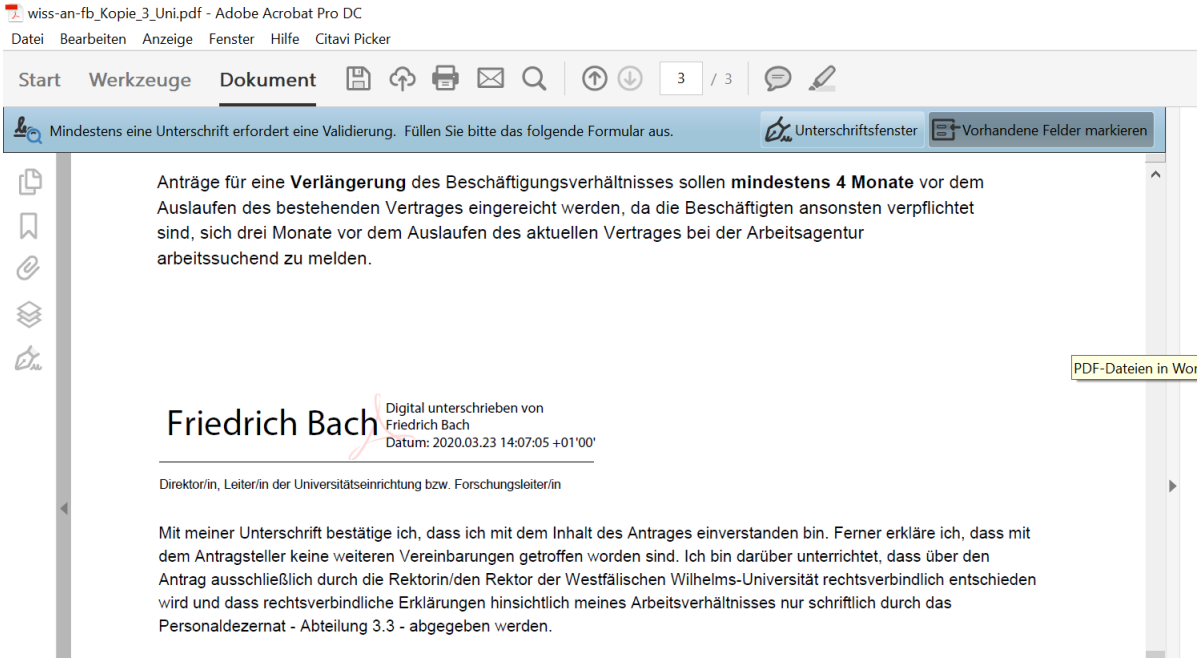

Abb. 10: Aufforderung zur Überprüfung einer Unterschrift beim Öffnen des Dokuments

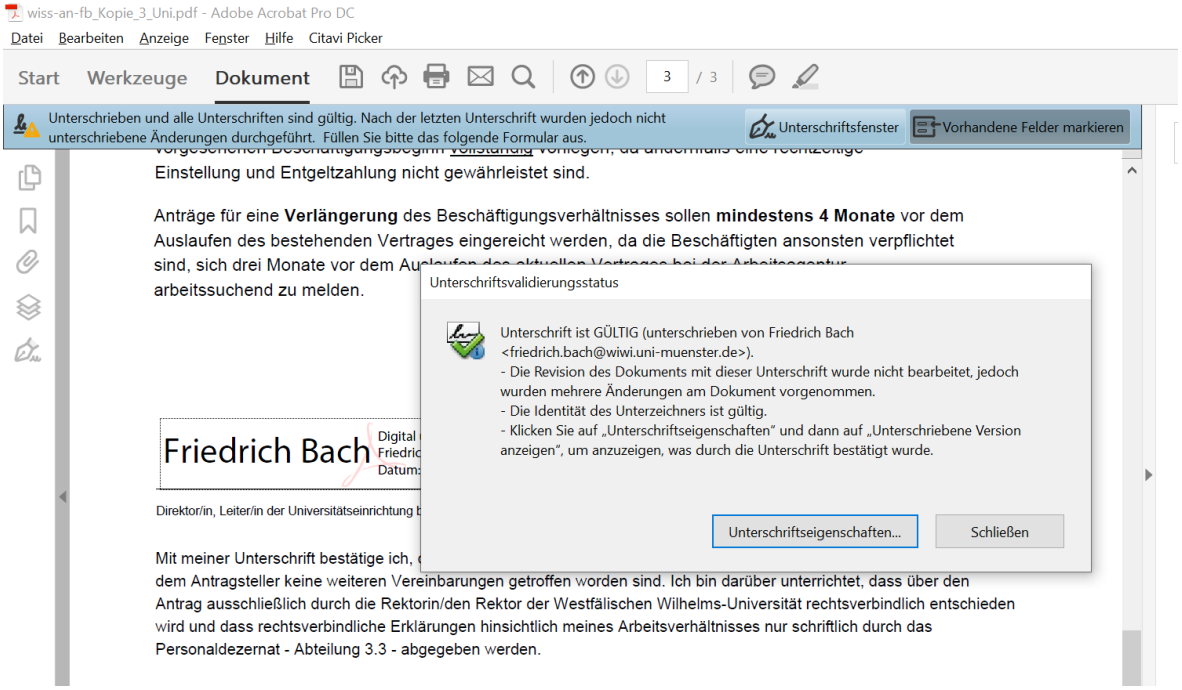

Abb. 11: Pop-Up-Fenster Unterschriftsvalidierungsstatus nach Klick auf die Unterschrift

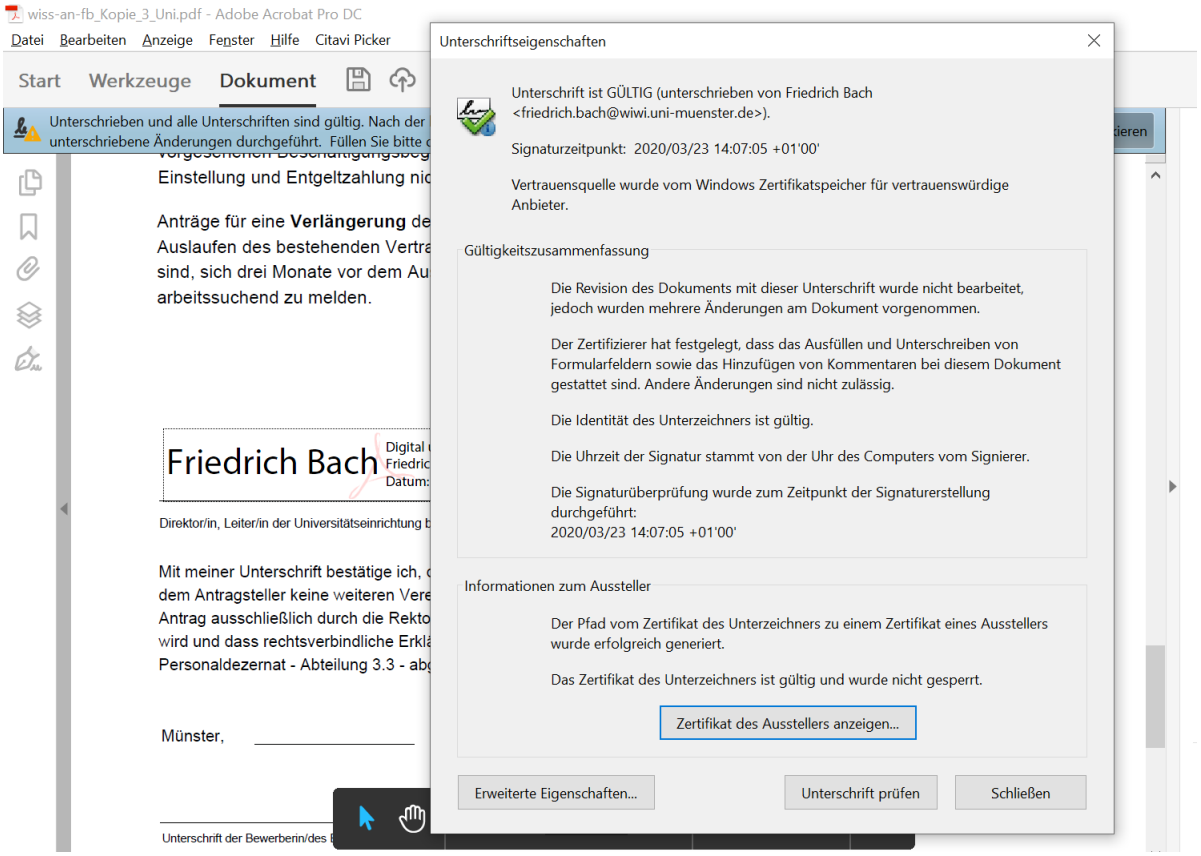

Abb. 12: Pop-Up-Fenster Unterschriftseigenschaften

Nach einem einfachen Klick auf die Unterschrift öffnet sich ein Pop-Up-Fenster mit dem Titel „Unterschriftsvalidierungsstatus“ (siehe Abb. 11). Hier sind bereits die wichtigsten Informationen zur Gültigkeit der Unterschrift abzulesen. Ein Klick auf den Button „Unterschriftseigenschaften“ in diesem Fenster öffnet ein weiteres, gleichnamiges Pop-Up-Fenster mit weiteren Informationen (siehe Abb. 12). Über die Buttons „Zertifikat des Ausstellers anzeigen“ und „Erweiterte Eigenschaften“ können ergänzende Angaben zum Zertifikat abgerufen werden (dazu gibt es hier allerdings keine Abbildungen mehr).