

Anleitung zur Prüfung der digitalen Signatur mit Adobe Reader XI (bzw. X)

Mit Hilfe dieser Anleitung können Sie die digitale Signatur des Mitteilungsschreibens überprüfen. Die Erläuterung erfolgt am Beispiel von Microsoft Windows 10 und Internet Explorer 11.

Aufgrund der Vielzahl der unterschiedlichen am Markt vorhandenen Betriebssysteme und Browser können wir die Anleitung leider nicht für alle möglichen Varianten zur Verfügung stellen. Wir bitten um Ihr Verständnis.

Bitte beachten Sie folgenden Hinweis:

Bei Mitteilungsschreiben für Anträge, die ab dem **23. Oktober 2019** gestellt wurden, wählen Sie bitte - abweichend von der nachfolgenden Beschreibung - die folgenden Zertifikate aus:

Bei den Bearbeitungsschritten I. (2) – (5) sowie II. (6) – (9) :

Root CA Zertifikate

> Bundesbank Root CA 2015 II

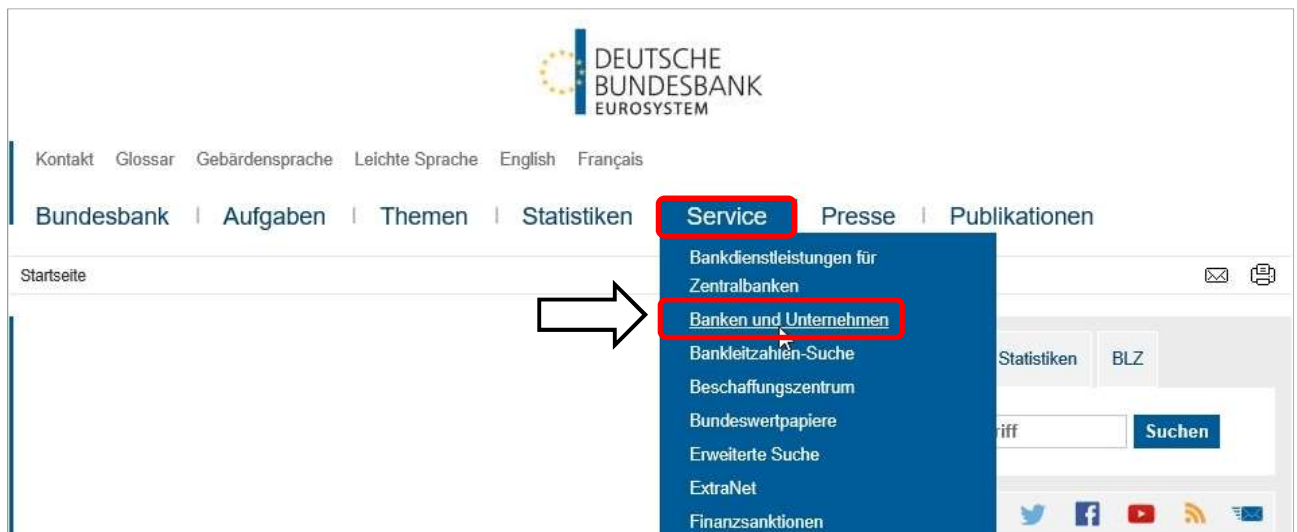
Bei den Bearbeitungsschritten I. (6) – (8) sowie II. (10) – (13):

Zertifikate der CA für Digitale Signatur

> CA for Digital Signature 2019

I. Installieren der Zertifikate

- (1) Auf der Homepage der Deutschen Bundesbank (www.bundesbank.de) unter **Service** → **Banken und Unternehmen** auswählen.



- (2) Den Auswahlpunkt **PKI** auswählen.



- (3) **Bundesbank Root CA 2014 I** auswählen.

Bankdienstleistungen für Zentralbanken

Banken und Unternehmen

- BBS
- EBS
- CAP
- Gläubigerversammlung
- KEV
- OMTOS
- PKI
- CP und CPS
- Erläuterungen
- Selbstbesicherung

- Bankleitzahlen-Suche
- Beschaffungszentrum
- Bundeswertpapiere
- Erweiterte Suche
- ExtraNet
- Finanzsanktionen
- Immobilienmanagement
- Mediathek
- Meldewesen
- Mitarbeiter/-innen der Bundesbank
- Newsletter
- Schlichtungsstelle
- Schule und Bildung
- Termine
- Weiterführende Links

Bundesbank Root CA 2014 I

Das Zertifikat ist mit dem Algorithmus SHA-1 selbstsigniert und hat eine Gültigkeitsdauer von zwölf Jahren. Der dem Root-CA-Zertifikat zugrundeliegende Schlüssel hat eine Länge von 4096 bit und wurde mit dem RSA Algorithmus generiert. Der Zertifikatsstandard bezieht sich auf das X.509v3-1996 Format. Das Zeitformat ist UTC (Universal Time Coordinated).

Das Zertifikat erlaubt die Nutzung des Schlüssels ausschließlich zur Signatur von Zertifikaten und Widerrufslisten. Zur eindeutigen Identifikation der Bundesbank Root CA 2014 I wird folgender Name (X.500-Distinguished-Names) verwendet.

Suche Statistiken BLZ

Suchbegriff **Suchen**

Zertifikat

Allgemein Details Zertifizierungspfad

Anzeigen: <Alle>

Feld	Wert
Seriennummer	00 b1 7e 3e bc 22 77 cd 0f
Signaturalgorithmus	sha1RSA
Signaturhashalgorithmus	sha1
Aussteller	pk@bundesbank.de, Bundesb...
Gültig ab	Montag, 22. Dezember 2014 1...
Gültig bis	Samstag, 19. Dezember 2026 ...
Antragsteller	pk@bundesbank.de, Bundesb...
Öffentlicher Schlüssel	RSA (4096 Bits)

E = pk@bundesbank.de
 CN = Bundesbank Root CA 2014 I for Central Bank Issues
 OU = Bundesbank PKI
 O = Bundesbank
 C = DE

Eigenschaften bearbeiten... In Datei kopieren...

Weitere Informationen über [Zertifikatdetails](#)

OK

Der Fingerprint: Als Sicherungsanker für das eigene bzw. auch andere Zertifikate dieser PKI fungiert die Bundesbank Root CA 2014 I. Sobald Sie der Root-CA vertrauen, vertrauen Sie auch allen Zertifikaten, die unter dieser Root-CA ausgestellt wurden. Daher muss unbedingt der Fingerprint der Root-CA vor Beginn des Verfahrens geprüft werden. Der Fingerprint befindet sich in der Regel auch auf den Briefen der Zertifizierungsstelle.

Fingerprint

Zertifikatsname	Hashverfahren	Fingerprint
Bundesbank Root CA 2014 I	SHA-1	54 30 71 d1 8a d5 b2 8c f2 85 3f e5 46 2f 26 67 1c 84 34 3b

Sicherheitszertifikat der Bundesbank Root CA 2014 I

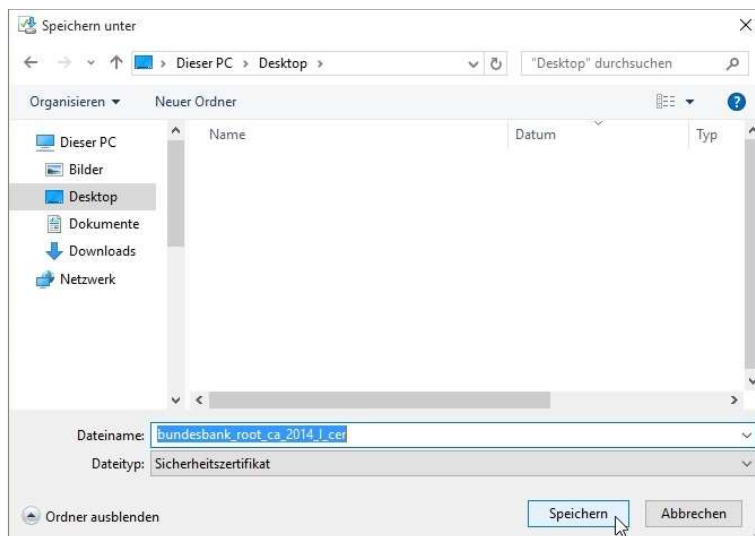
Bundesbank Root CA 2014 I
2 KB, File Recorder

Möchten Sie „bundesbank_root_ca_2014_1_cer.cer“ (1,85 KB) von „bundesbank.de“ öffnen oder speichern?

Öffnen Speichern **Speichern unter** Speichern und öffnen

- (4) Das Zertifikat **Bundesbank Root CA 2014 I** mit der rechten Maustaste anklicken, dann **Ziel speichern unter...** auswählen oder mit der linken Maustaste anklicken und unter **Speichern** auf **Speichern unter** klicken.

- (5) Als Speicherort einen lokalen Datenträger auswählen (z. B.: c:\temp) oder auf dem Desktop speichern.



- (6) Danach sind die Schritte (3) bis (5) auch für das zweite Zertifikat durchzuführen: Wählen Sie hierfür bitte **CA for Digital Signature 2015** aus.

Startseite > Service > Service für Banken und Unternehmen > PKI- Public Key Infrastructure

Bankdienstleistungen für Zentralbanken

Banken und Unternehmen

- BBS
- EBS
- CAP
- Gläubigerversammlung
- KEV
- OMTOS
- PKI**
- CP und CPS
- Erläuterungen
- Selbstbesicherung

Bankleitzahlen-Suche

Beschaffungszentrum

Bundeswertpapiere

Erweiterte Suche

ExtraNet

Finanzsanktionen

Immobilienmanagement

Mediathek

Meldewesen

Mitarbeiter/-innen der Bundesbank

Newsletter

Schlichtungsstelle

Schule und Bildung

Public Key Infrastructure (PKI)

Die Deutsche Bundesbank betreibt am Standort Düsseldorf eine Public Key Infrastructure (PKI). Für diese PKI wird eine zweistufige Zertifizierungsstruktur mit selbstsignierten Root-Zertifikaten verwendet. Die Root-CA's zertifizieren ausschließlich nachgelagerte fachliche CA's. Die Deutsche Bundesbank ist Mitglied der TeleTrust European Bridge CA (EBCA). Die von der PKI der Deutschen Bundesbank ausgestellten Zertifikate erfüllen die Voraussetzungen der fortgeschrittenen Signatur nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG).

Root CA Zertifikate

- Bundesbank Root CA 2015 II ▶
- Bundesbank Root CA 2014 I ▶
- Bundesbank Root CA 2010 ▶

Zertifikate der CA für E-Mailsicherheit

- CA for Email-Security 2014 ▶
- Benutzerzertifikate ▶

Zertifikate der CA für User Authentisierung

- CA for User Authentication 2015 ▶
- CA for User Authentication 2013 ▶

Zertifikate der CA für Digitale Signatur

- CA for Digital Signature 2015 ▶**
- CA for Digital Signature 2012 ▶

Suche | Statistiken | BLZ

Suchbegriff

Adresse

Postanschrift
Deutsche Bundesbank

Kontakt

PKI Services

- [Telefon](#)
- [Fax](#)
- [E-Mail](#)

European Bridge CA

Bankdienstleistungen für Zentralbanken

Banken und Unternehmen

- BBS
- EBS
- CAP
- Gläubigerversammlung
- KEV
- OMTOS
- PKI**
 - CP und CPS
 - Erläuterungen
- Selbstbesicherung
- Bankleitzahlen-Suche
- Beschaffungszentrum
- Bundeswertpapiere
- Erweiterte Suche
- ExtraNet
- Finanzsanktionen
- Immobilienmanagement
- Mediathek
- Meldewesen
- Mitarbeiter/-innen der Bundesbank
- Newsletter
- Schlichtungsstelle
- Schule und Bildung
- Termine
- Weiterführende Links

CA for Digital Signature 2015

Das Zertifikat ist mit dem Algorithmus SHA-1 von der Bundesbank Root CA 2014 I signiert und hat eine Gültigkeitsdauer von sechs Jahren. Der dem CA-Zertifikat zugrundeliegende Schlüssel hat eine Länge von 4096 bit und wurde mit dem RSA Algorithmus durch die Bundesbank Root CA 2014 I generiert. Der Zertifikatsstandard bezieht sich auf das X.509v3-1996 Format. Das Zeitformat ist UTC (Universal Time Coordinated).

Das Zertifikat erlaubt die Nutzung des Schlüssels ausschließlich zur Signatur von Zertifikaten und Widerrufslisten. Zur eindeutigen Identifikation der Bundesbank CA for Digital Signature 2015 wird folgender Name (X.500-Distinguished-Names) verwendet:

Suche | Statistiken | BLZ

Suchbegriff **Suchen**

Zertifikat

Alle | Details | Zertifizierungspfad

Anzeigen: <Alle>

Feld	Wert
Seriennummer	01
Signaturalgorithmus	sha1RSA
Signaturhashalgorithmus	sha1
Aussteller	pki@bundesbank.de, Bundesb...
Gültig ab	Freitag, 2. Januar 2015 14:04...
Gültig bis	Donnerstag, 31. Dezember 20...
Antragsteller	pki@bundesbank.de, CA for D...
Öffentlicher Schlüssel	RSA (4096 Bits)

E = pki@bundesbank.de
 CN = CA for Digital Signature 2015
 OU = Digital Signature Certificates
 O = Bundesbank
 C = DE

[Eigenschaften bearbeiten...](#) [In Datei kopieren...](#)

Weitere Informationen über [Zertifikatdetails](#)

OK

Fingerprint

Zertifikat	Hashverfahren	Fingerprint
CA for Digital Signature 2015	SHA-1	48 d3 dd 08 1b 87 75 9a 96 10 70 25 85 af 73 c3 89 60 fa df

Sicherheitszertifikat der CA for Digital Signature 2015

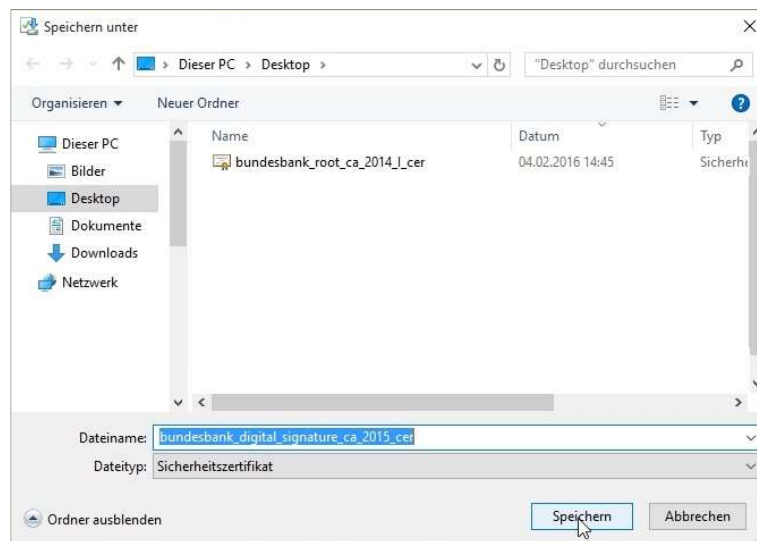
 CA for Digital Signature 2015 CRL
2 KB, FileType: cer

Möchten Sie „bundesbank_digital_signature_ca_2015_cer.cer“ (2,04 KB) von „bundesbank.de“ öffnen oder speichern?

Öffnen Speichern Speichern unter... Speichern und öffnen

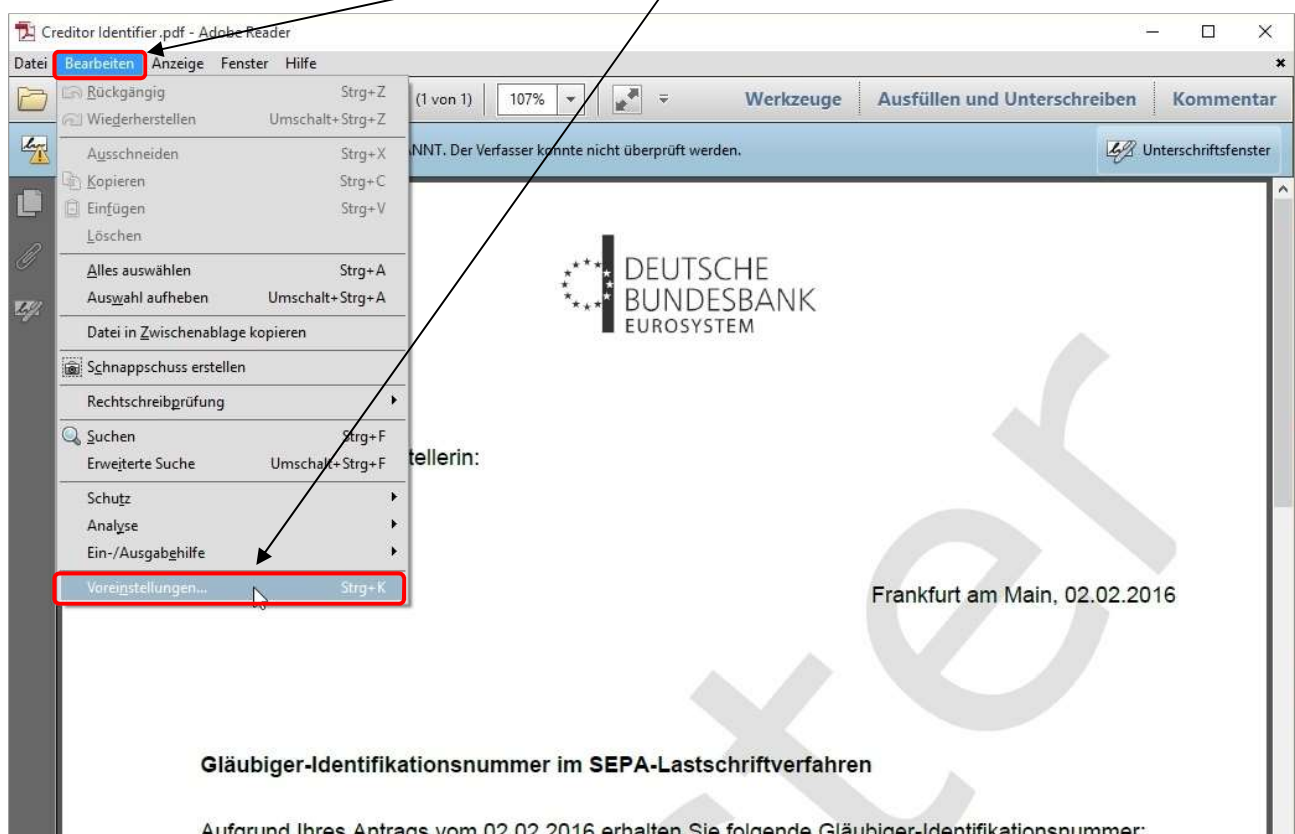
- (7) Das Zertifikat **CA for Digital Signature 2015 CRL** mit der rechten Maustaste anklicken, dann **Ziel speichern unter...** auswählen oder mit der linken Maustaste anklicken und unter **Speichern** auf **Speichern unter** klicken.

- (8) Als Speicherort einen lokalen Datenträger auswählen (z. B.: c:\temp) oder auf dem Desktop speichern.



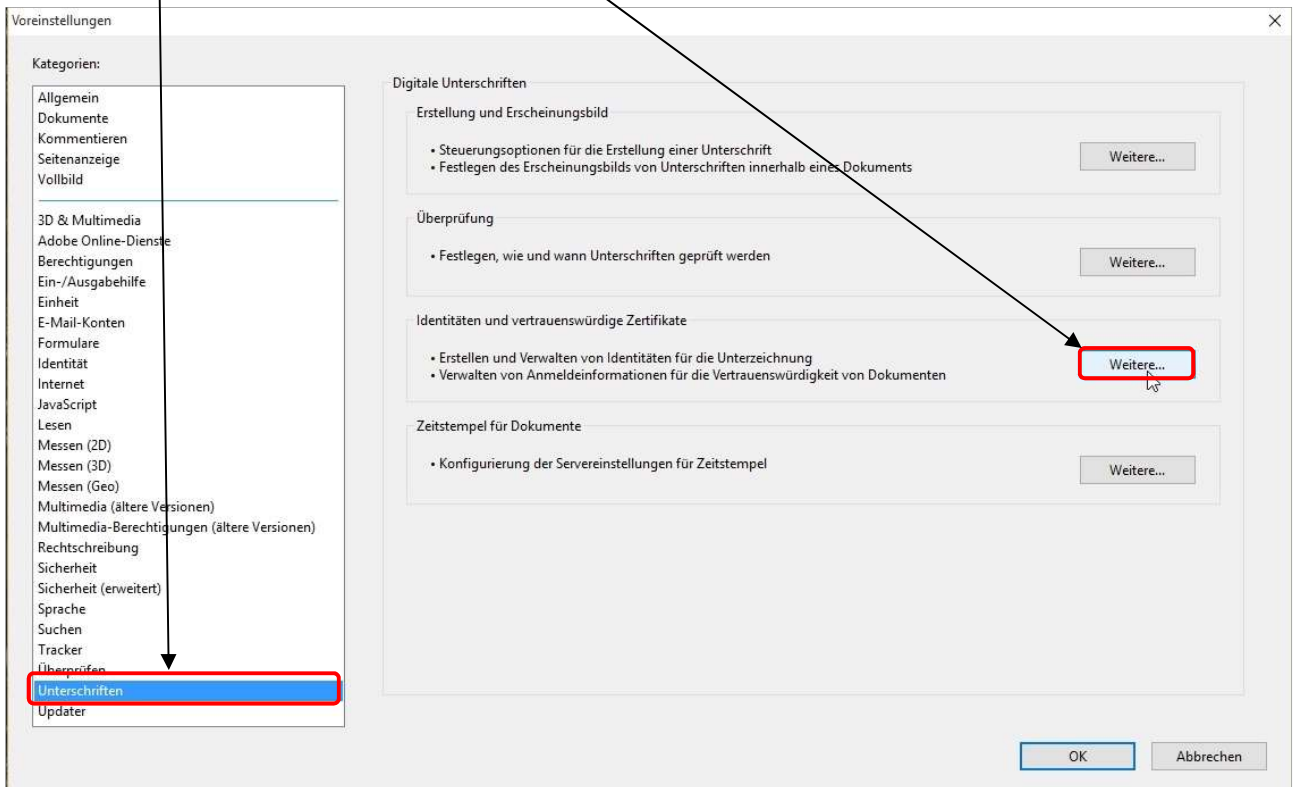
II. Zertifikate den vertrauenswürdigen Kontakten hinzufügen und Signatur überprüfen (am Beispiel der Adobe Reader Version XI.x)

- (1) Adobe **Reader** und Mitteilungsschreiben öffnen.
- (2) In der Menüleiste unter **Bearbeiten** → **Voreinstellungen...** wählen.

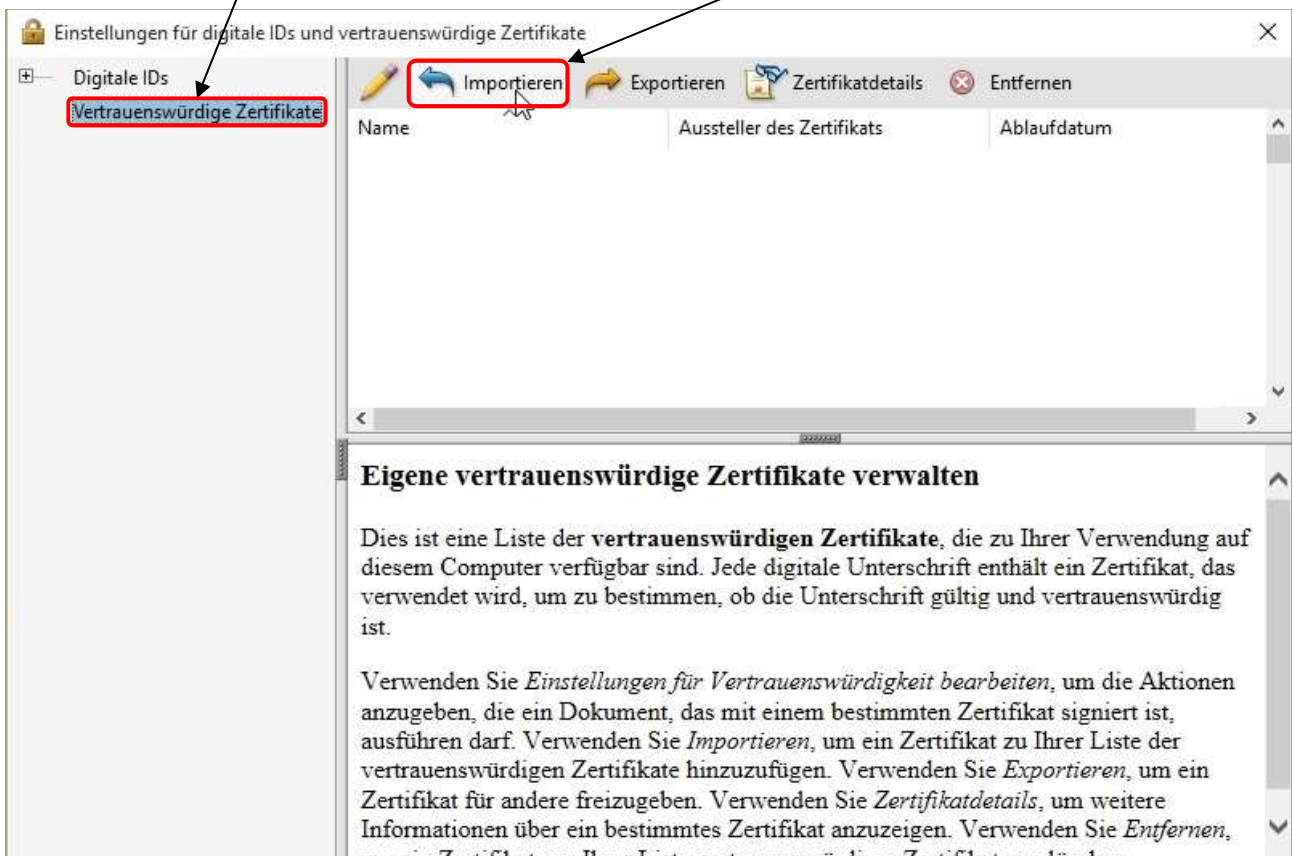


(Adobe Reader Version X:
unter **Bearbeiten** → **Schutz** → **Vertrauenswürdige Identitäten verwalten...** → „**Kontakte hinzufügen...**“ dann weiter mit (5))

(3) **Unterschriften** auswählen und dann bei „Identitäten und vertrauenswürdige Zertifikate“ auf **Weitere...** klicken.

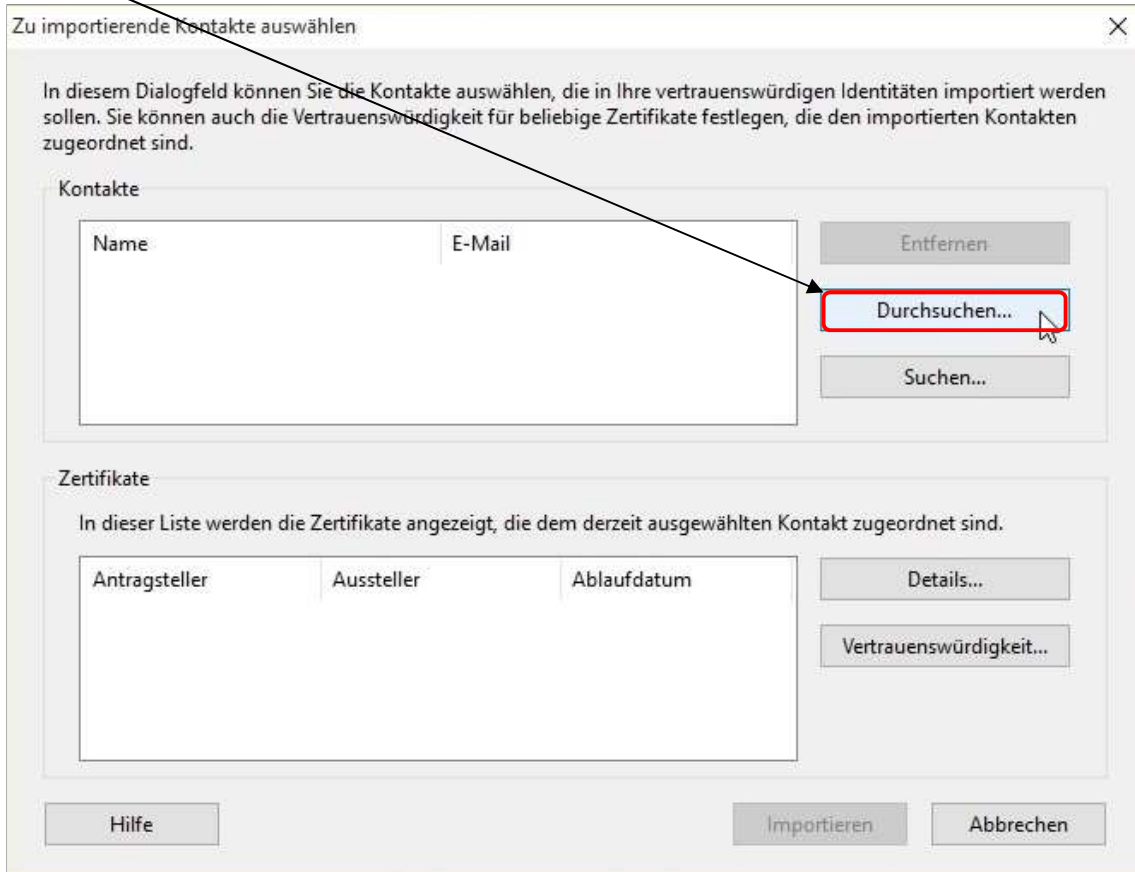


(4) **Vertrauenswürdige Zertifikate** und anschließend **Importieren** auswählen*).

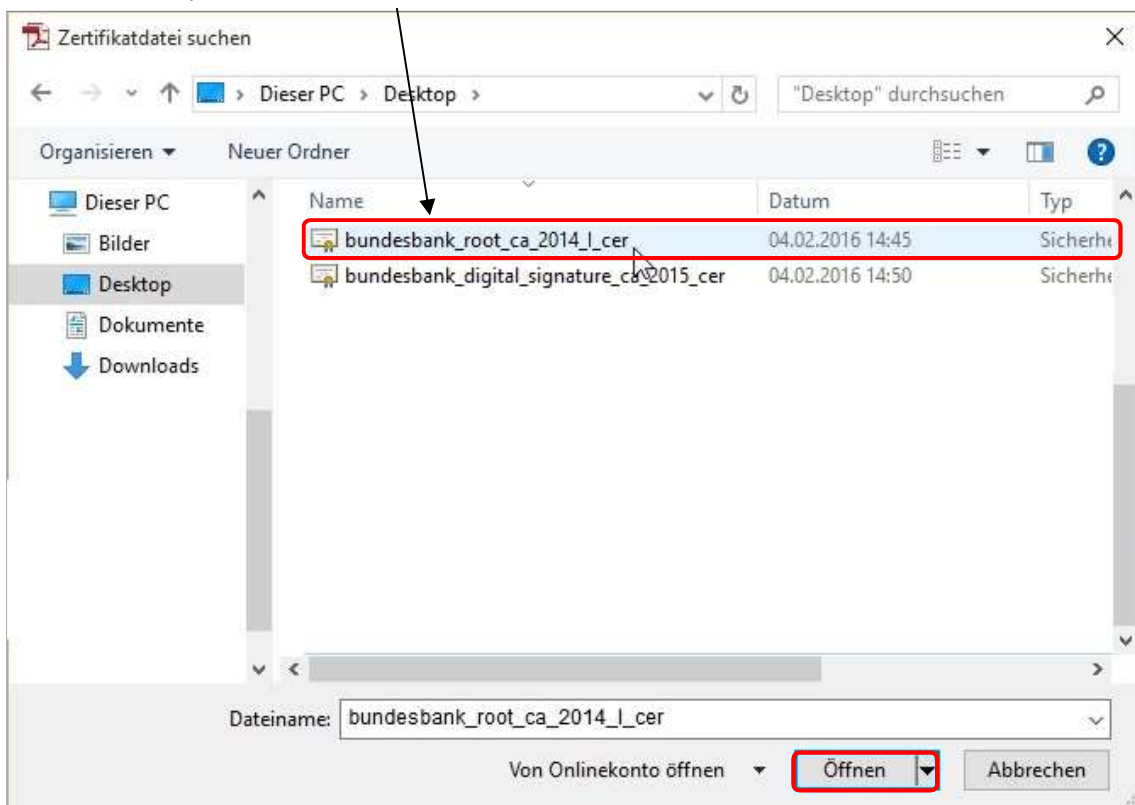


*) In Firmennetzwerken lassen unter Umständen Ihre firmeninternen Sicherheitseinstellungen diesen Import nicht zu. Zur Lösung setzen Sie sich bitte mit Ihrer IT in Verbindung.

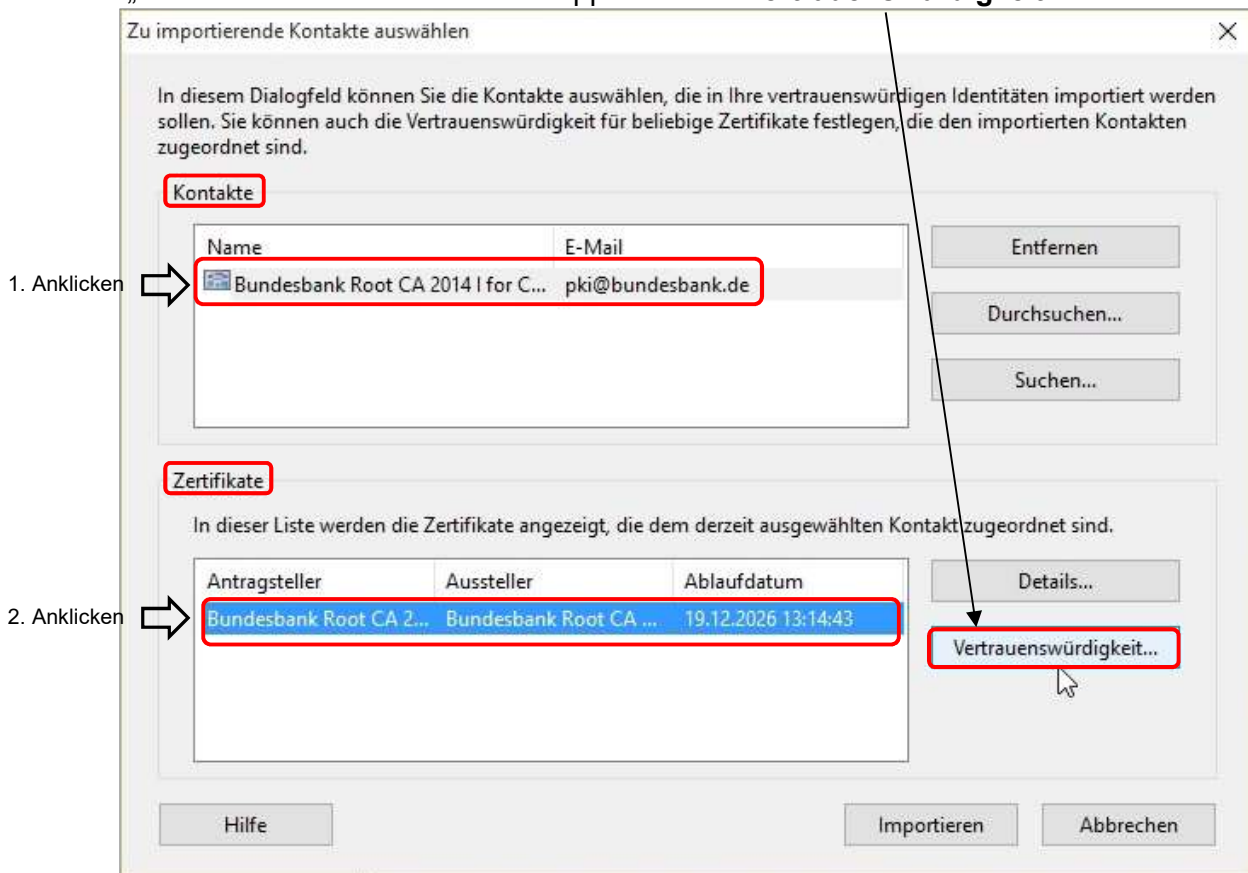
(5) Auf **Durchsuchen...** klicken.



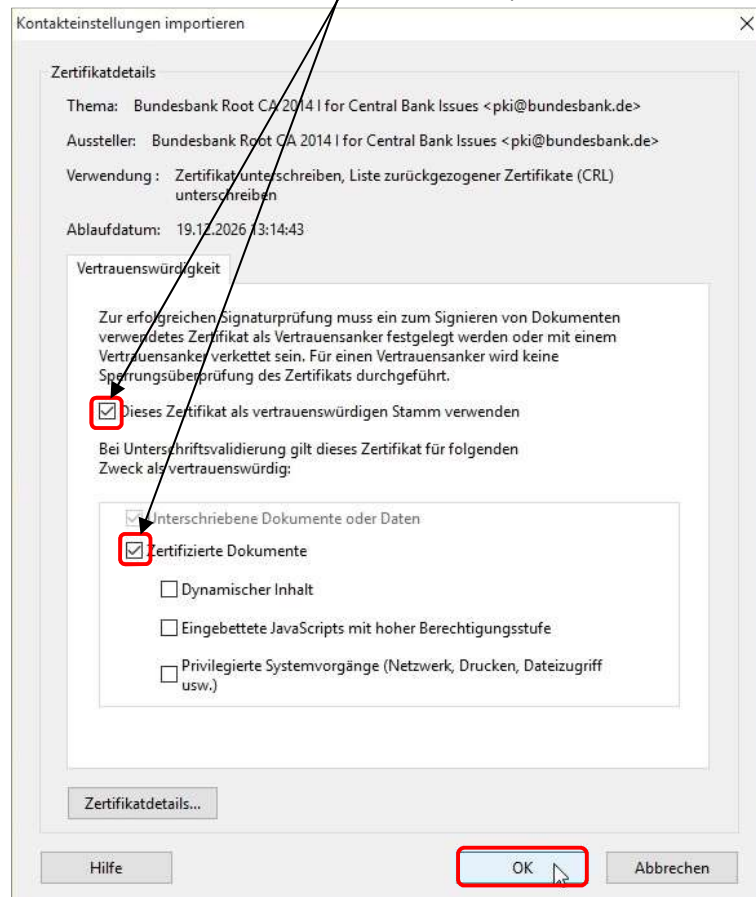
(6) Anschließend aus dem Verzeichnis, in dem die Zertifikate gespeichert wurden (z. B.: c:\temp oder Desktop), das erste Zertifikat mit Doppelklick auswählen oder mit Klick auf **Öffnen**.



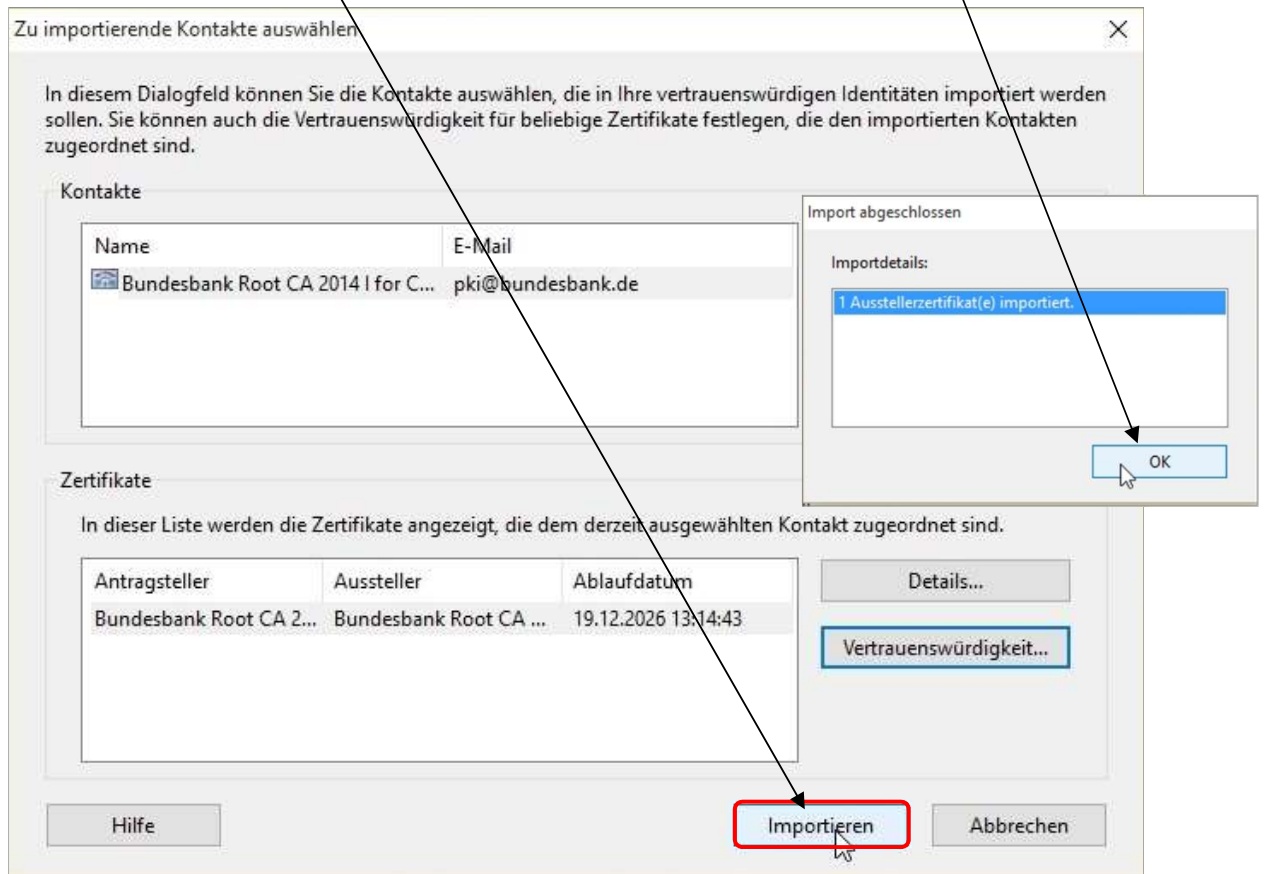
- (7) Bei „Kontakte“ das importierte Zertifikat auswählen, anschließend dieses unter „Zertifikate“ auswählen und mit Doppelklick auf **Vertrauenswürdigkeit...** bearbeiten.



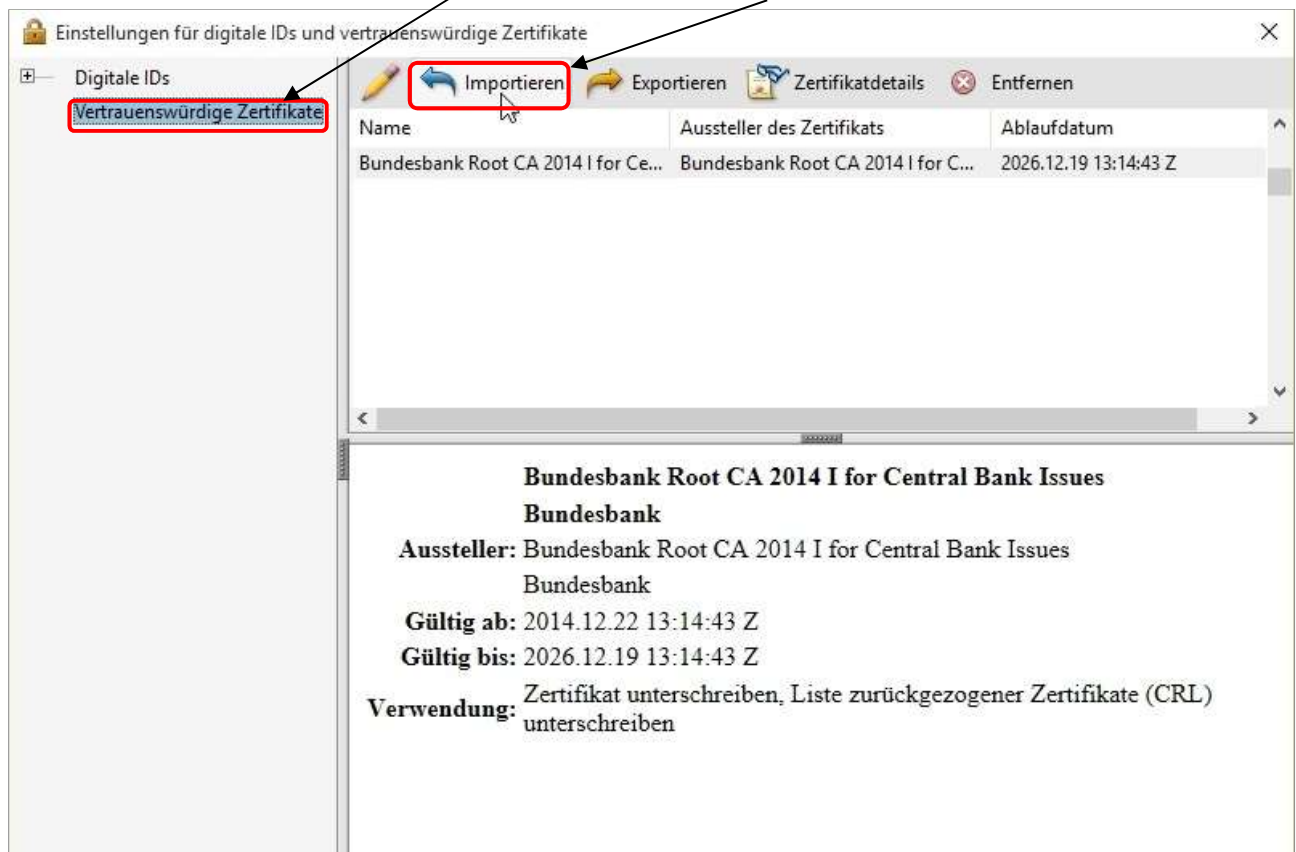
- (8) An den markierten Stellen bitte ein Häkchen setzen (falls dort keines vorhanden), dann auf **OK**.



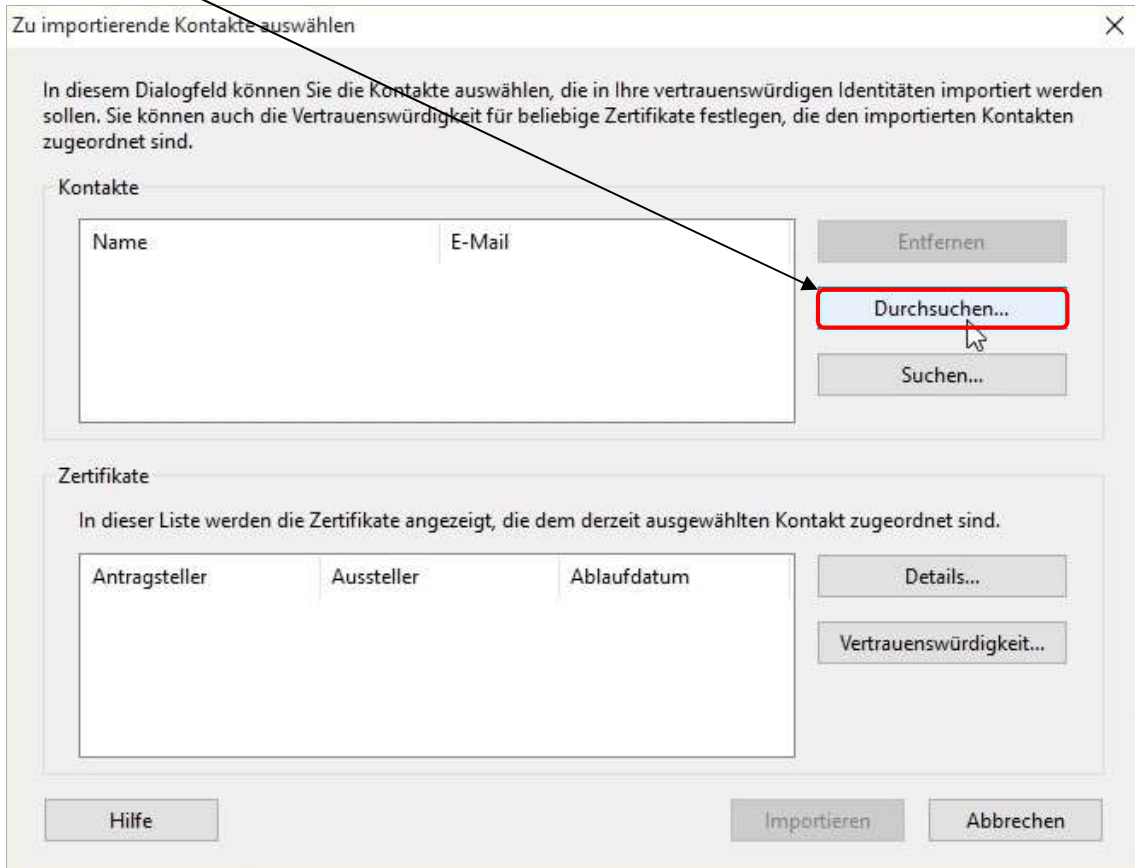
(9) Klicken Sie auf **Importieren**, anschließend Erfolgsmeldung „Import abgeschlossen“ bestätigen.



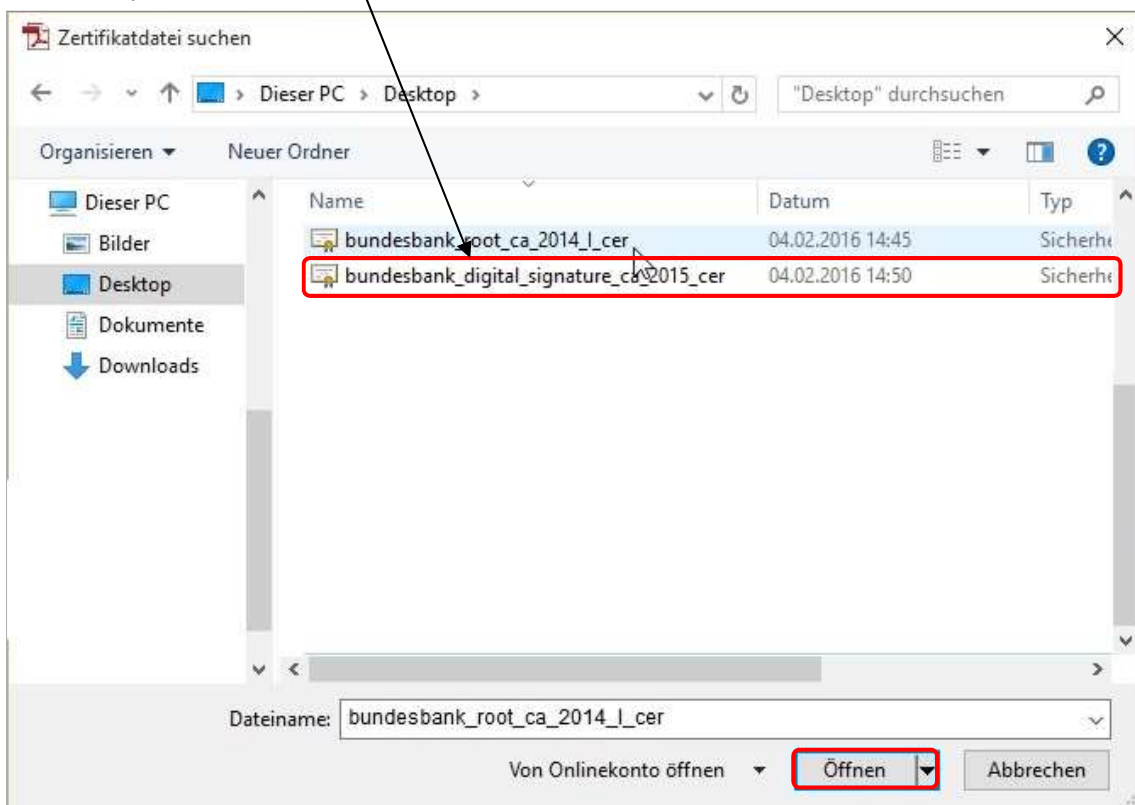
(10) Anschließend das zweite Zertifikat ebenfalls importieren wie nachfolgend bis (13) beschrieben: Wählen Sie unter **Vertrauenswürdige Zertifikate - Importieren**.



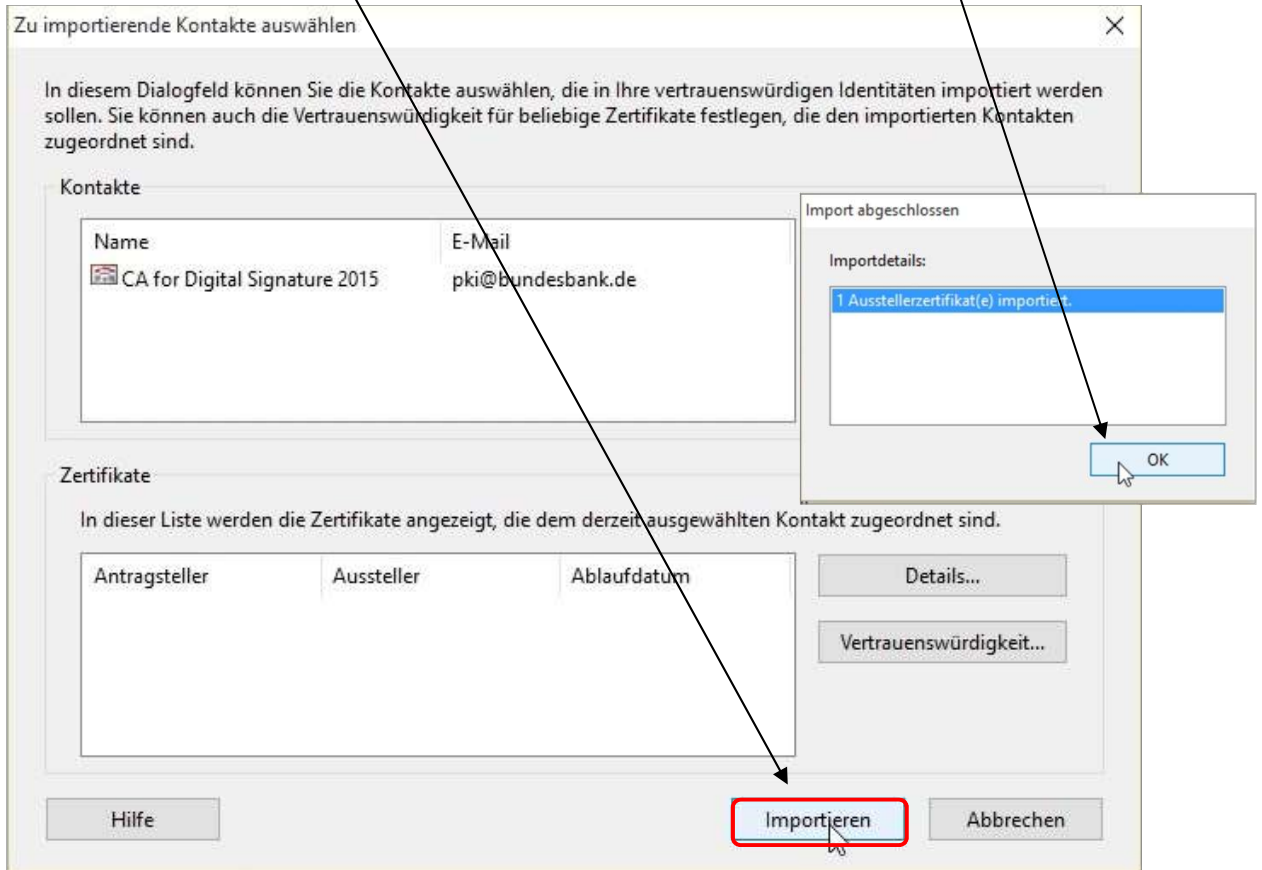
(11) Auf **Durchsuchen...** klicken.



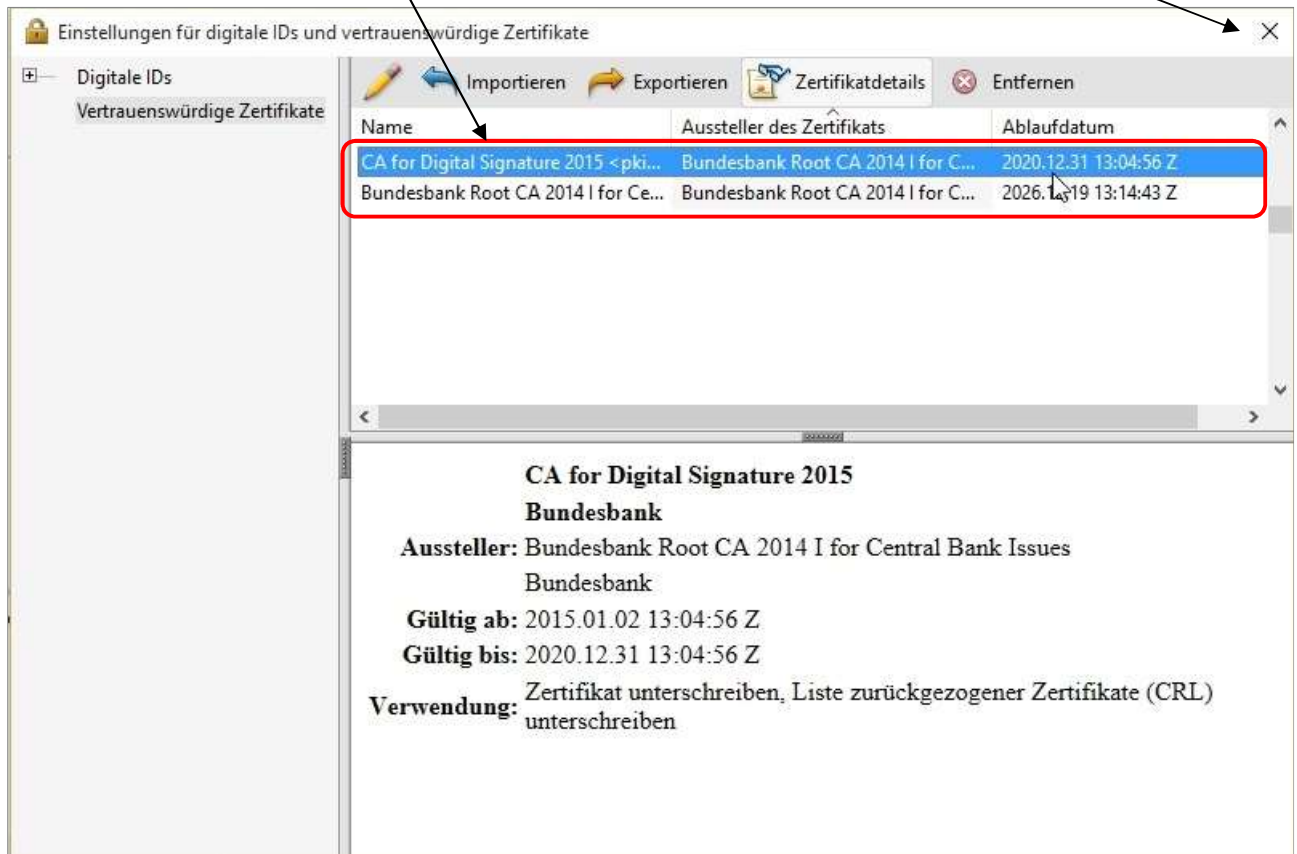
(12) Aus dem Verzeichnis, in dem die Zertifikate gespeichert wurden (z. B.: c:\temp oder Desktop), das zweite Zertifikat mit Doppelklick auswählen oder mit Klick auf **Öffnen**.



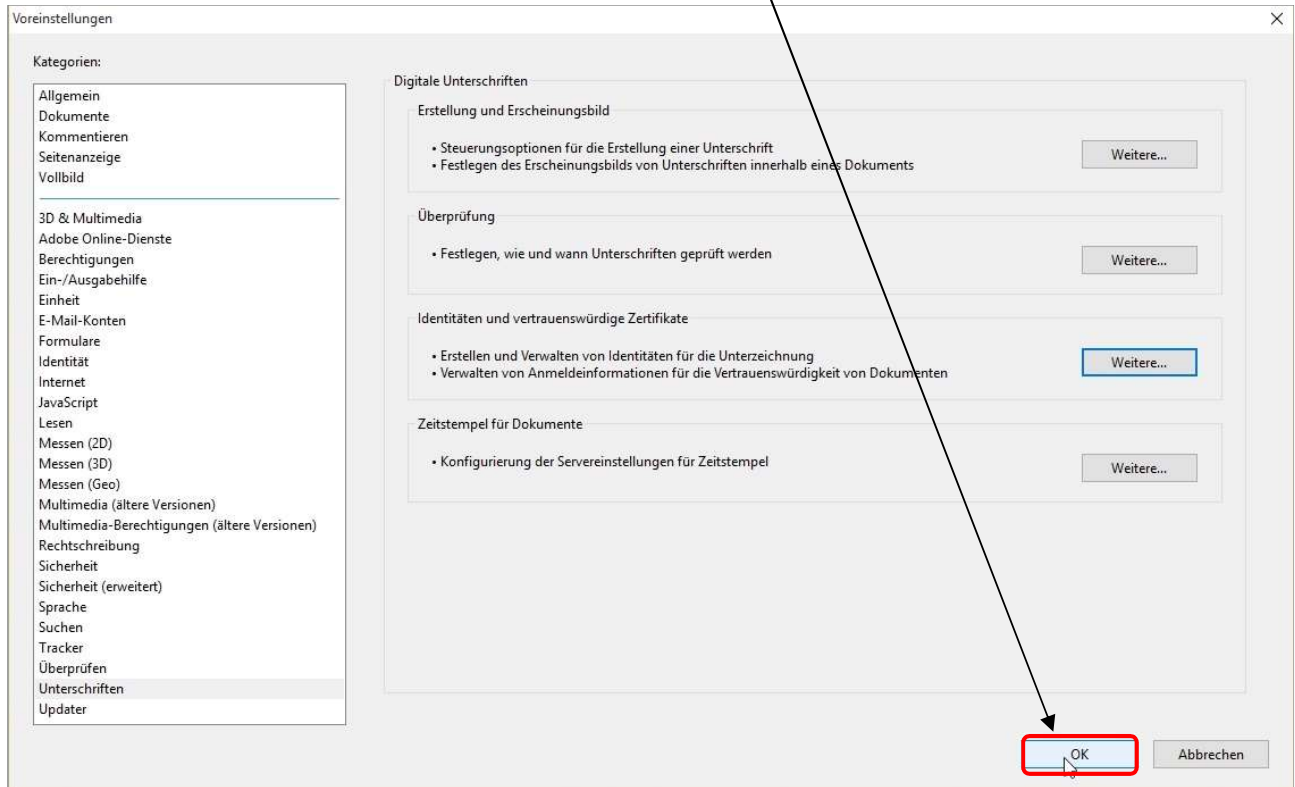
(13) Klicken Sie auf **Importieren**, anschließend Erfolgsmeldung „Import abgeschlossen“ bestätigen.



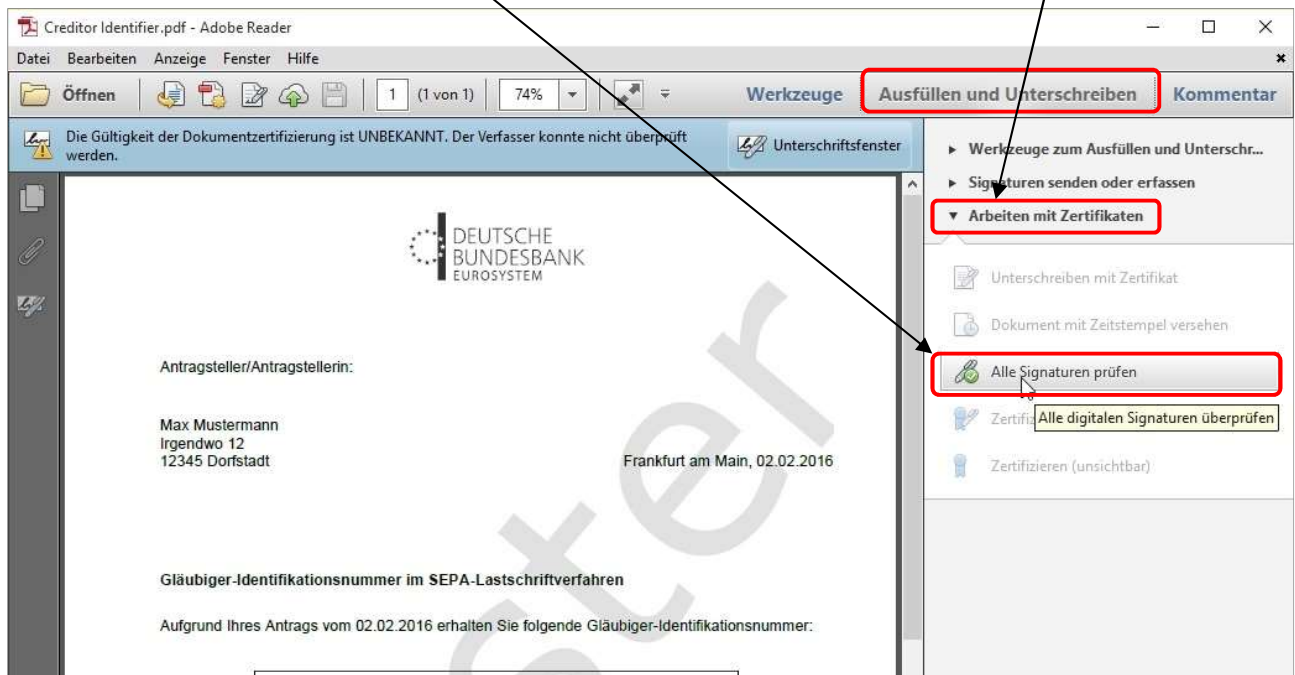
(14) Sie sehen die importierten Zertifikate, anschließend dieses Fenster schließen:



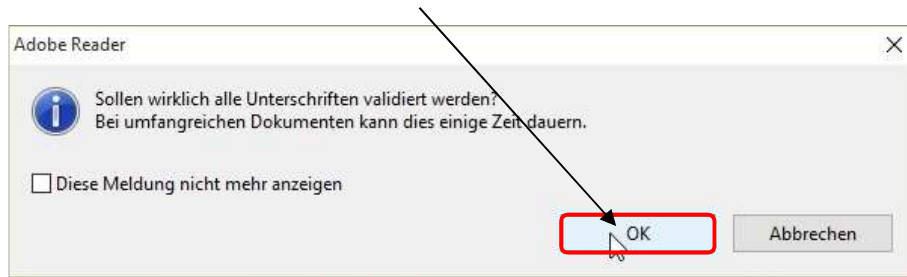
(15) Schließen Sie das Fenster „Voreinstellungen“ mit **OK**.



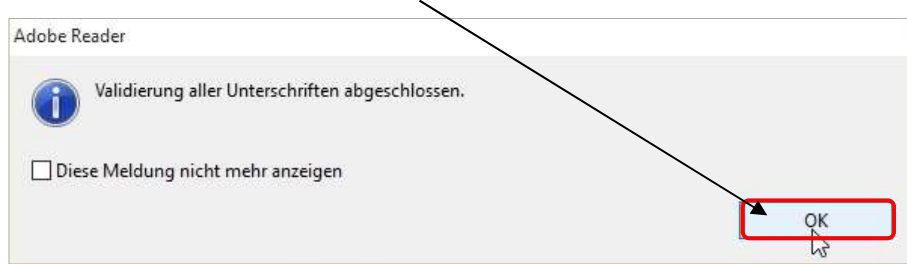
(16) Zur Überprüfung der Signatur unter **Ausfüllen und Unterschreiben - Arbeiten mit Zertifikaten**, dann **Alle Signaturen prüfen** auswählen.



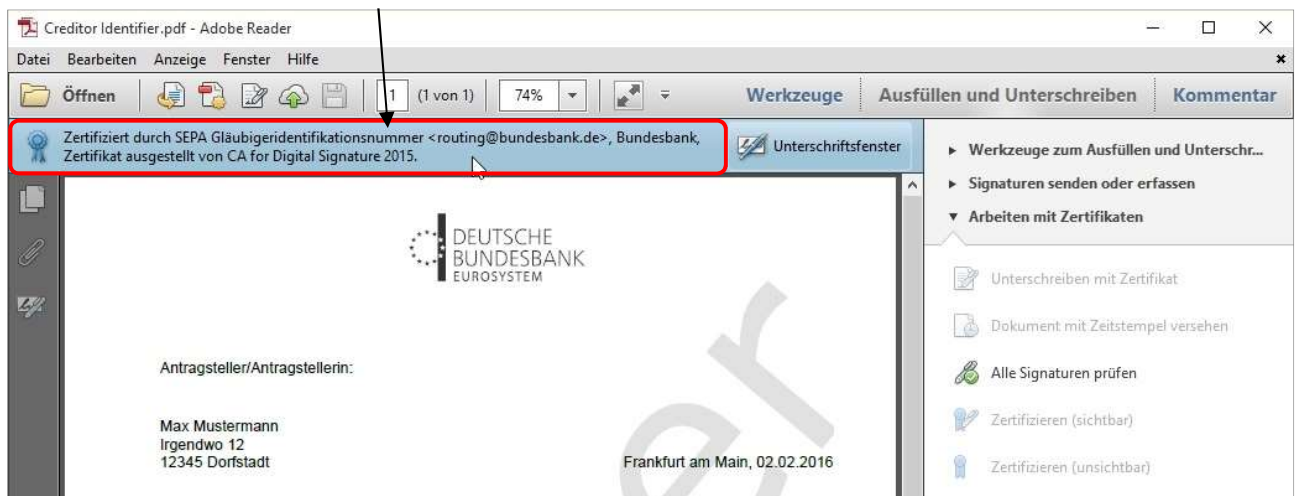
(17) Die Validierung der Signaturen mit **OK** bestätigen.



(18) Den Abschluss der Validierung mit **OK** bestätigen.



(19) Sie erhalten das Ergebnis der Signaturprüfung:
„Zertifiziert durch SEPA Gläubigeridentifikationsnummer <routing@bundesbank.de>...“



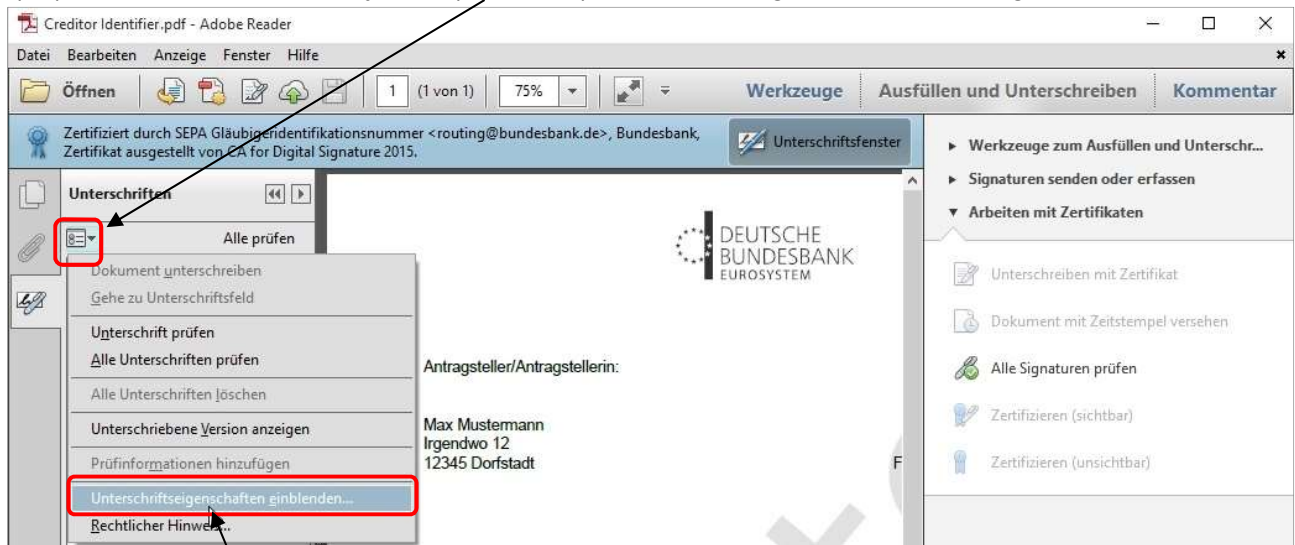
(20) Weitere Informationen zur digitalen Unterschrift erhalten Sie mit Klick auf **Unterschriftsfenster**.



(21) Diese Zeile durch Anklicken auswählen.

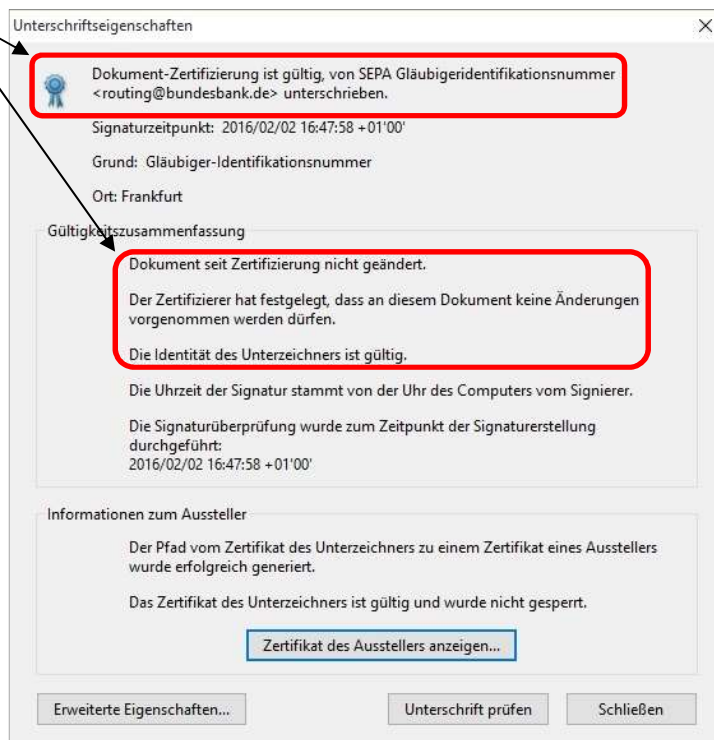


(22) Durch Klick auf das Symbol (Optionen) öffnet sich folgende Auswahlmöglichkeit:



Unterschriftseigenschaften einblenden... auswählen.

Diese Meldungen müssen erscheinen:



(23) Die heruntergeladenen und gespeicherten Zertifikate (z. B. auf: c:\temp oder Desktop) können gelöscht werden.