Acrobat Reader DC einrichten für TCS-Geant/Sectigo Zertifikate

Stand: 31.03.2022

Betriebssystem: Windows 10

Anwendung: Acrobat Reader DC

Zusätzlich benötigt:

(T-TeleSec\_GlobalRoot\_Class\_2.crt)

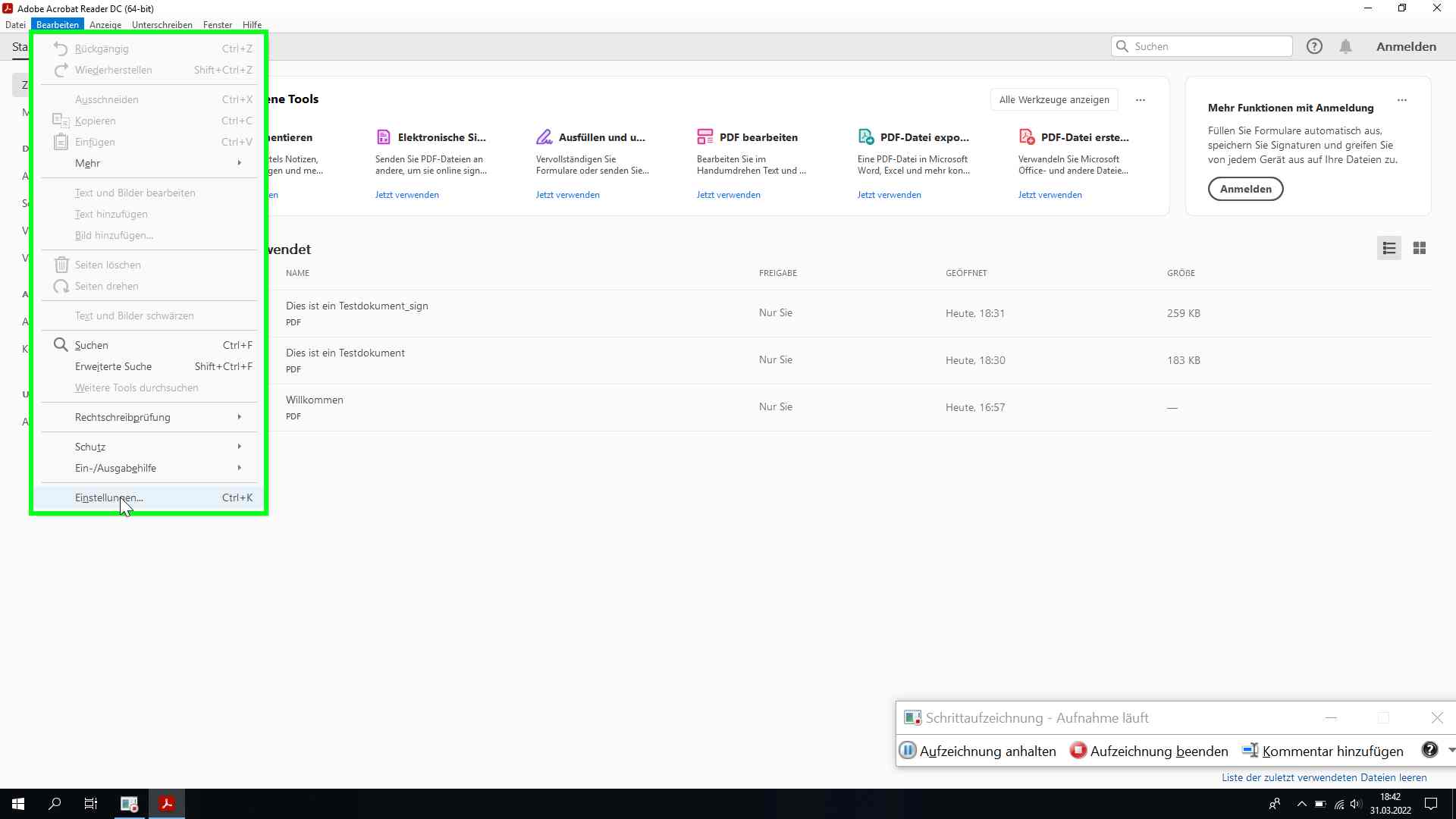
Rootcert\_TelecomSec2.crt

Ecc-root-2021.cer

UserTrustRSAohne Richtlinien.cer

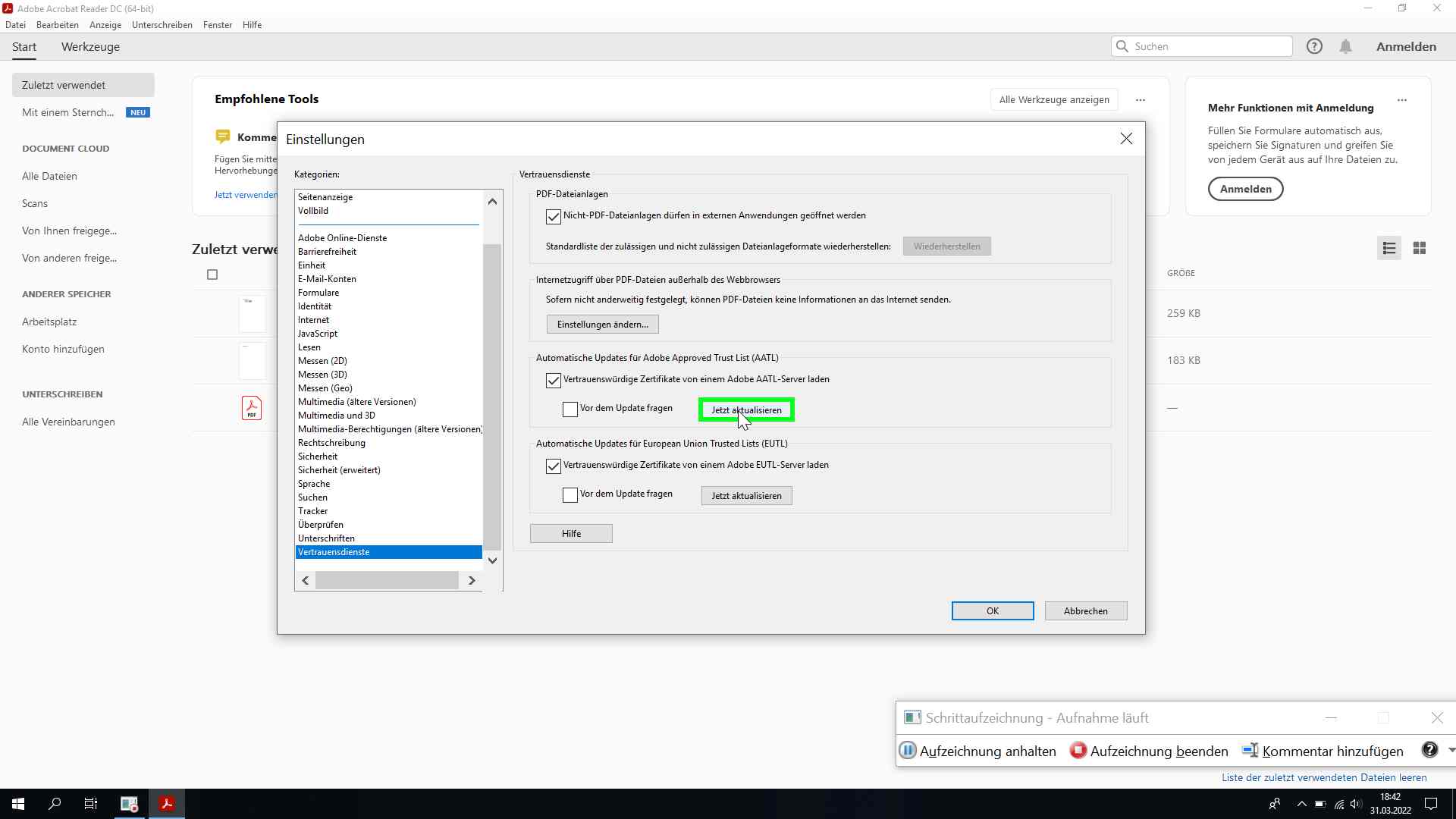
Acrobat Reader DC starten

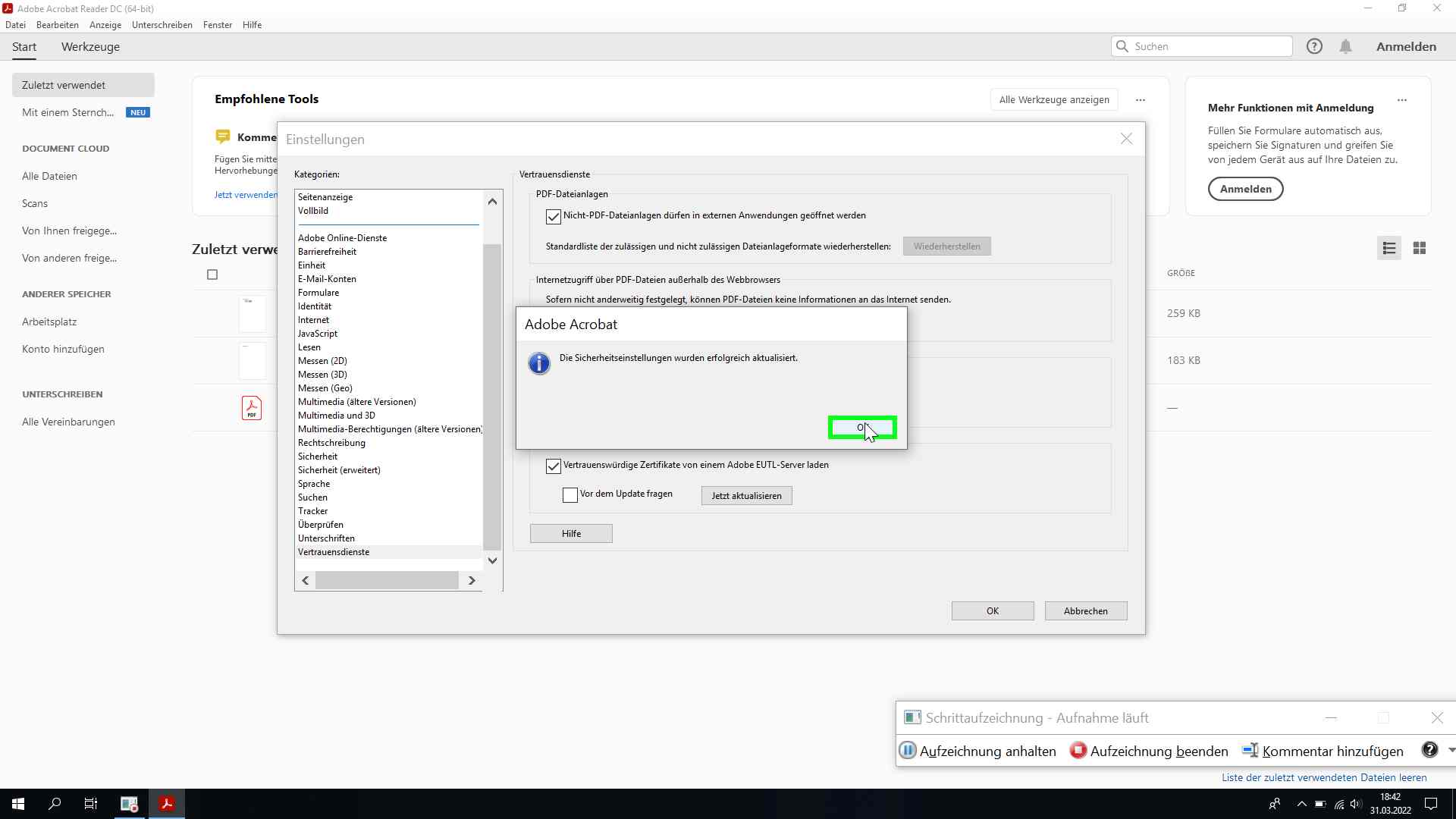
Adobe Acrobat-Einstellungen aufrufen

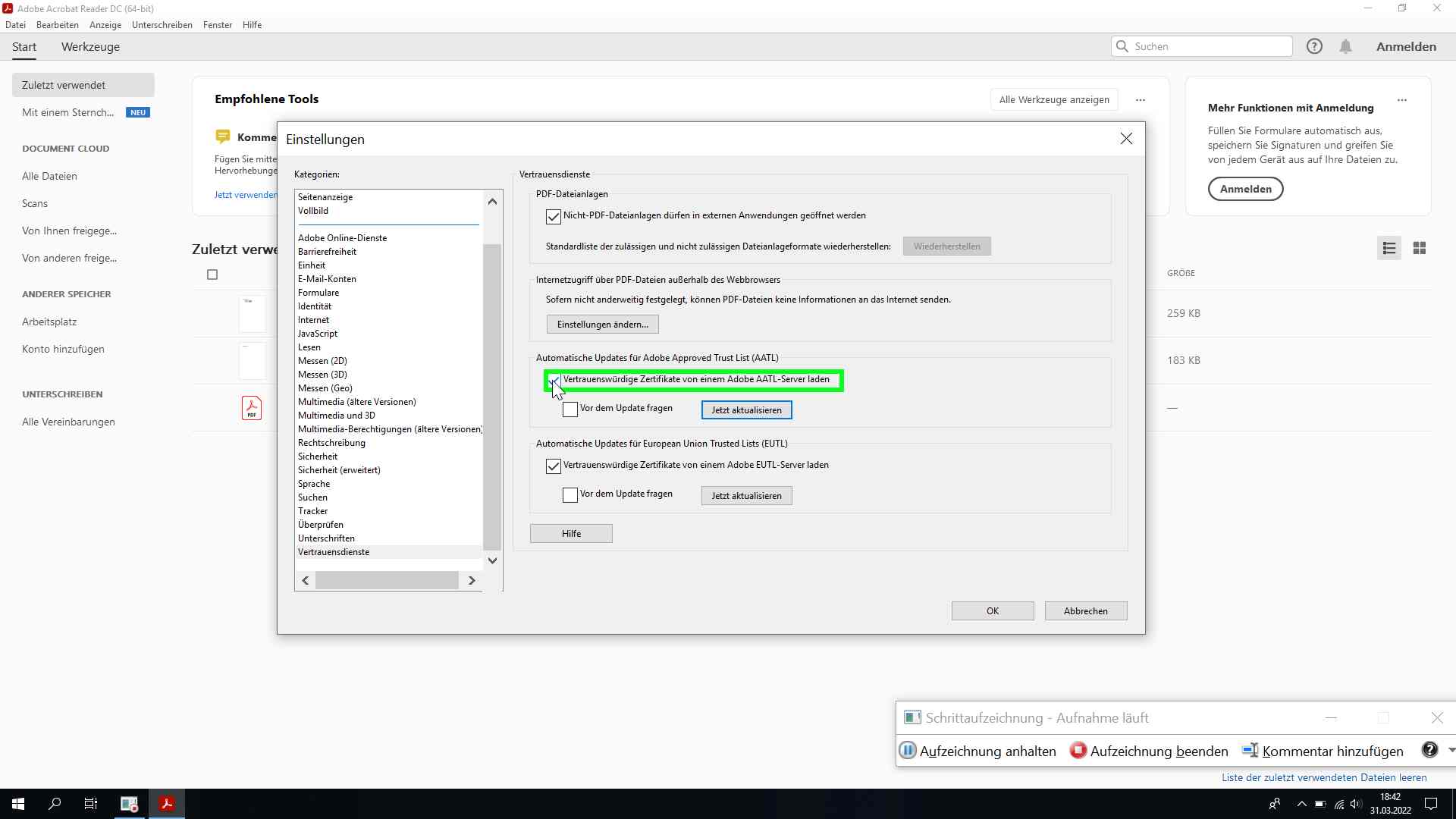


Einstellen der Vertrauensdienste

Die AATL (Adobe Approved Trust List) manuell aktualisieren.



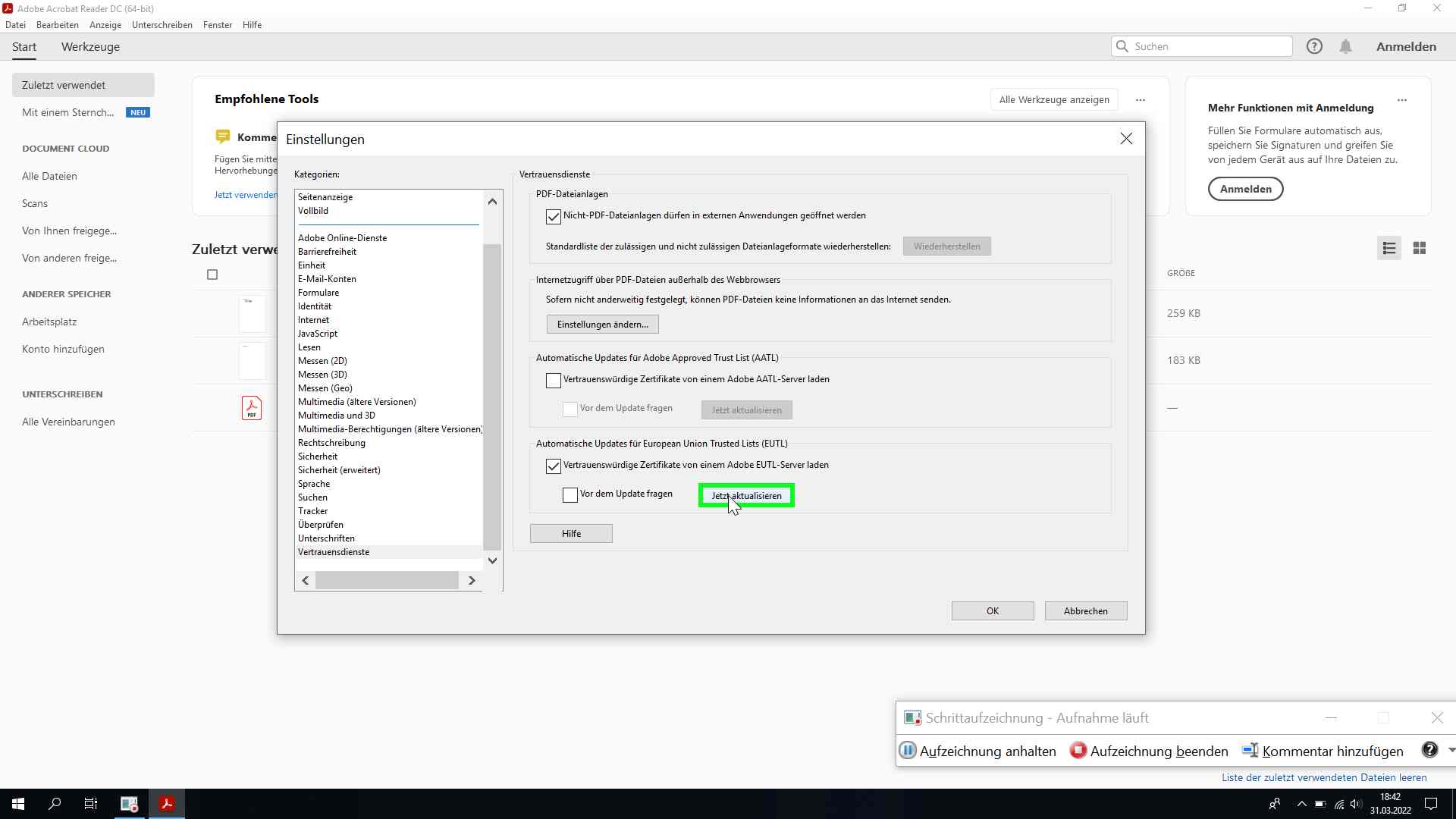


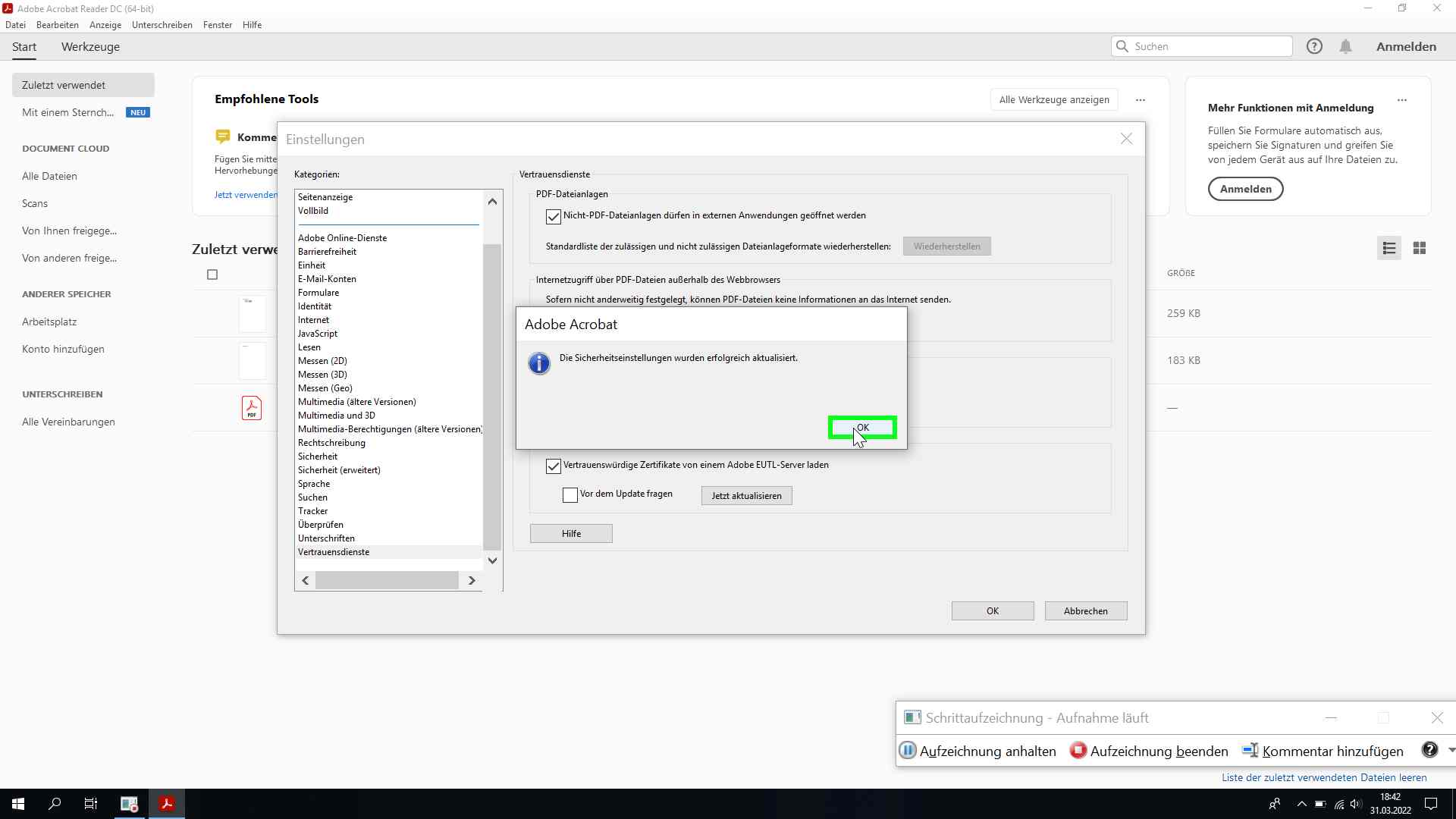


Die Option „automatische Updates für Adobe Approved Trust List (AATL) anschließend deaktivieren.

Wenn die automatischen Updates der AATL nicht deaktiviert werden, würden die später in der Konfiguration vorgenommene Änderung der Richtlinienprüfung im Falle eines Updates überschrieben werden.

Anschließend wird auch die European Union Trusted List (EUTL) manuell aktualisiert.

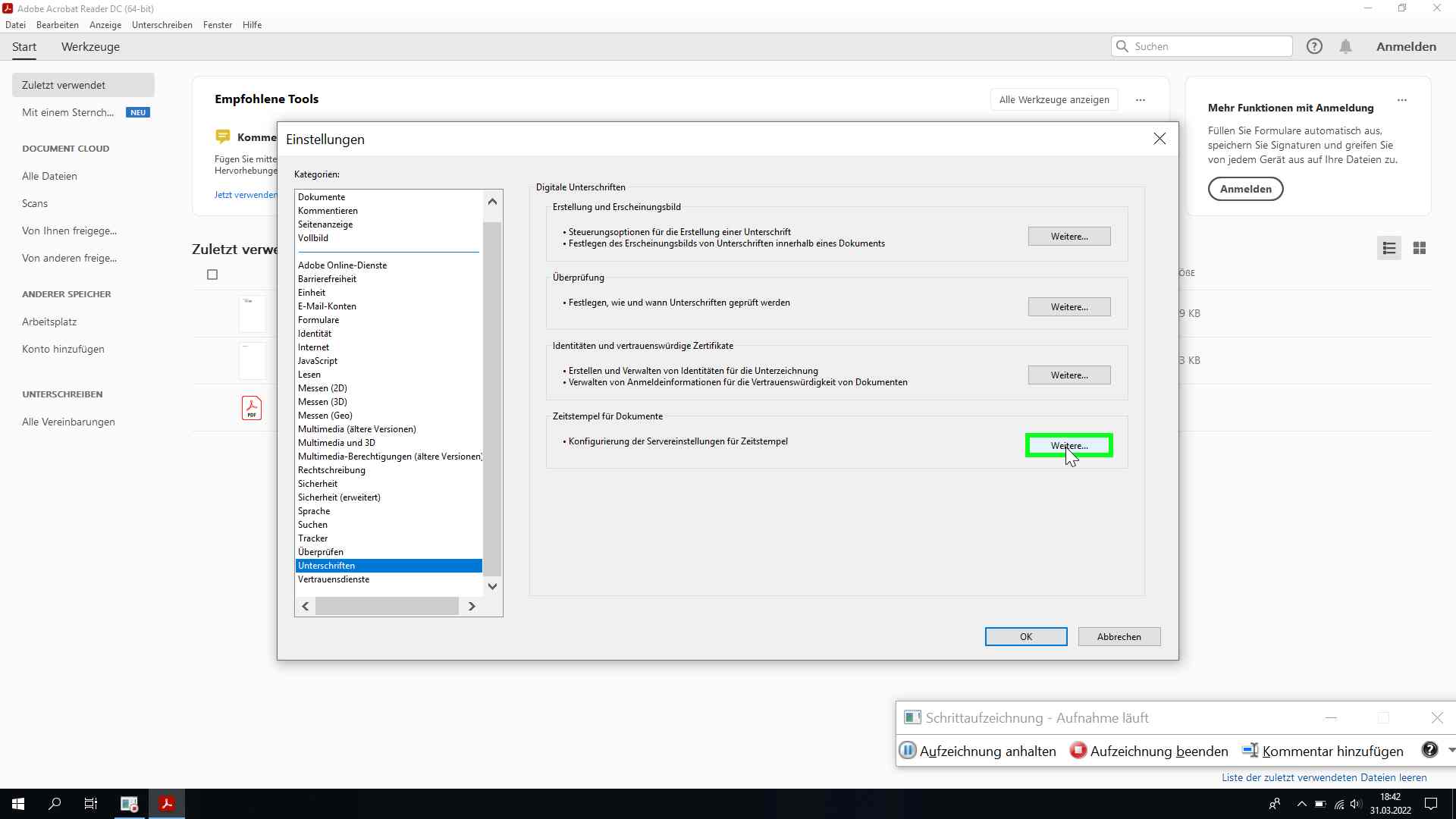




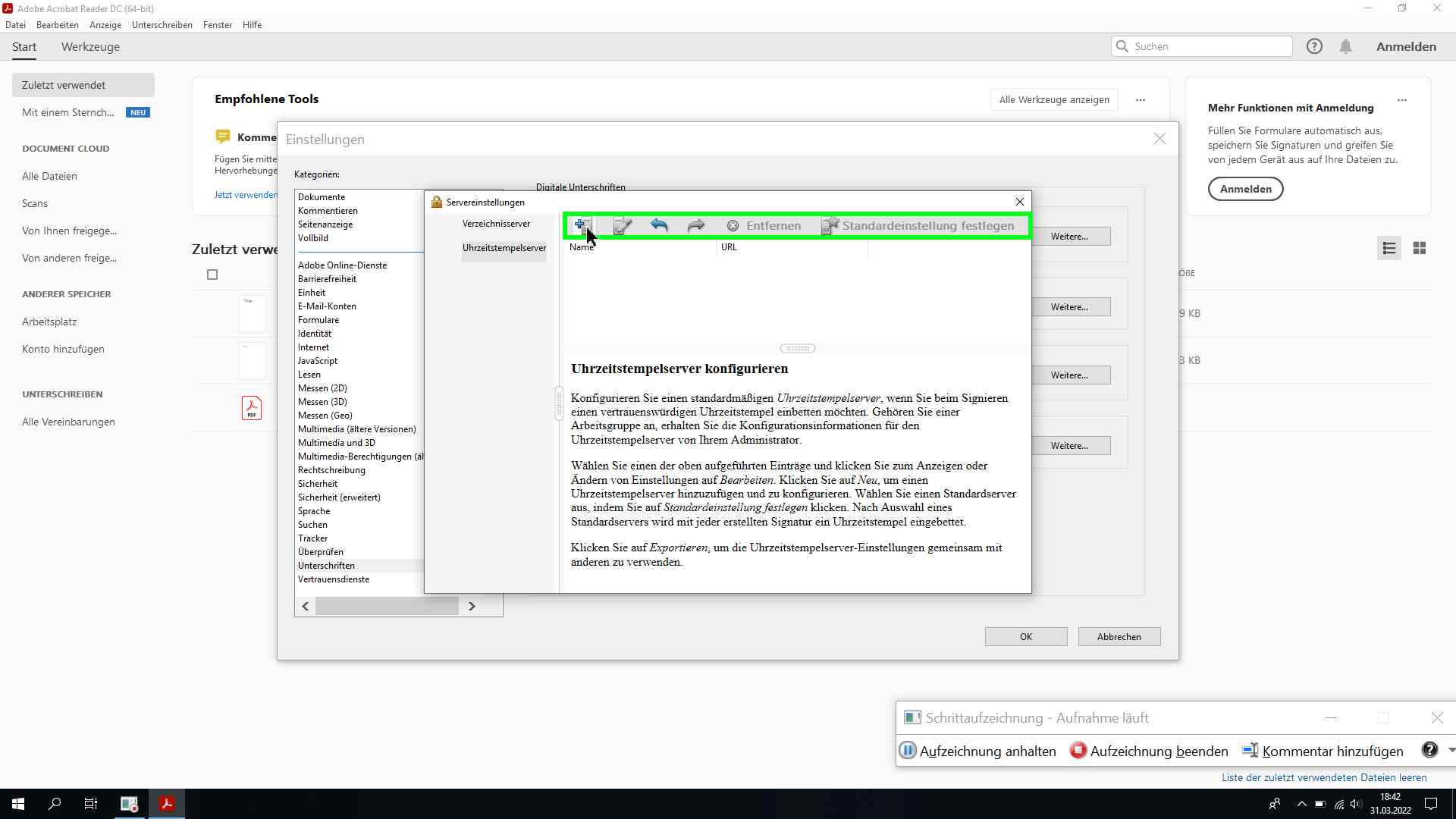
Hier können/sollen die automatischen Updates weiterhin aktiv sein.

Einstellen des Zeitstempeldienstes

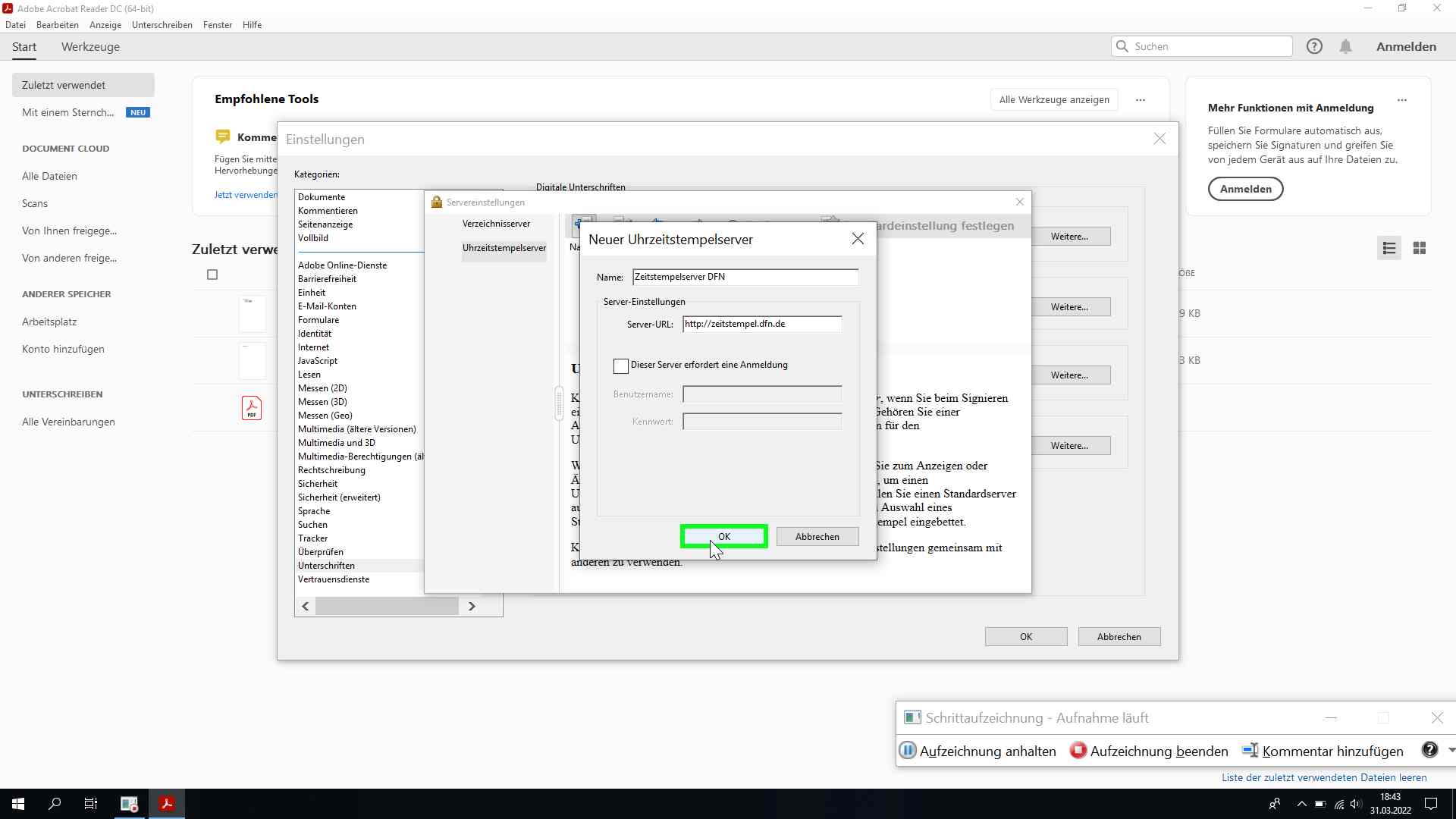
Wechseln Sie in die Kategorie „Unterschriften“ und rufen dort die Konfiguration der Servereinstellungen für den Zeitstempeldienst auf.



Wenn dort noch kein Eintrag vorhanden ist, fügen Sie einen neuen Eintrag über den“Hinzufügen“-/“Pluszeichen“-Button hinzu

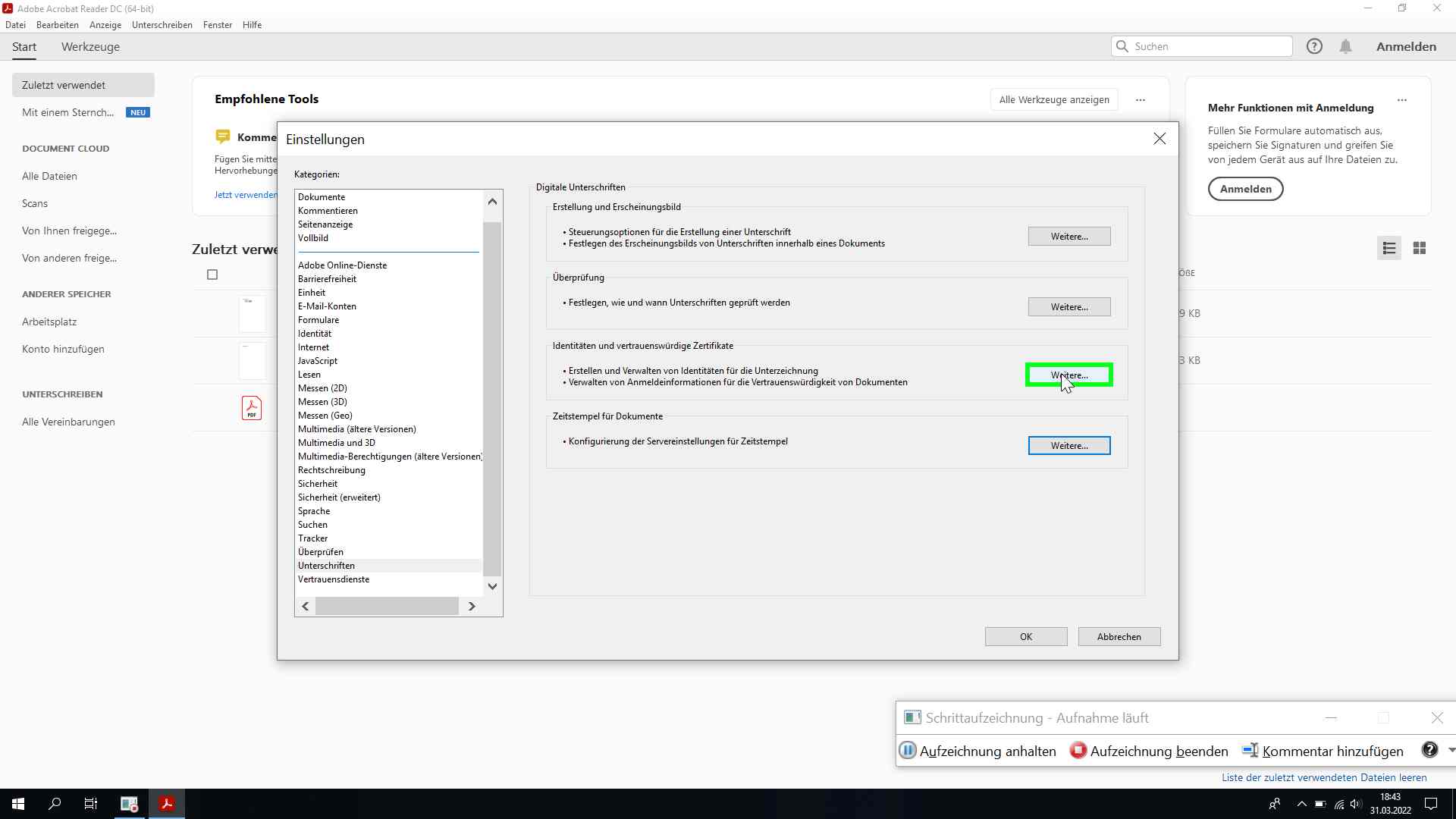


Tragen Sie dort unter Name „DFN Zeitstempelserver“ und unter Server-URL “http://zeitstempel.dfn.de/“ ein.



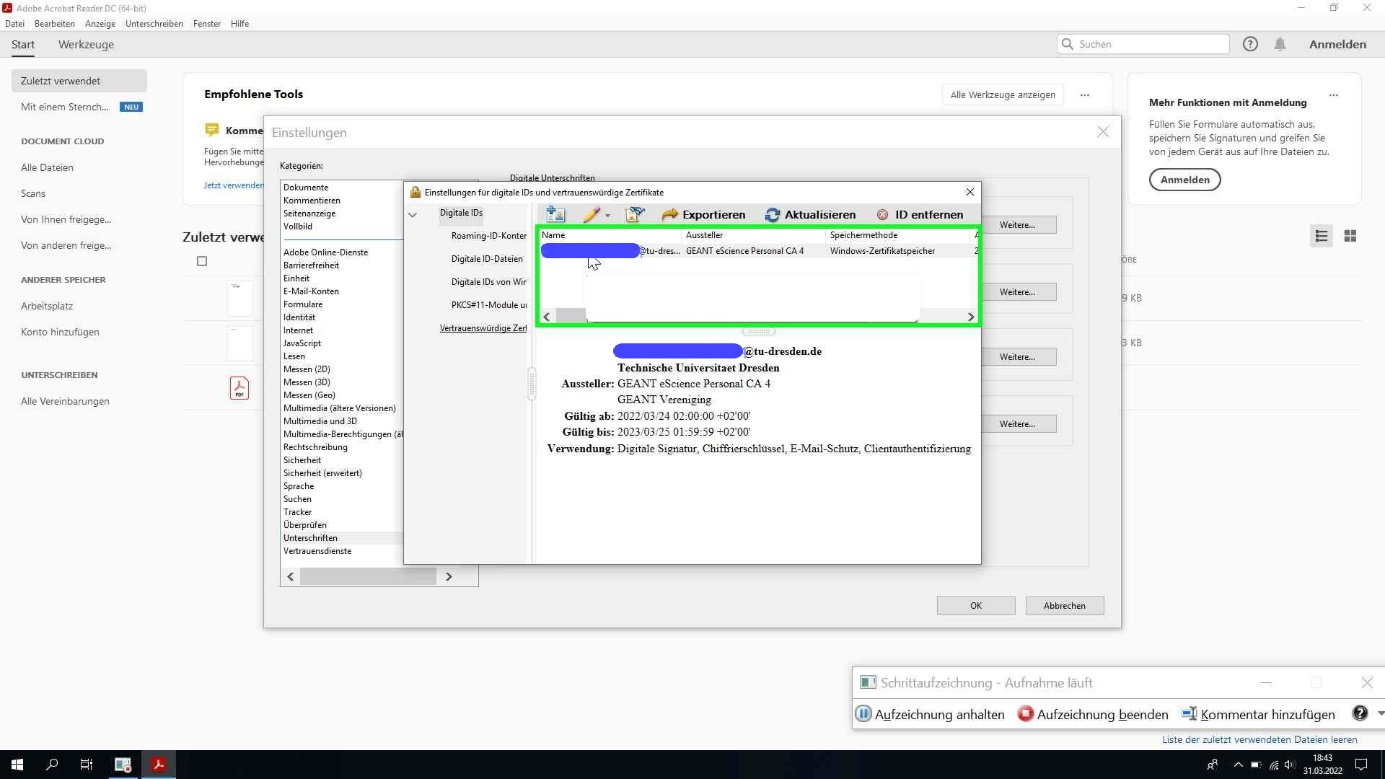
Einstellungen der Identitäten und vertrauenswürdigen Zertifikate

Bleiben Sie in der Kategorie „Unterschriften“ und wechseln zu „der Identitäten und vertrauenswürdigen Zertifikate“

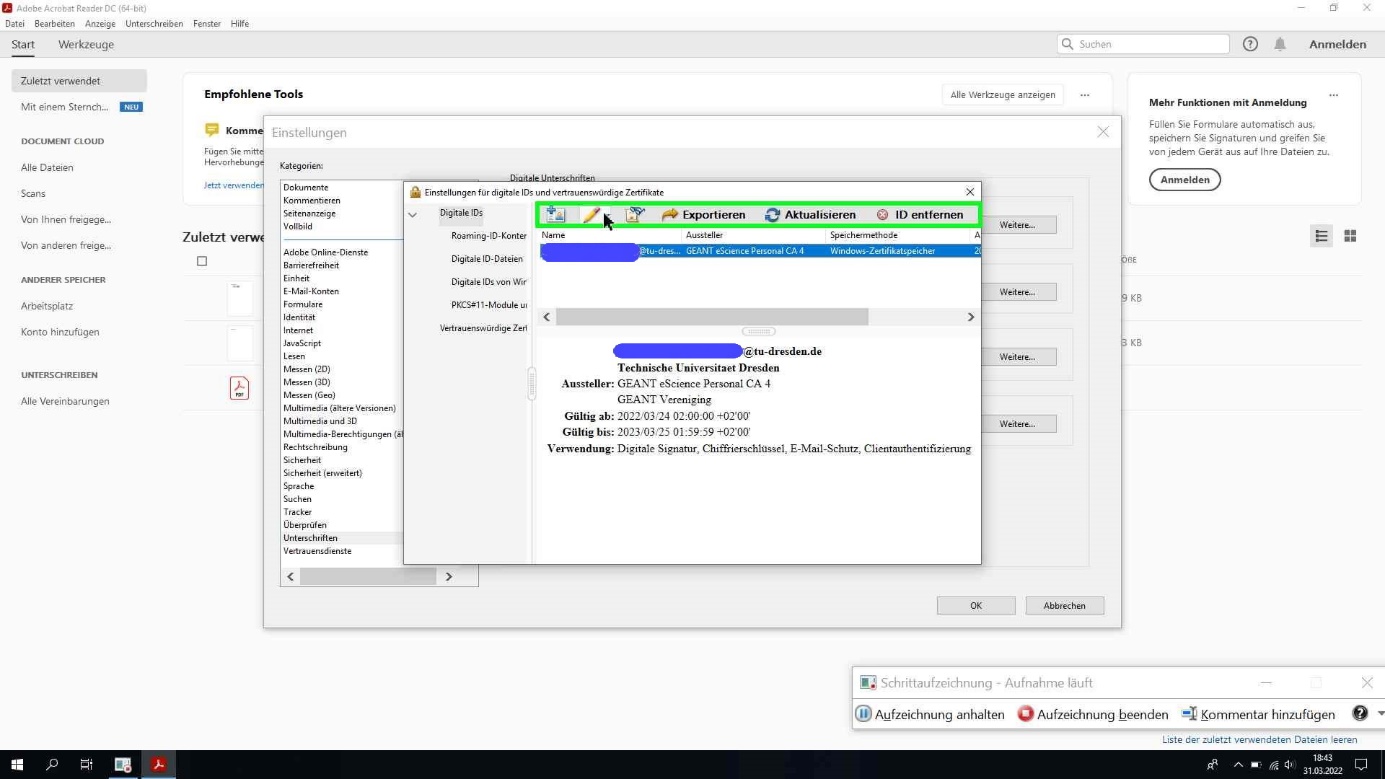


Festlegen des Unterschriftenzertifikats

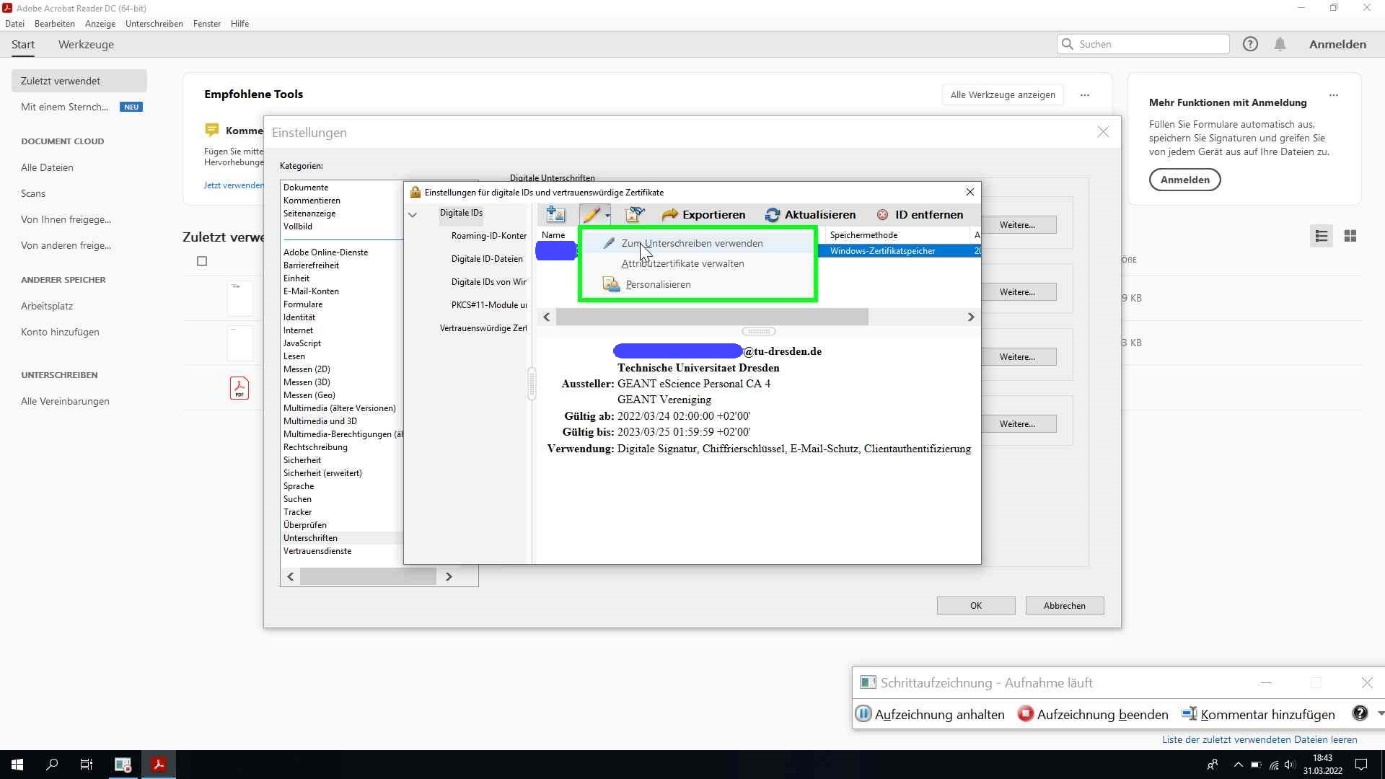
Aus der Liste mit den unter „Digitale-IDs“ (-Digitale IDs von Windows)aufgeführten Zertifikaten markieren Sie Ihr aktiv gültiges Zertifikat.



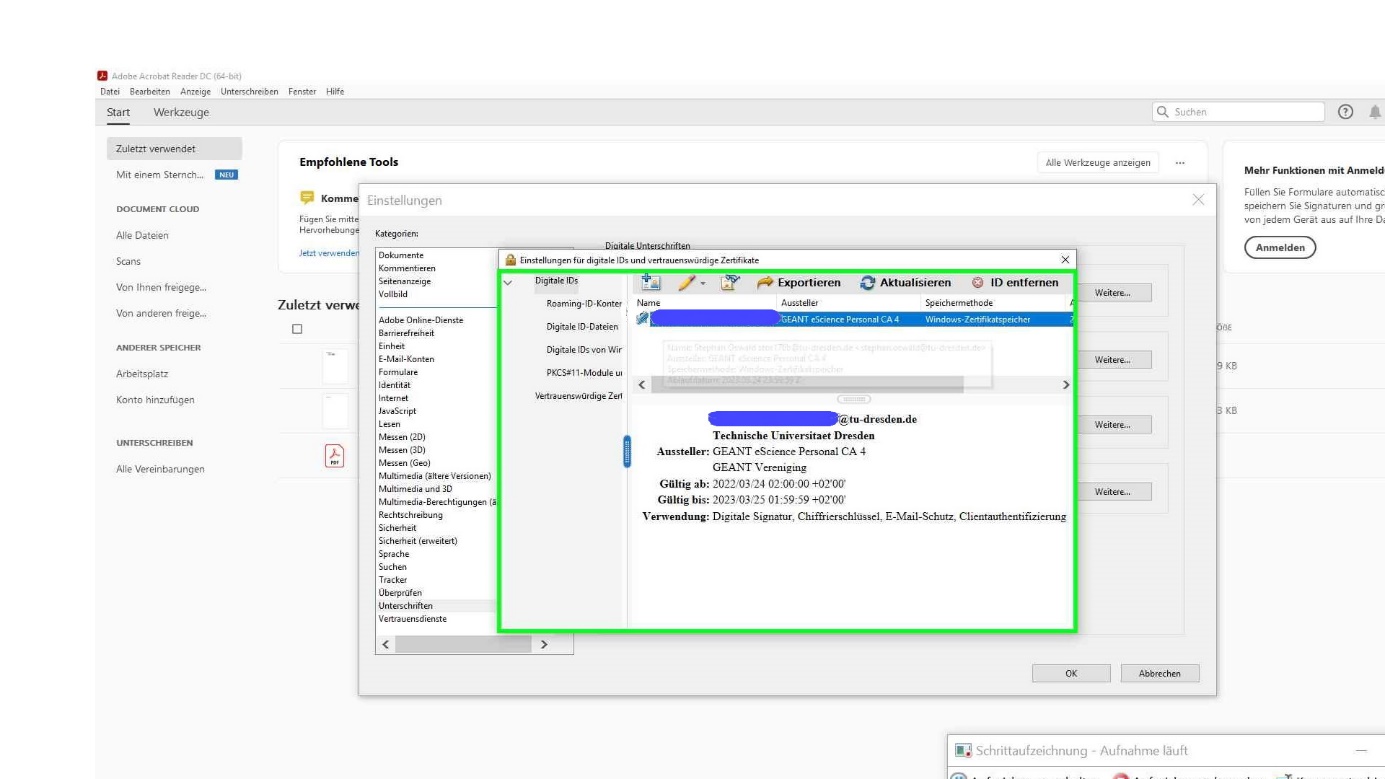
Wählen Sie das „Bleistift“-Symbol oder den „Bearbeiten“-Button.



Markieren Sie die Option „Zum Unterschreiben verwenden“



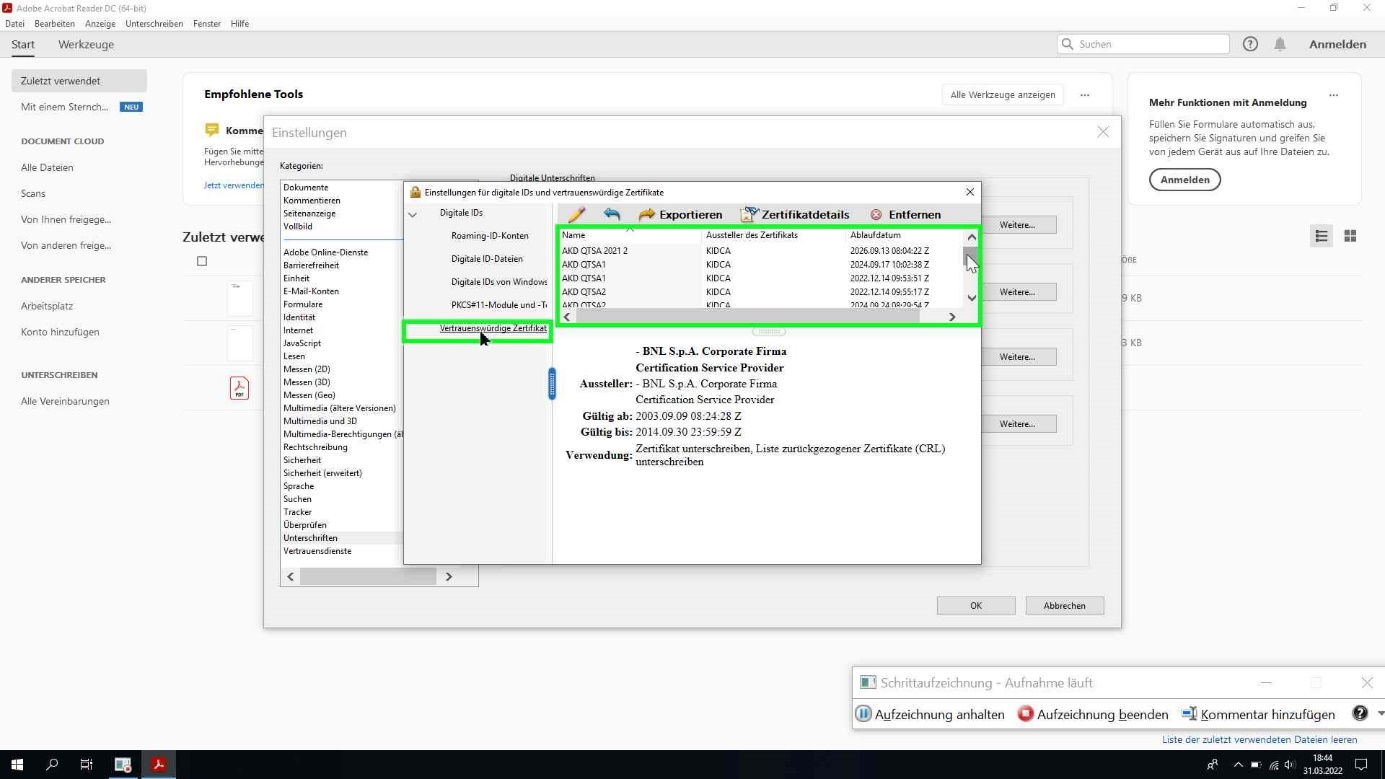
Das zum Unterschreiben zu verwendende Zertifikat erhält in der Liste ein (bläuliches) Stift-Symbol vorangestellt.



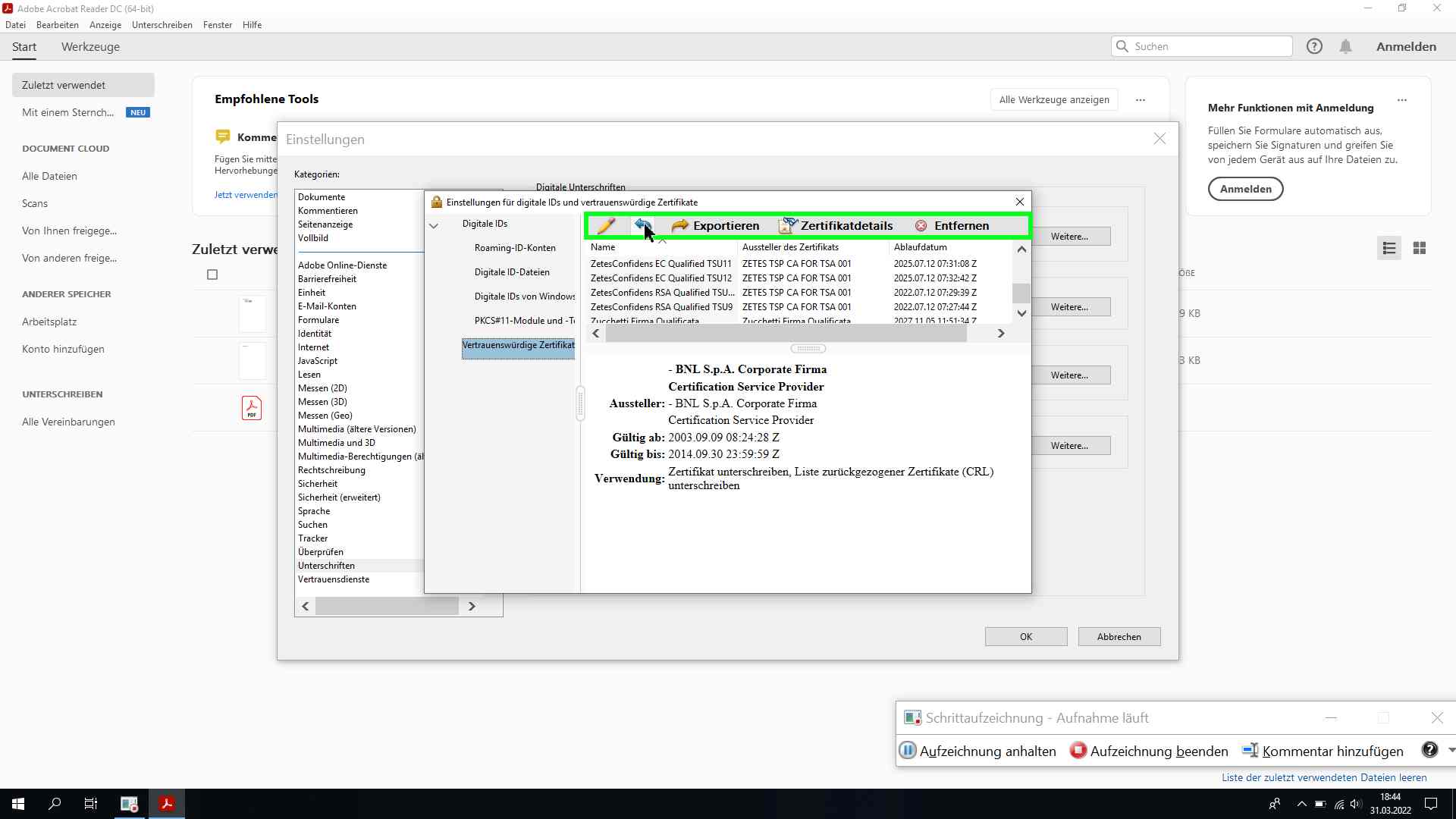
Einstellungen der vertrauenswürdigen Zertifikate

Wechseln Sie zu den vertrauenswürdigen Zertifikaten

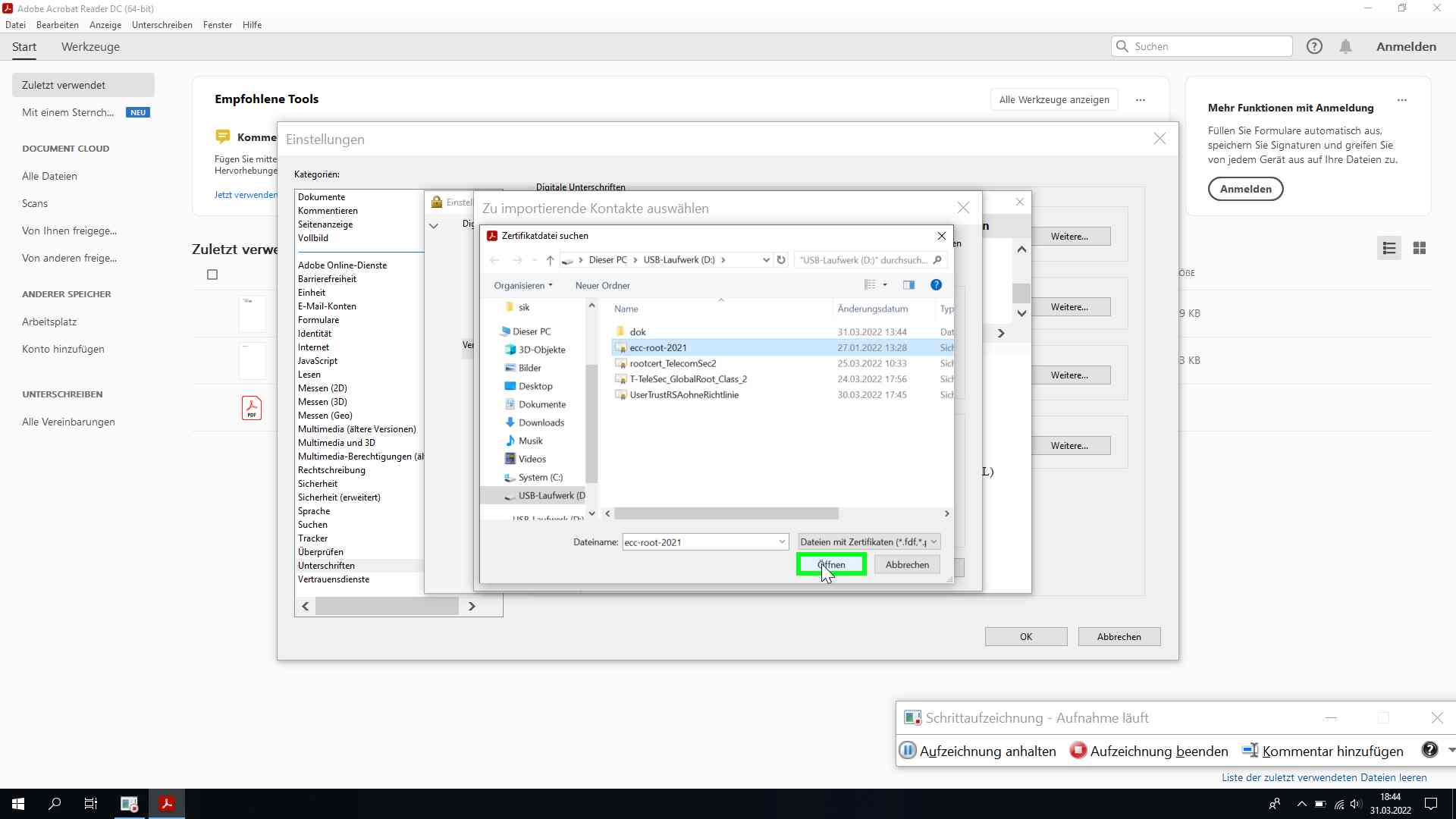
Import des UserTrust ECC-Zertifikats



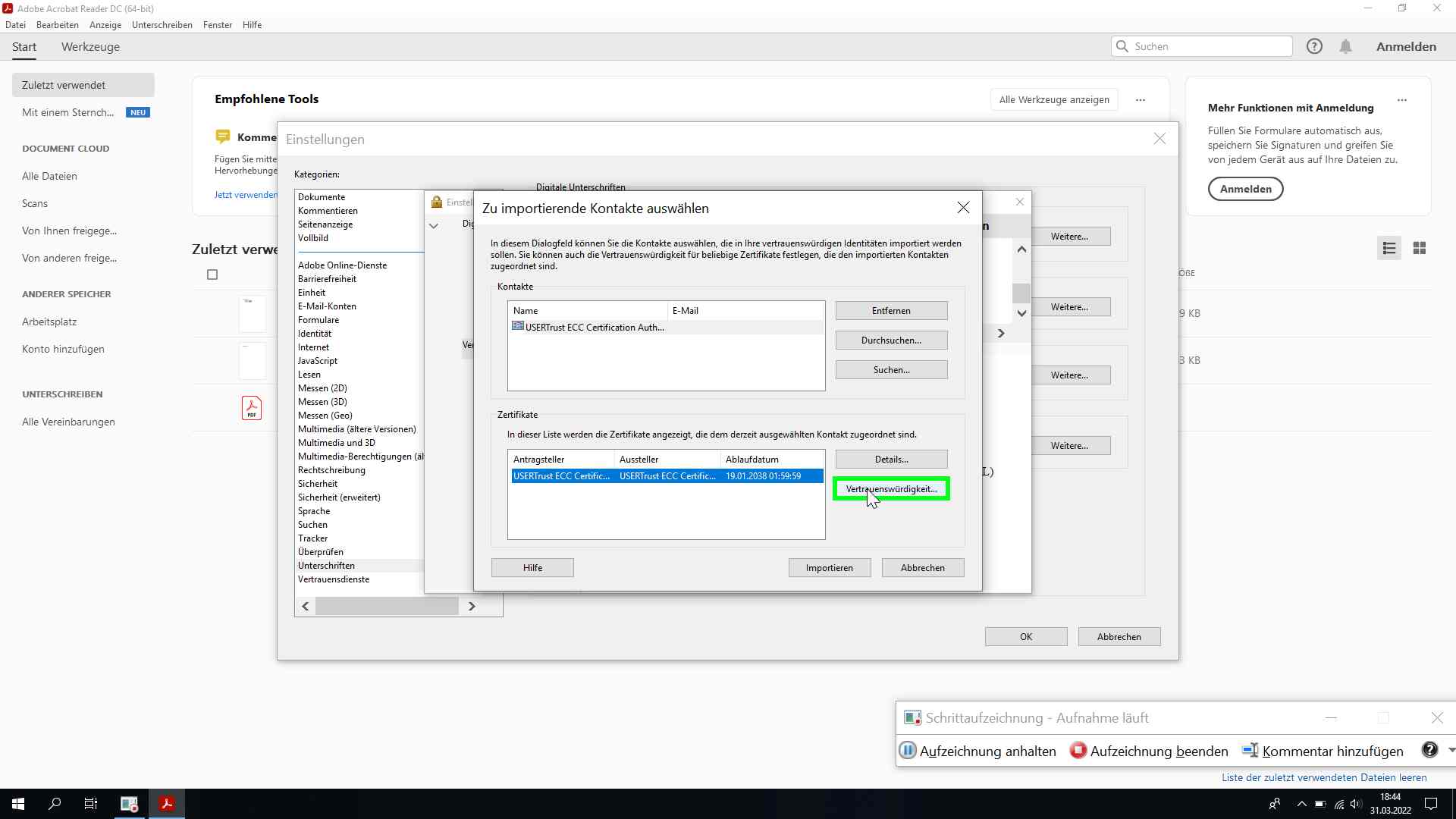
Klicken Sie auf den „Importieren“/ „blauen Linkspfeil“-Button



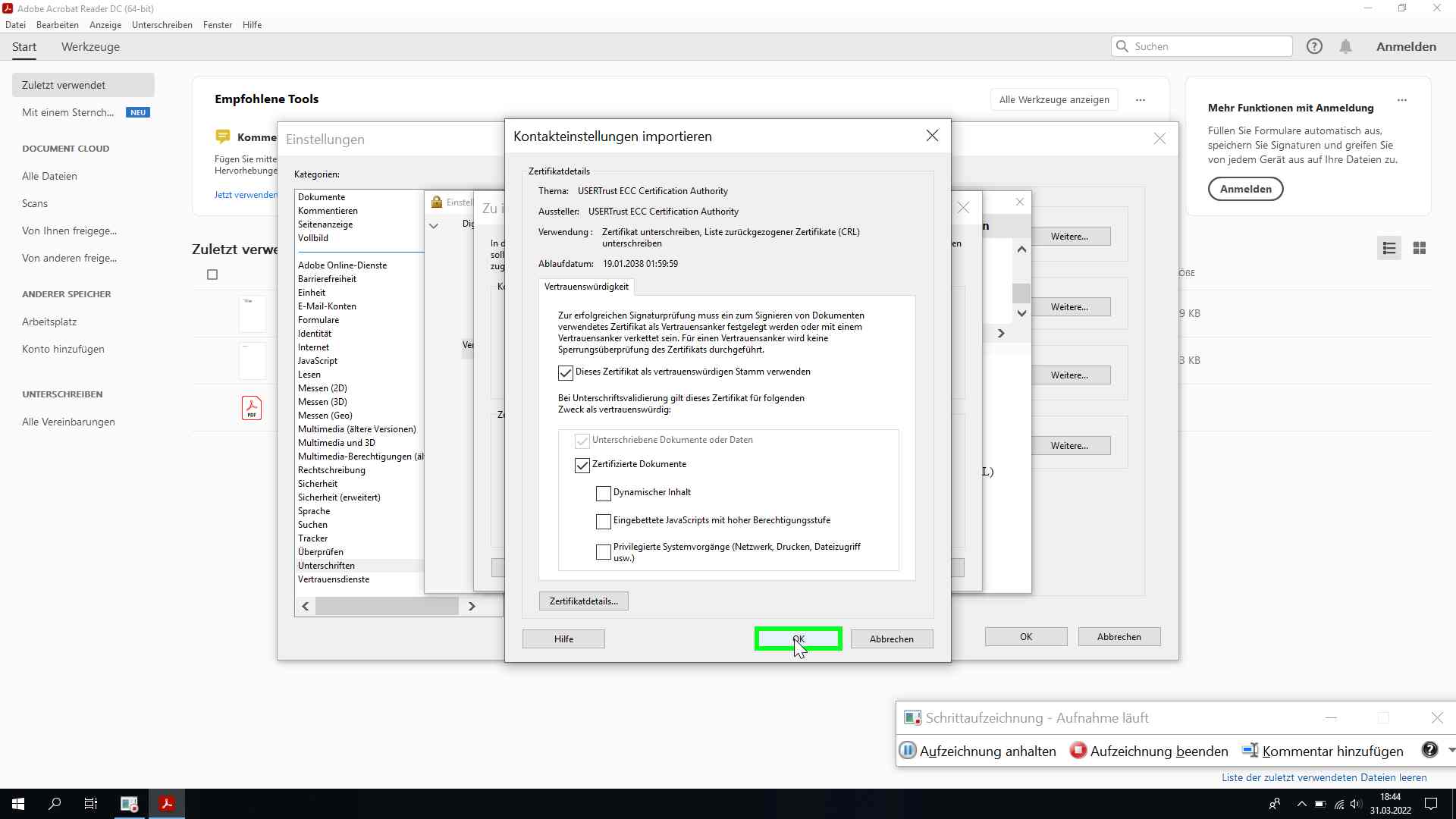
Suchen Sie mittels des Durchsuchen-Buttons die Datei „Ecc-root-2021.cer“, die Sie zuvor heruntergeladen haben (siehe oben) und öffnen es. (Wenn das Zertifikat nicht in der Auswahlliste angezeigt wird, den Filter im Feld „Dateiname“ durch die Eingabe von „\*.cer“ ändern.)



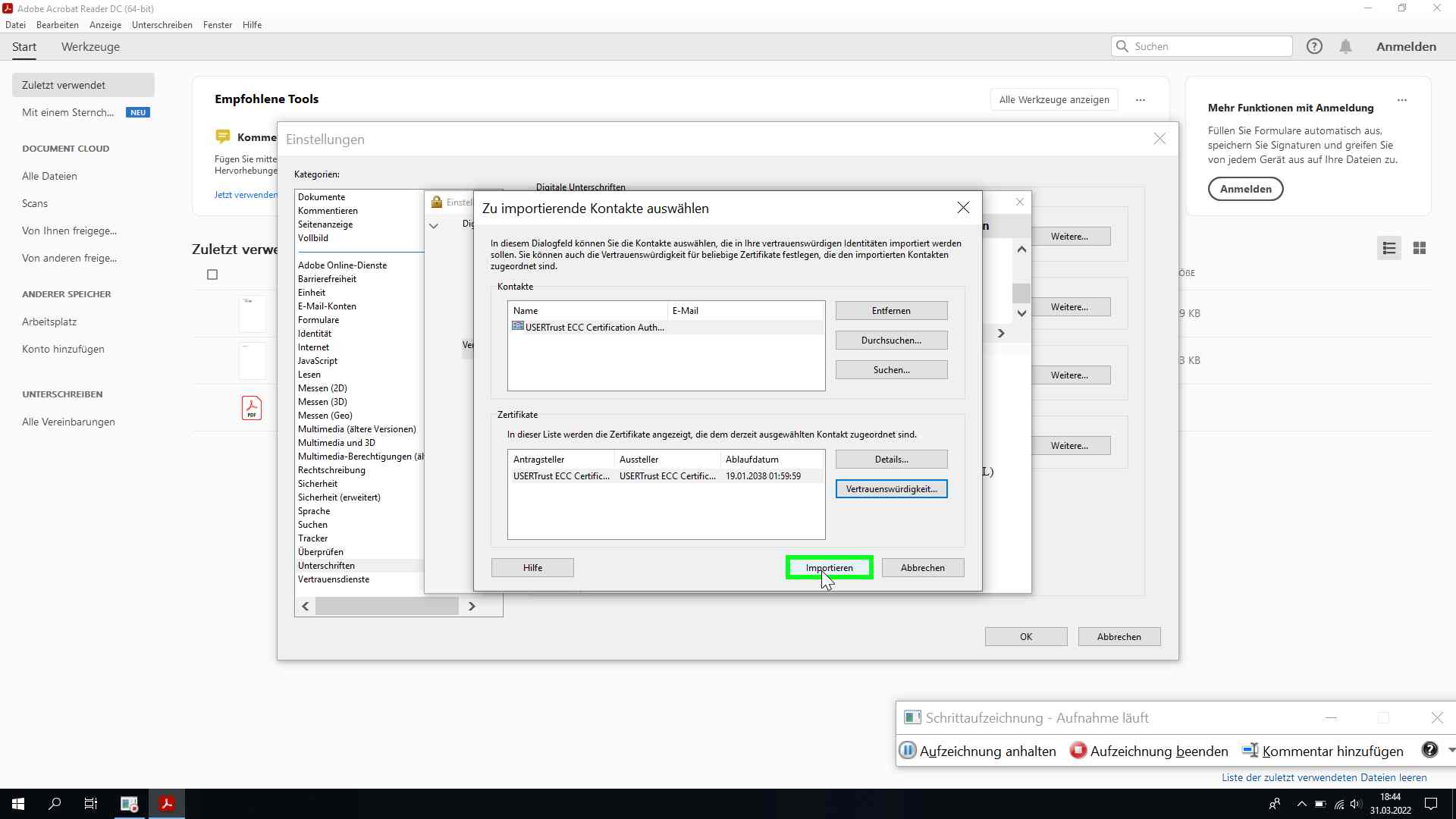
Nachdem Sie die Zertifikatdatei zunächst im oberen Bereich markiert haben, können Sie sie auch im unteren Bereich markieren und mit dem Button „Vertrauenswürdigkeit“ bearbeiten.



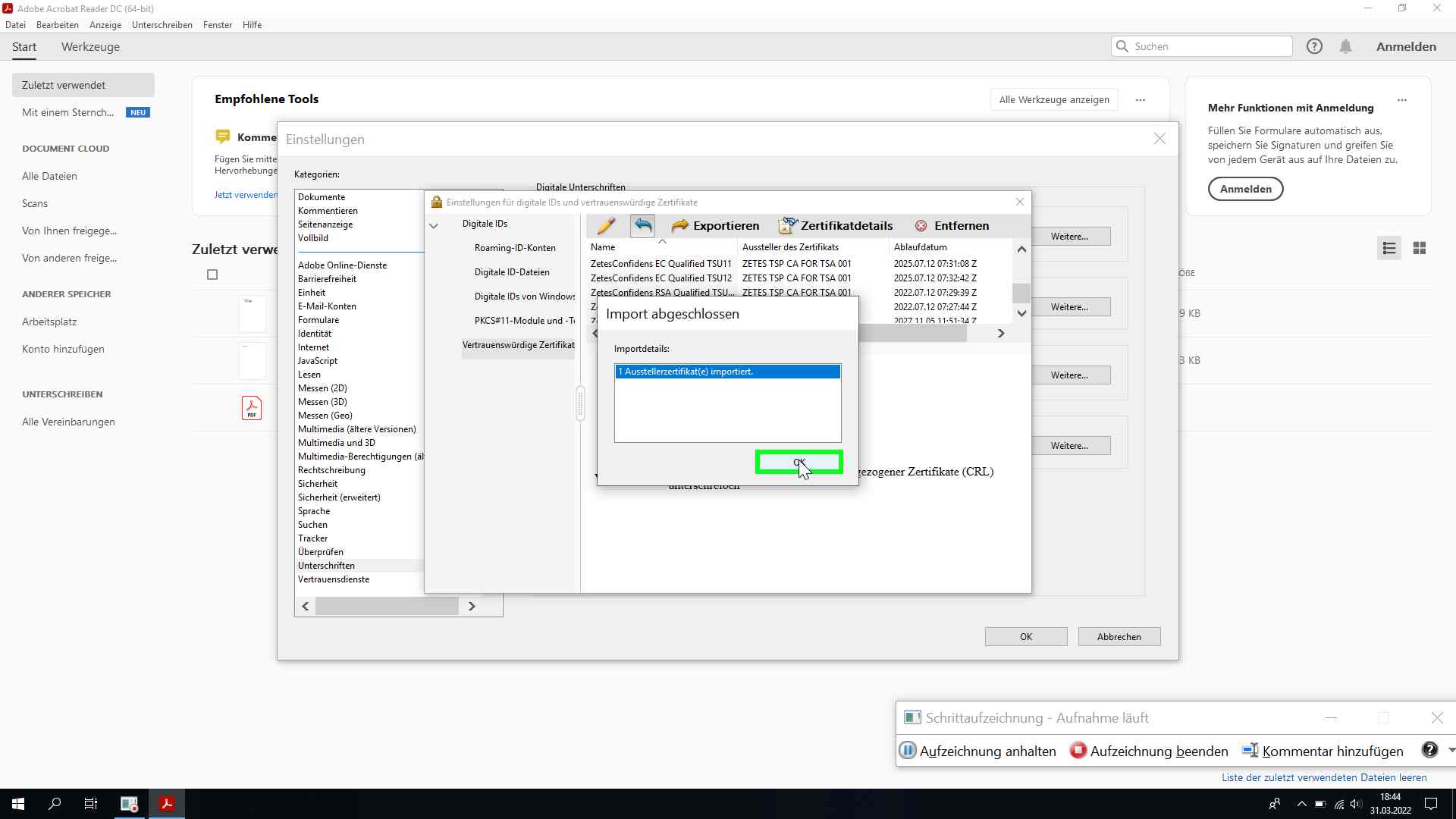
Markieren Sie dieses Zertifikat für „Dieses Zertifikat als vertrauenswürdigen Stamm verwenden“ und setzen danach die Option „“Zertifizierte Dokumente“. Schließen Sie die Bearbeitung mit „OK“ ab.



Nun wird das Zertifikat importiert.

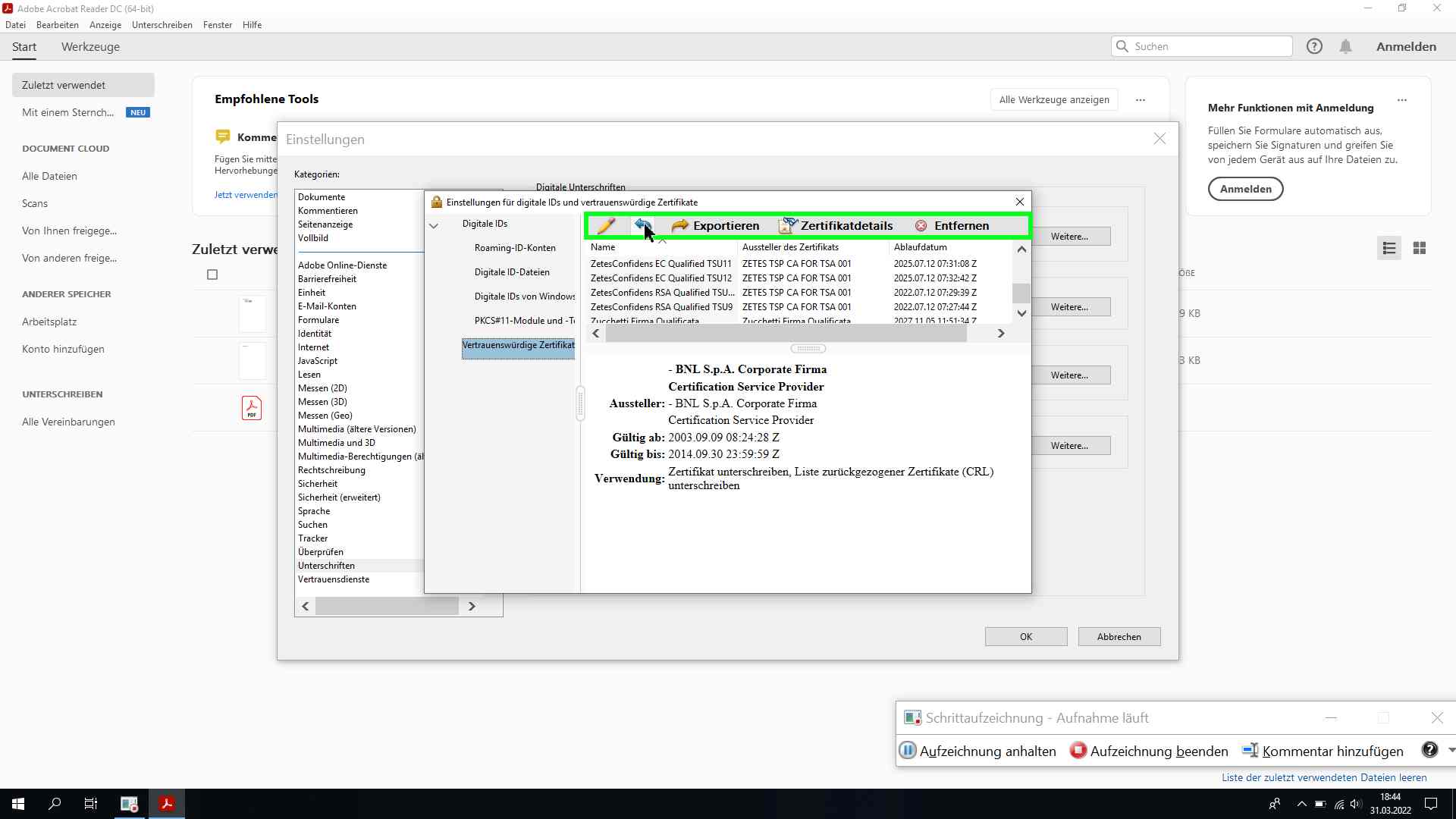


Das Meldungsfenster nach dem Import kann geschlossen werden. Sollte das Zertifikat bereits vorhanden gewesen sein, weicht die Rückmeldung leicht vom gezeigten Bild ab.

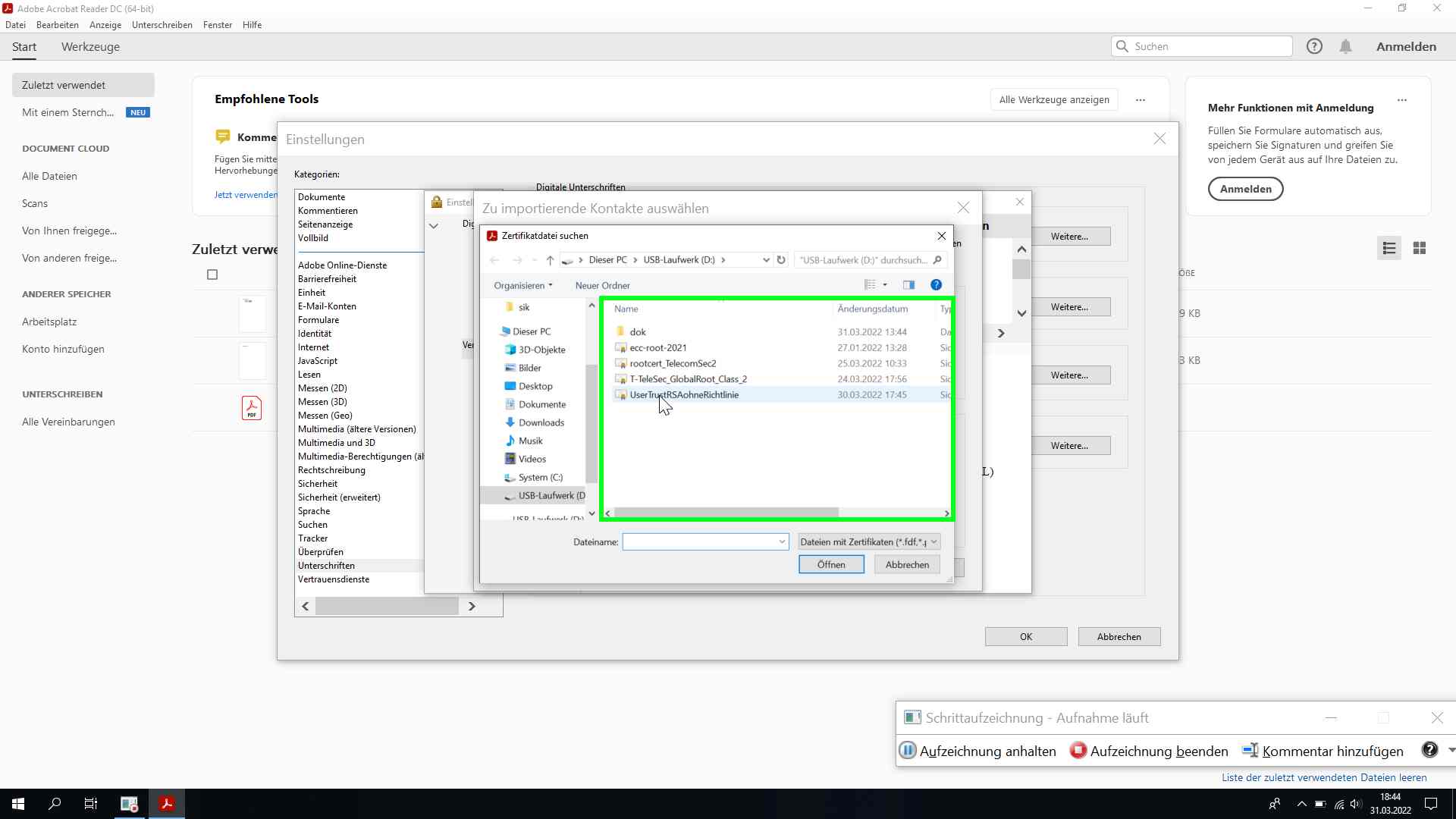


Import des UserTrust RSA-Zertifikats

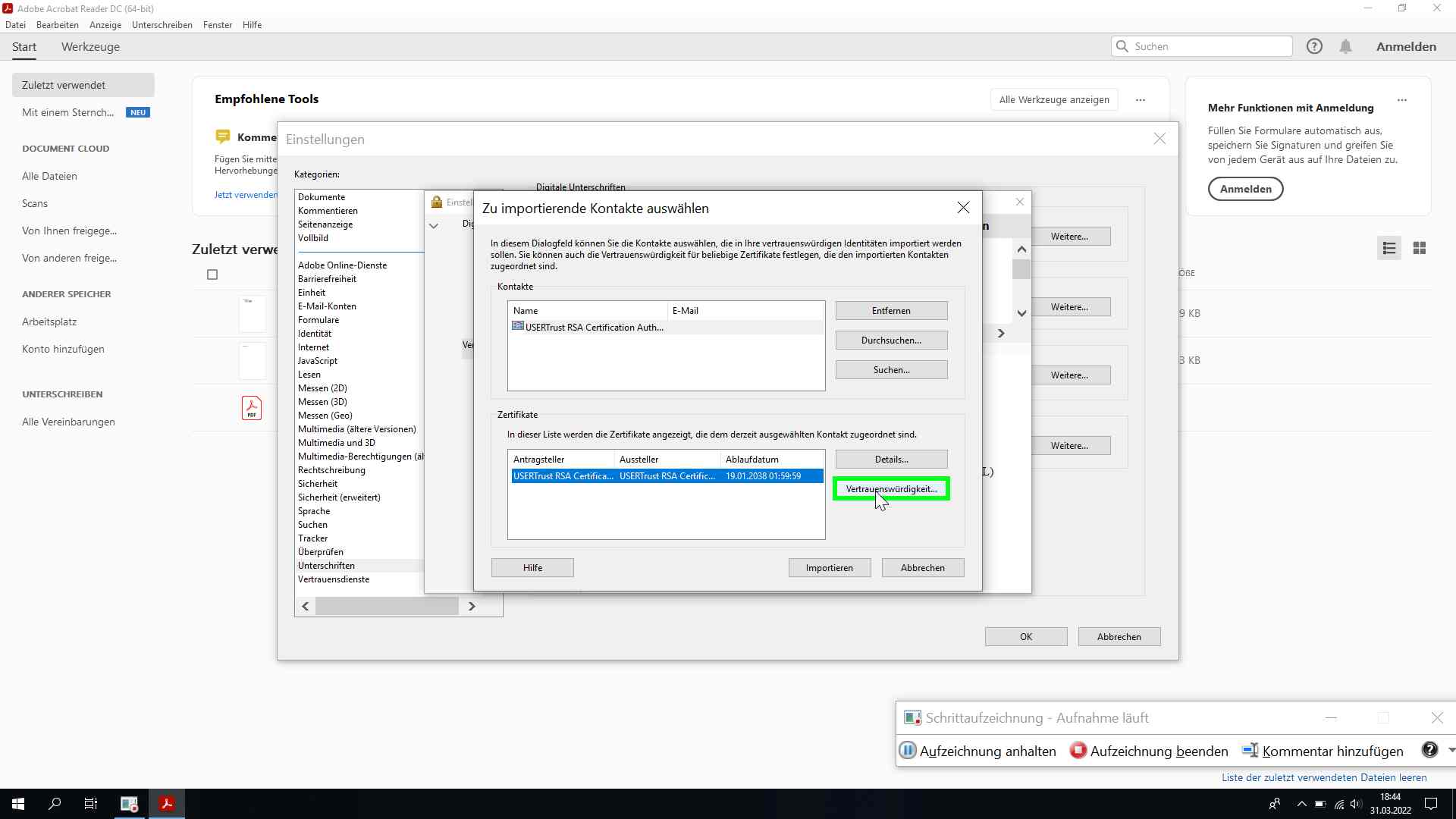
Klicken Sie auf den „Importieren“/ „blauen Linkspfeil“-Button



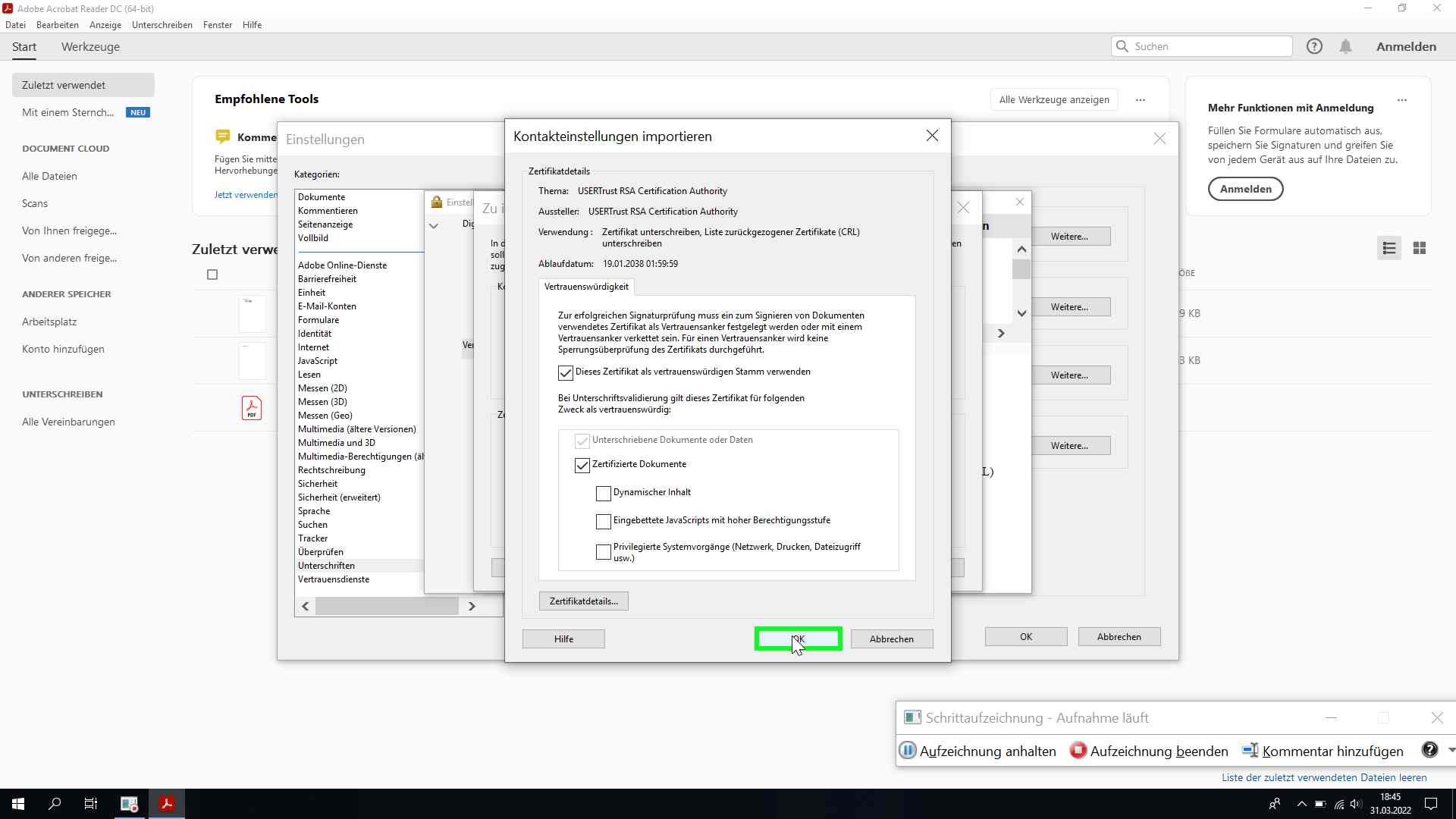
Suchen Sie mittels des Durchsuchen-Buttons die Datei „UserTrustRSAohne Richtlinie.cer“, die Sie zuvor heruntergeladen haben (siehe oben) und öffnen es. (Wenn das Zertifikat nicht in der Auswahlliste angezeigt wird, den Filter im Feld „Dateiname“ durch die Eingabe von „\*.cer“ ändern.)



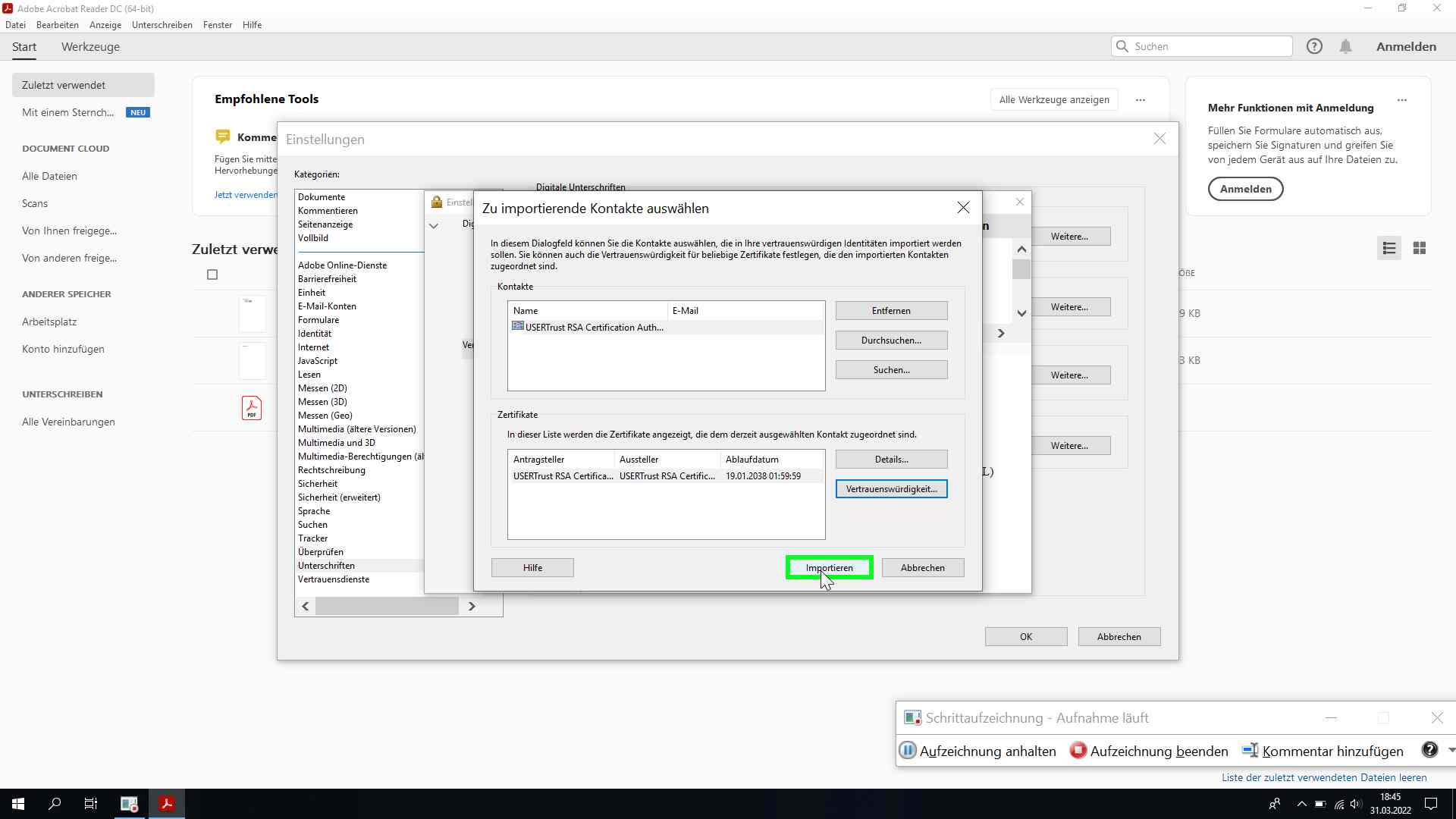
Nachdem Sie die Zertifikatdatei zunächst im oberen Bereich markiert haben, können Sie sie auch im unteren Bereich markieren und mit dem Button „Vertrauenswürdigkeit“ bearbeiten.



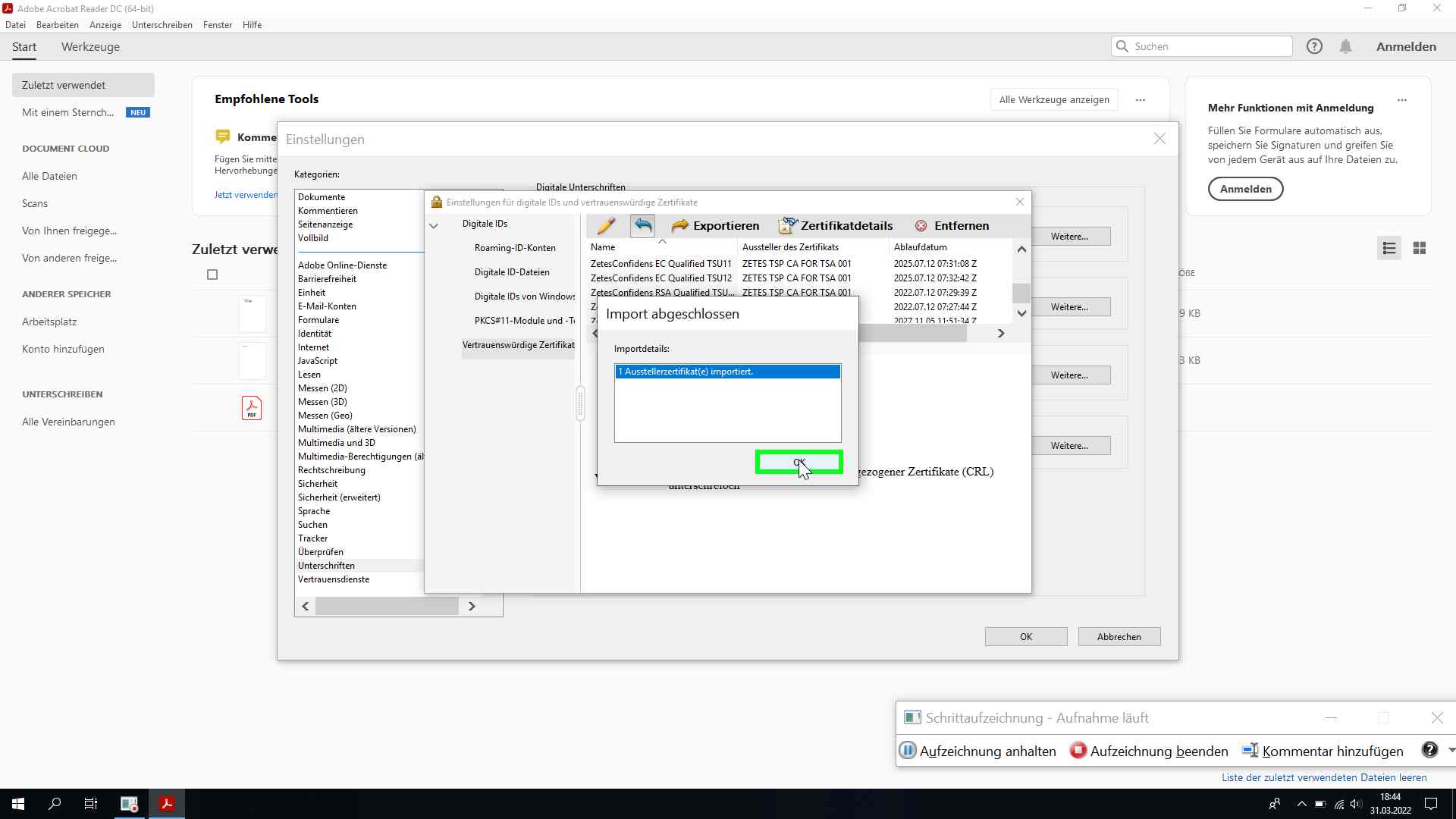
Markieren Sie dieses Zertifikat für „Dieses Zertifikat als vertrauenswürdigen Stamm verwenden“ und setzen danach die Option „“Zertifizierte Dokumente“. Schließen Sie die Bearbeitung mit „OK“ ab.



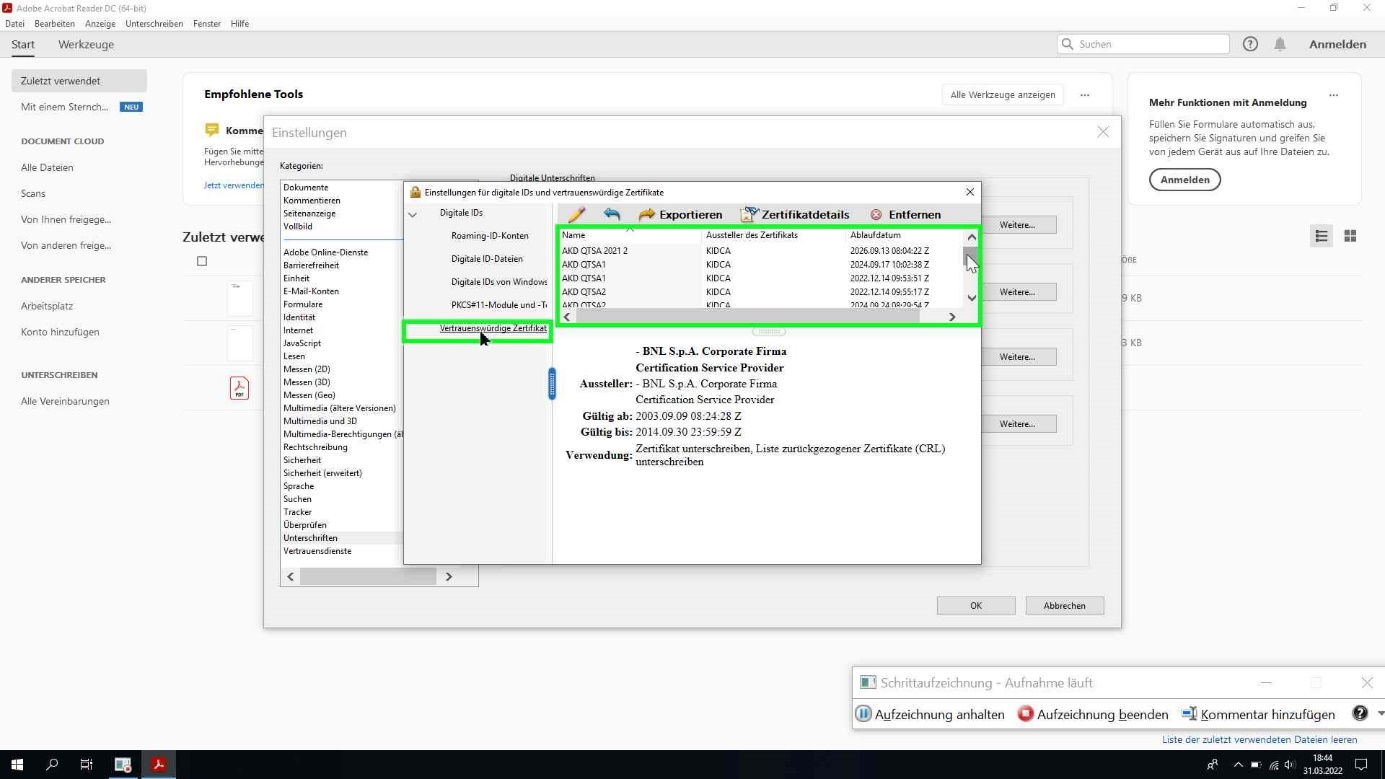
Nun wird das Zertifikat importiert.



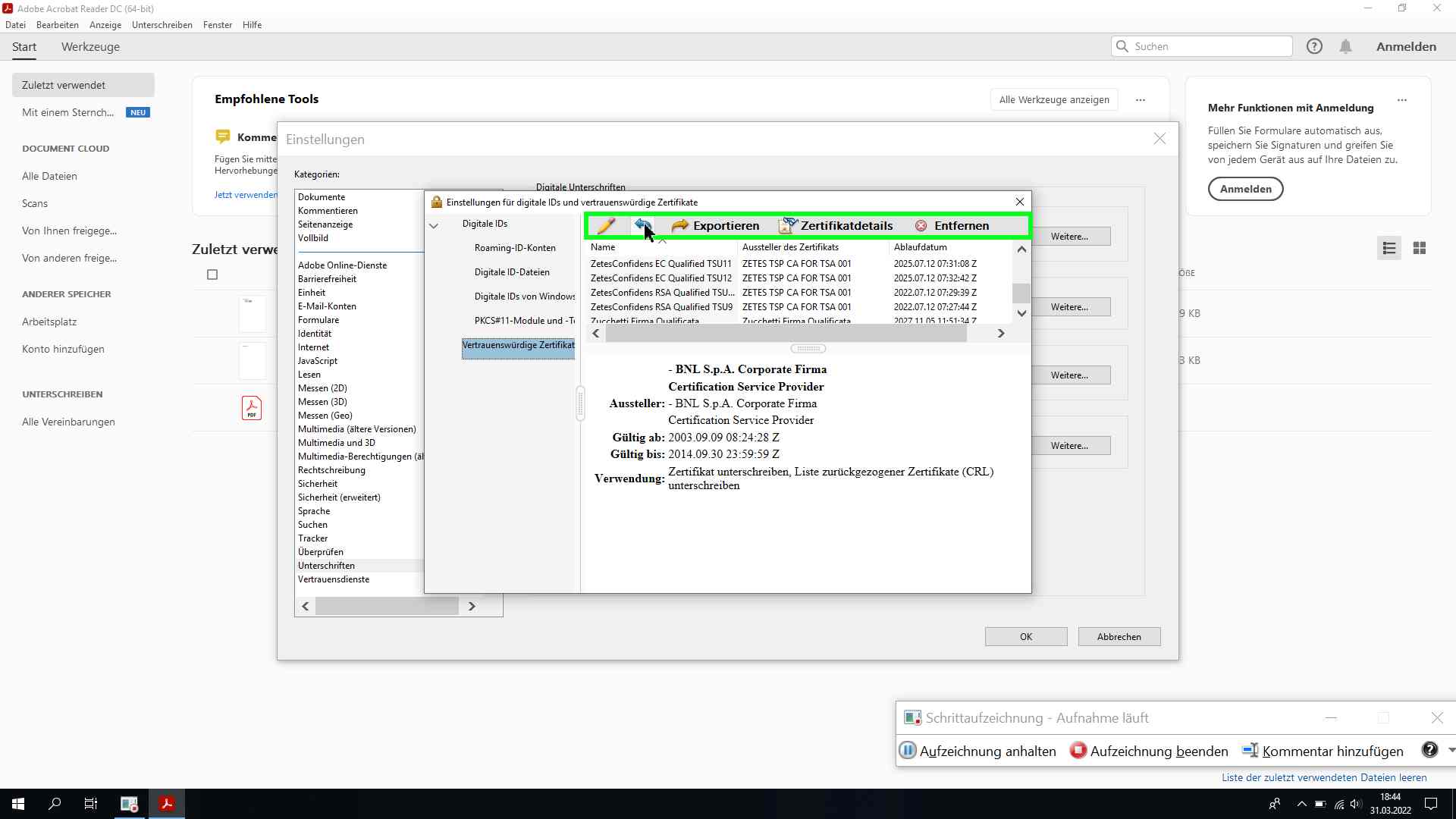
Das Meldungsfenster nach dem Import kann geschlossen werden. Sollte das Zertifikat bereits vorhanden gewesen sein, weicht die Rückmeldung leicht vom gezeigten Bild ab.



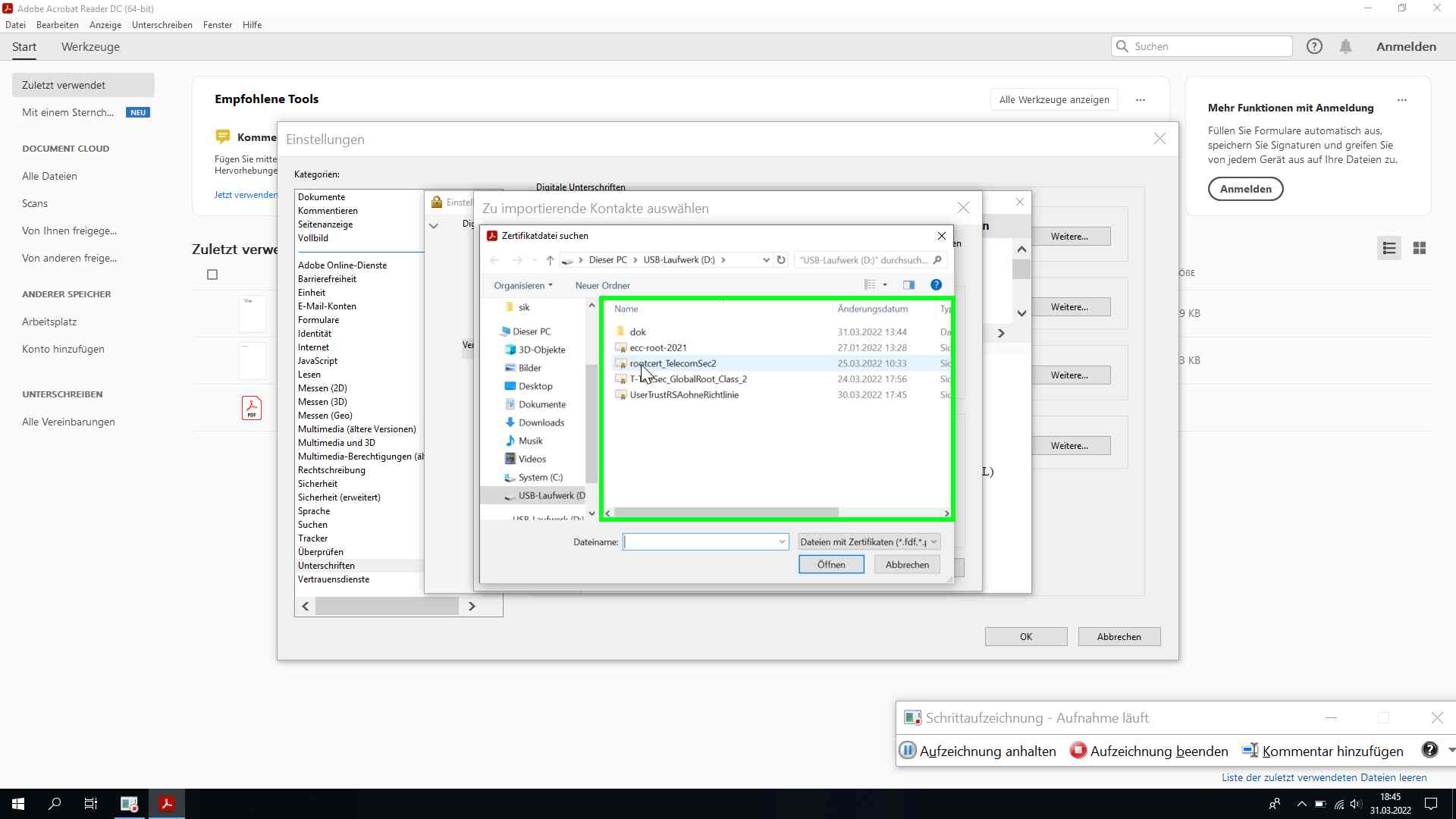
Import des Telekom-Sec2-Zertifikats



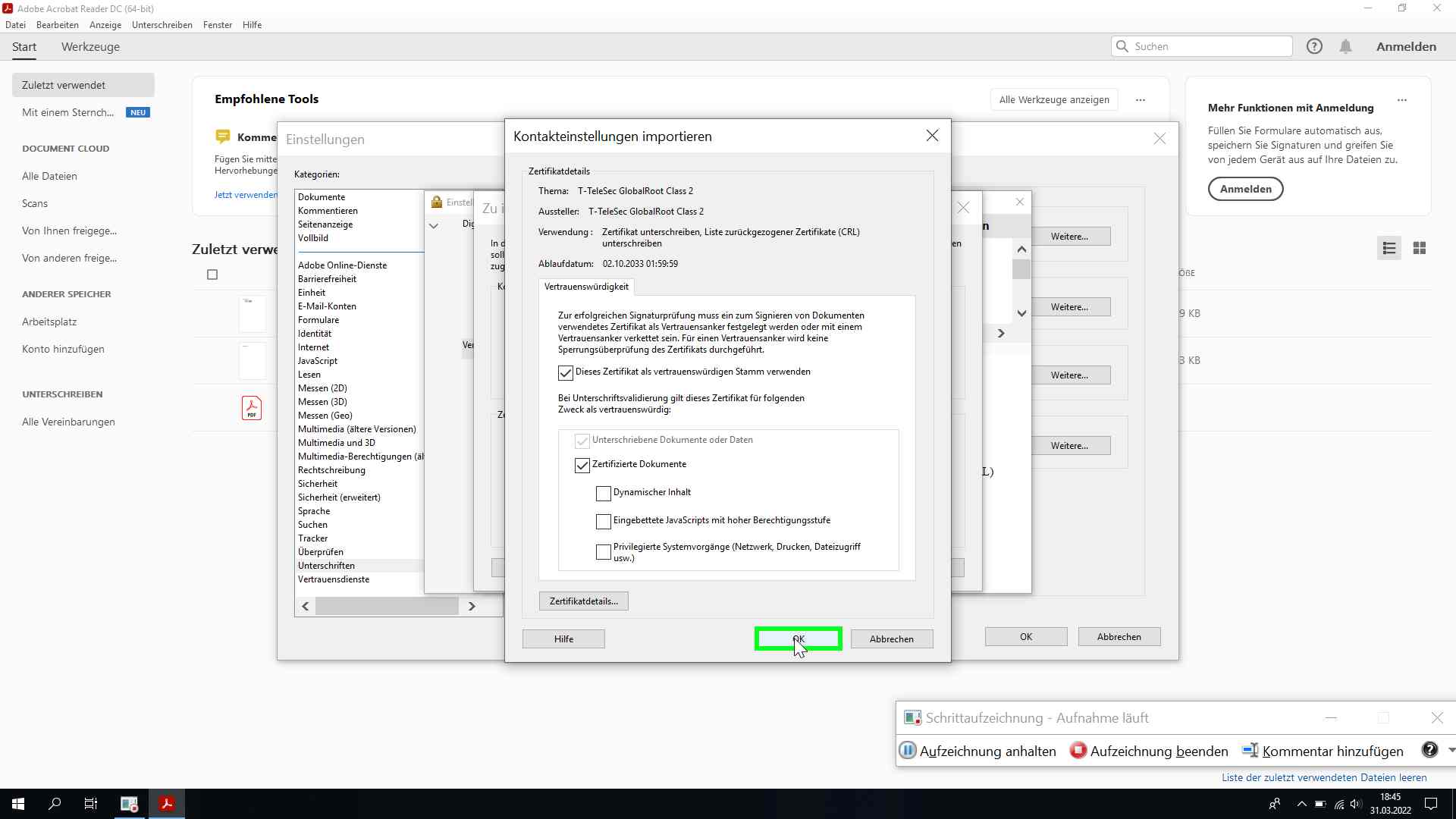
Klicken Sie auf den „Importieren“/ „blauen Linkspfeil“-Button



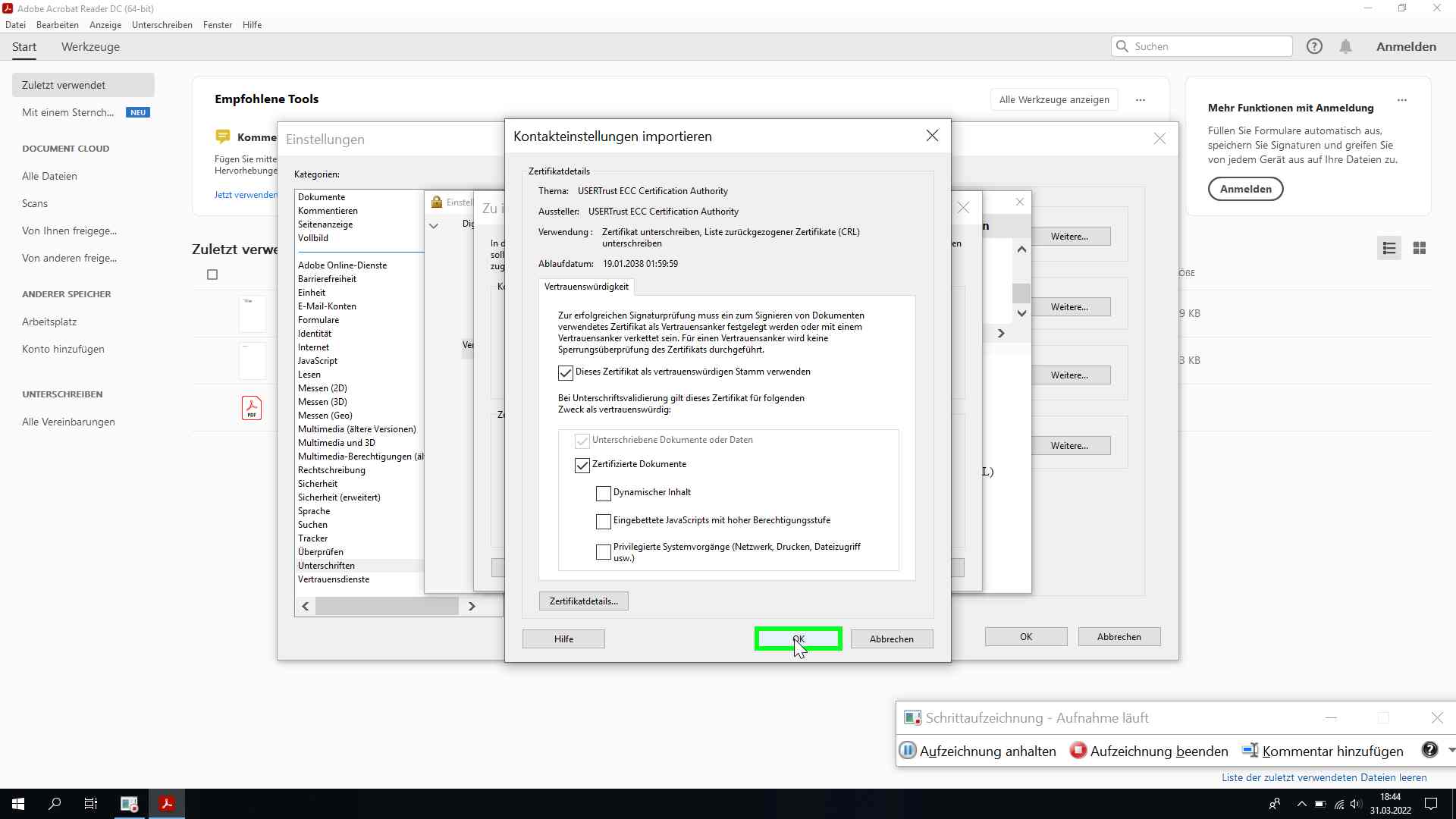
Suchen Sie mittels des Durchsuchen-Buttons die Datei „rootcert\_TelecomSec2.cer“, die Sie zuvor heruntergeladen haben (siehe oben) und öffnen es. (Wenn das Zertifikat nicht in der Auswahlliste angezeigt wird, den Filter im Feld „Dateiname“ durch die Eingabe von „\*.cer“ ändern.)



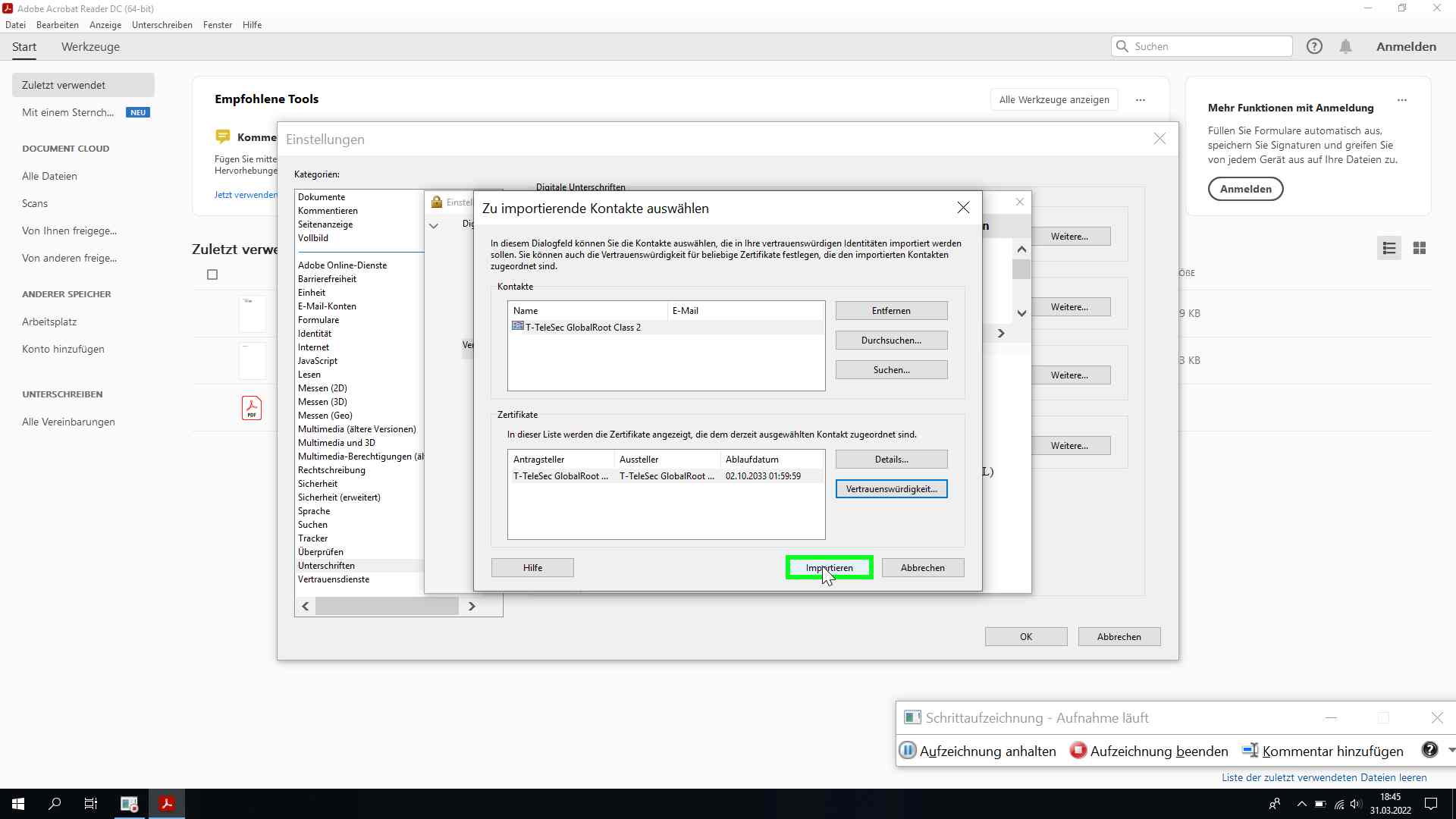
Nachdem Sie die Zertifikatdatei zunächst im oberen Bereich markiert haben, können Sie sie auch im unteren Bereich markieren und mit dem Button „Vertrauenswürdigkeit“ bearbeiten.



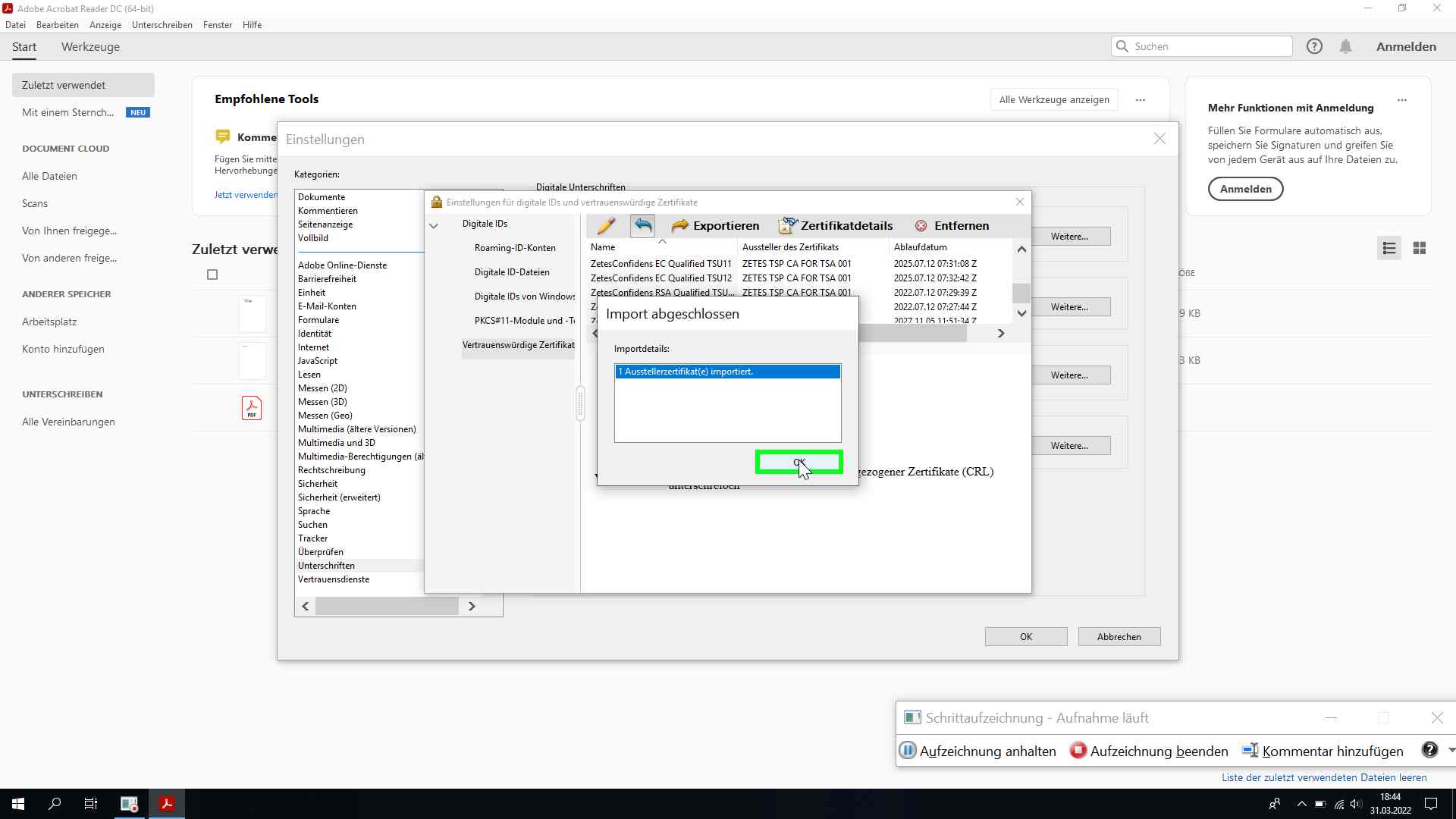
Markieren Sie dieses Zertifikat für „Dieses Zertifikat als vertrauenswürdigen Stamm verwenden“ und setzen danach die Option „“Zertifizierte Dokumente“. Schließen Sie die Bearbeitung mit „OK“ ab.



Nun wird das Zertifikat importiert.



Das Meldungsfenster nach dem Import kann geschlossen werden. Sollte das Zertifikat bereits vorhanden gewesen sein, weicht die Rückmeldung leicht vom gezeigten Bild ab.



**[Noch T-TeleSec\_GlobalRoot\_Class hier einfügen ]**

Sicherheitseinstellungen der TU Dresden einstellen

**[Sicherheitseinstellungen TU hier einfügen]**

<https://tu-dresden.de/zih/ressourcen/dateien/dienste/arbeitsumgebung/e_mail/dateien/tu_dresden_adobe_security>

**[Überprüfen in Testdokument infügen]**

**[Prüfen einer Unterschrift einfügen]**