Anleitung zur Prüfung der digitalen Signatur mit Adobe Acrobat Pro (Version 2023)

Mit Hilfe dieser Anleitung können Sie die digitale Signatur des Mitteilungsschreibens überprüfen.
Die Erläuterung erfolgt am Beispiel von Microsoft Windows 10 und dem Browser Microsoft Edge.

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.

1 Installieren der Zertifikate

1.1 Das Zertifikat Bundesbank Root CA 2015 II

1. Auf der Homepage der Deutschen Bundesbank (www.bundesbank.de) den Link **Service ➔ Banken und Unternehmen** auswählen:

Abbildung 1: Auswahl Service – Banken und Unternehmen

2. Den Auswahlpunkt **Public Key Infrastructure (PKI)** auswählen:

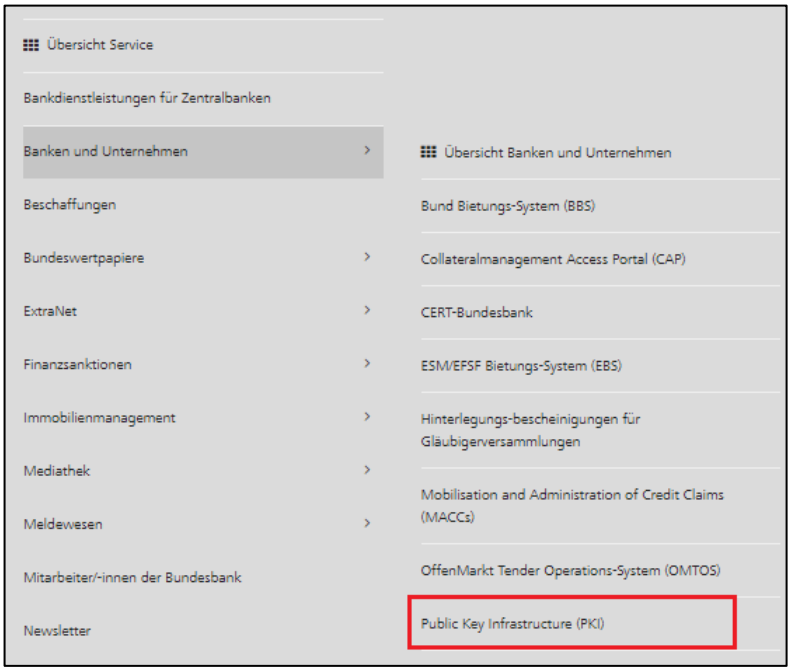


Abbildung 2: Auswahl Public Key Infrastructure (PKI)

3. Das Zertifikat **Bundesbank Root CA 2015 II** auswählen

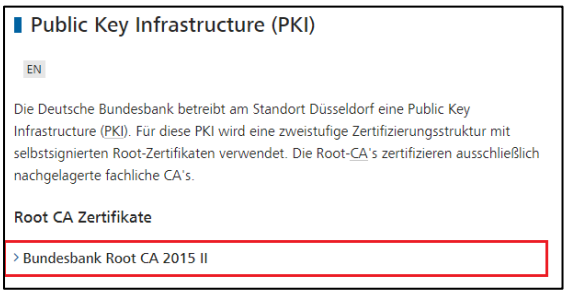


Abbildung 3: Auswahl Bundesbank Root CA 2015 II

4. Man erhält die folgende Seite:

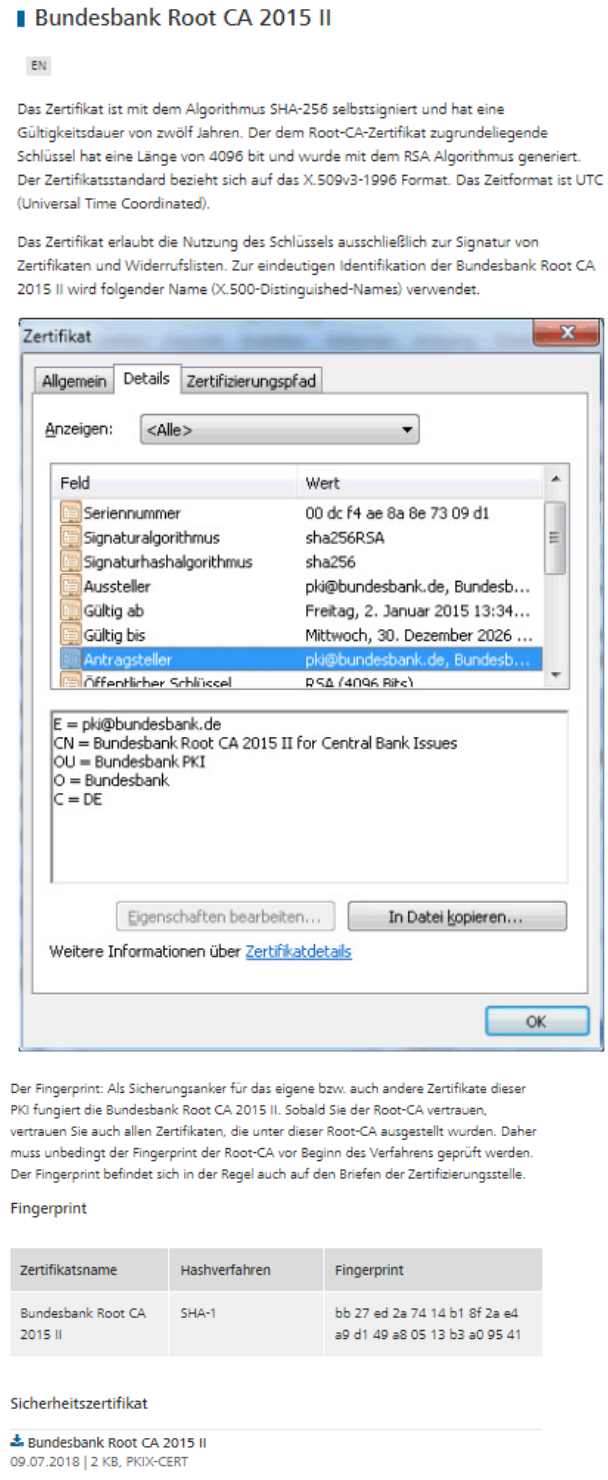


Abbildung 4: Ansicht Seite Bundesbank Root CA 2015 II

5. Das Zertifikat **Bundesbank Root CA 2015 II** herunterladen und speichern (z. B. auf: c:\temp oder Desktop).

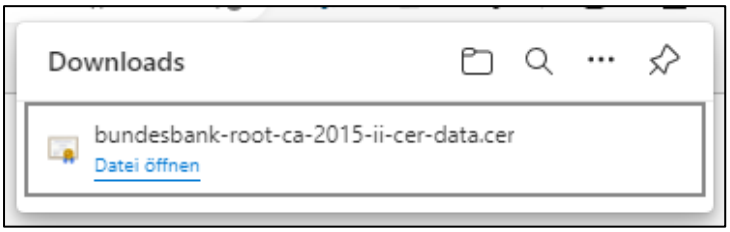


Abbildung 5: Download Zertifikat

1.2 Das Zertifikat CA for Digital Signature 2019

1. Auf der Homepage der Deutschen Bundesbank (www.bundesbank.de) den Link **Service ➔ Banken und Unternehmen** auswählen (analog 1.1).
2. Den Auswahlpunkt **Public Key Infrastructure (PKI)** auswählen (analog 1.1).
3. Das Zertifikat **CA for Digital Signature 2019** auswählen

Abbildung 6: Auswahl CA for Digital Signature 2019

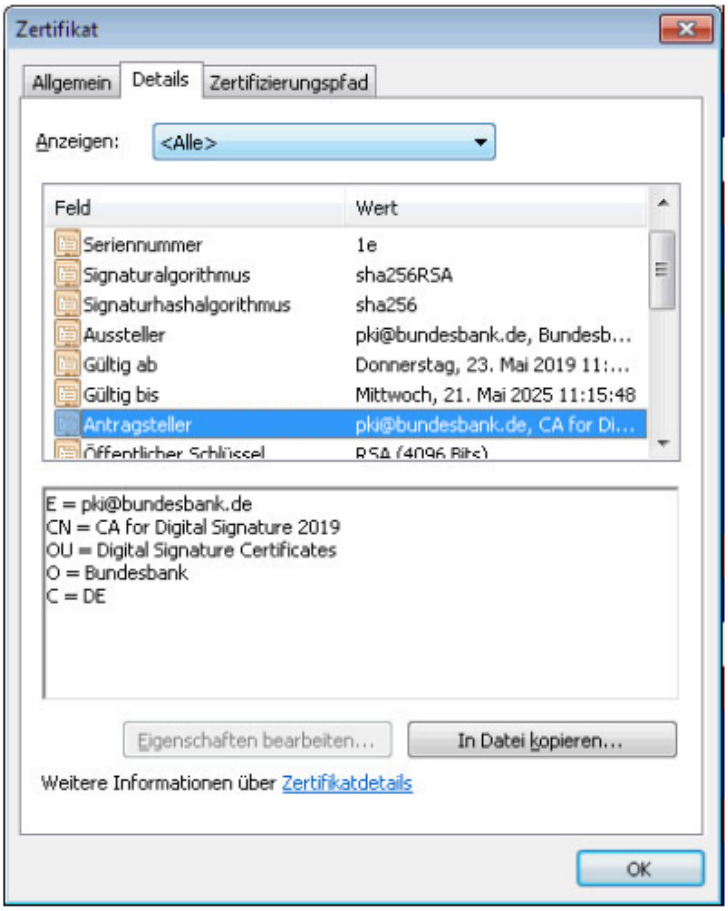
4. Man erhält die folgende Seite:

CA for Digital Signature 2019

EN

Das Zertifikat ist mit dem Algorithmus SHA-256 von der Bundesbank Root CA 2015 II 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 2015 II 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 2019 wird folgender Name (X.500-Distinguished-Names) verwendet:



Fingerprint

Zertifikat	Hashverfahren	Fingerprint
CA for Digital Signature 2019	SHA-256	4d 6a 6b 40 04 a3 dd 4f 0a 53 a8 55 a2 d2 15 0b 3c 7a c2 fb

Sicherheitszertifikat

CA for Digital Signature 2019
2 KB, CER

Abbildung 7: Ansicht Seite CA for Digital Signature 2019

5. Das Zertifikat **CA for Digital Signature 2019** herunterladen und speichern (z. B. auf: c:\temp oder Desktop).

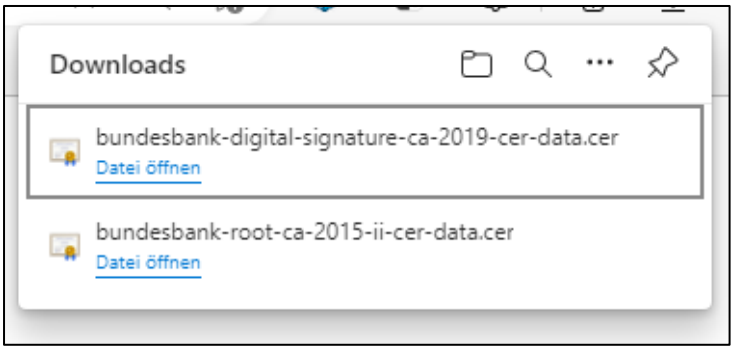


Abbildung 8: Download Zertifikat

2 Zertifikate den vertrauenswürdigen Kontakten hinzufügen und Signatur überprüfen

2.1 Einstieg

1. Das Mitteilungsschreiben zum Beispiel mit dem PDF-Reader **Adobe Acrobat Pro** öffnen.
2. In der Menüleiste den Auswahlpunkt **Bearbeiten ➔ Einstellungen…** wählen.

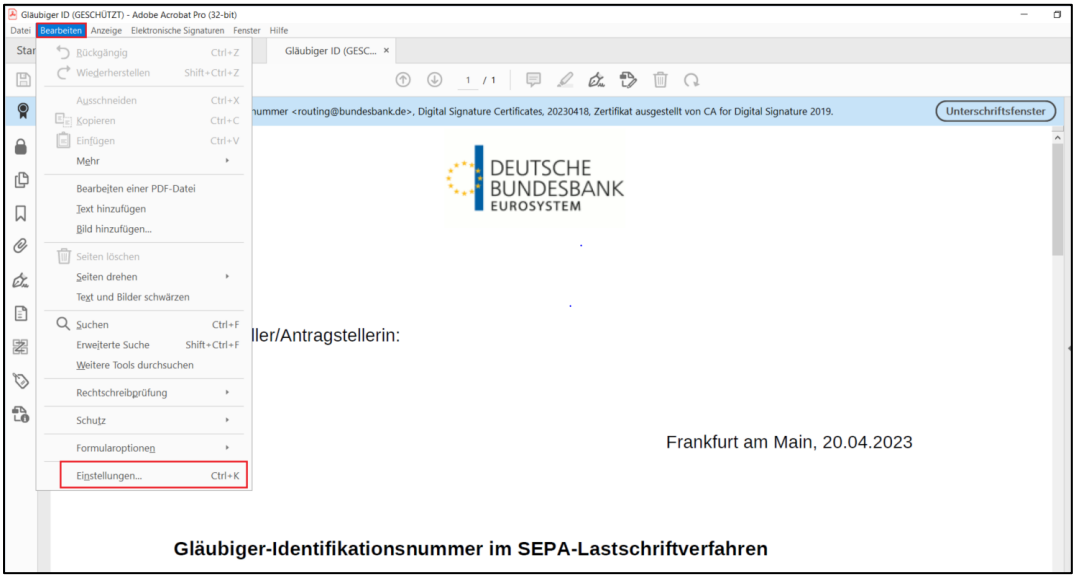


Abbildung 9: Ansicht Auswahl Bearbeiten - Einstellungen

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

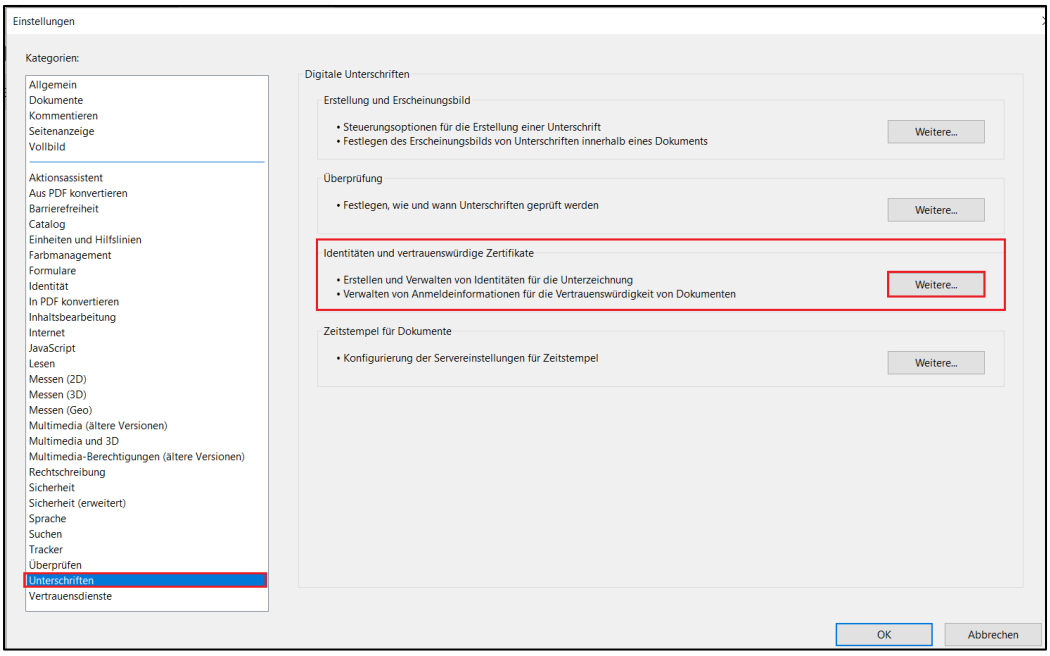


Abbildung 10: Ansicht Auswahl Unterschriften - Identitäten und vertrauenswürdige Zertifikate - Weitere

2.2 Das Zertifikat Bundesbank Root CA 2015 II importieren

Zunächst das erste Zertifikat importieren wie nachfolgend beschrieben:

1. Punkt **Vertrauenswürdige Zertifikate** und **Importieren** auswählen[1].

Abbildung 11: Ansicht Auswahl Vertrauenswürdige Zertifikate - Importieren

2. Auf **Durchsuchen…** klicken.

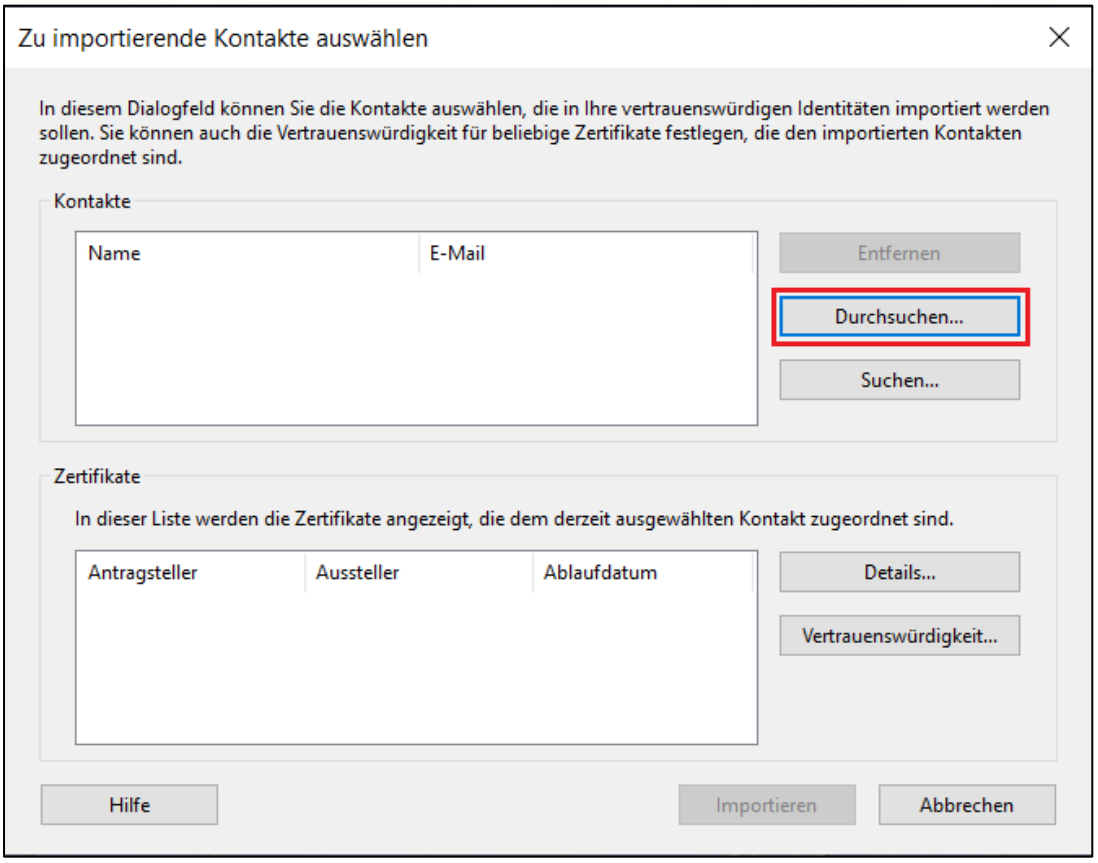


Abbildung 12: Ansicht Auswahl Durchsuchen

3. Anschließend aus dem Verzeichnis, in dem die Zertifikate gespeichert wurden (z. B.: c:\temp oder Desktop), das erste Zertifikat bundesbank-root-ca-2015-ii-cer-data.cer mit Doppelklick auswählen oder mit Klick auf **Öffnen**.

Abbildung 13: Ansicht Auswahl Zertifikat bundesbank-root-ca-2015-ii-cer-data.cer

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

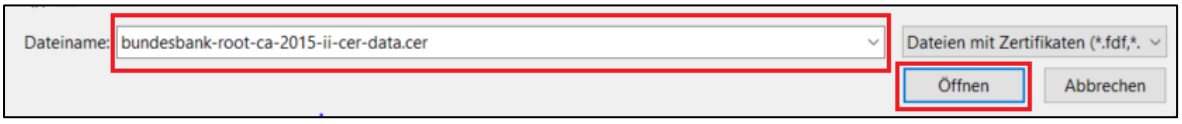


Abbildung 14: Ansicht Auswahl Zertifikat öffnen

4. Bei „Kontakte“ **(1)** das importierte Zertifikat auswählen, anschließend dieses unter „Zertifikate“ **(2)** auswählen und mit Doppelklick auf **Vertrauenswürdigkeit…** **(3)** bearbeiten.

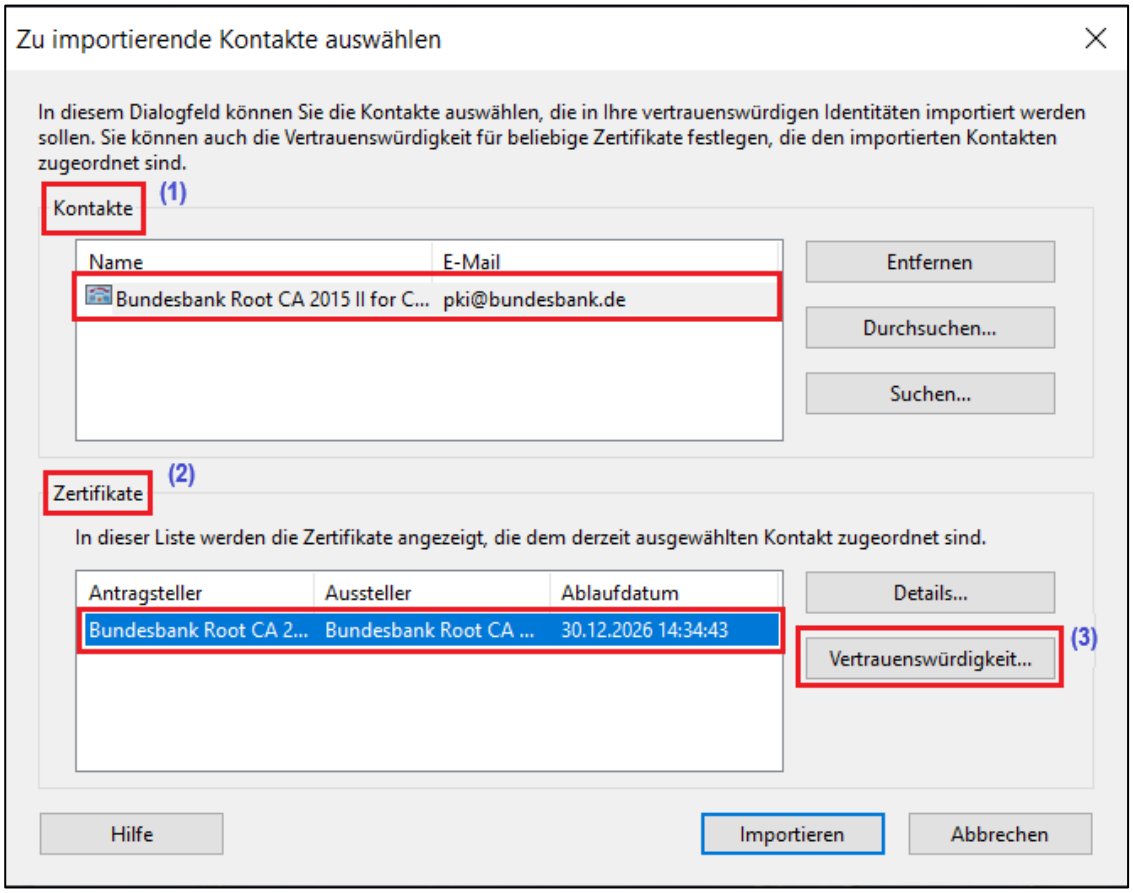


Abbildung 15: Ansicht Auswahl Vertrauenswürdigkeit bearbeiten

5. An den Stellen „*Dieses Zertifikat als vertrauenswürdigen Stamm verwenden*“ und „*Zertifizierte Dokumente*“ bitte ein Häkchen setzen (falls dort keines vorhanden), dann auf **OK**.

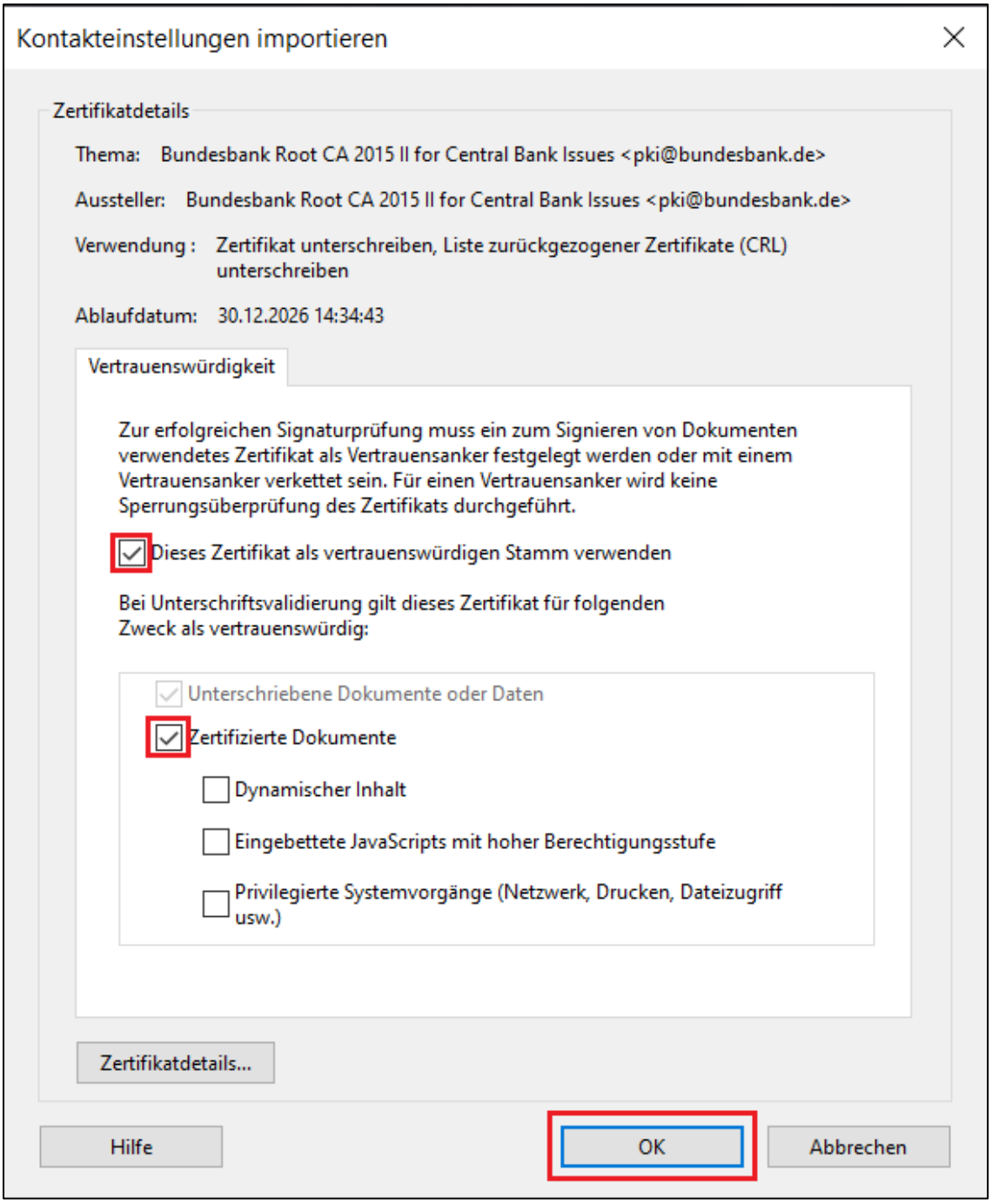


Abbildung 16: Ansicht Auswahl Verwendung des Zertifikats als vertrauenswürdigen Stamm

6. Klicken Sie auf **Importieren**

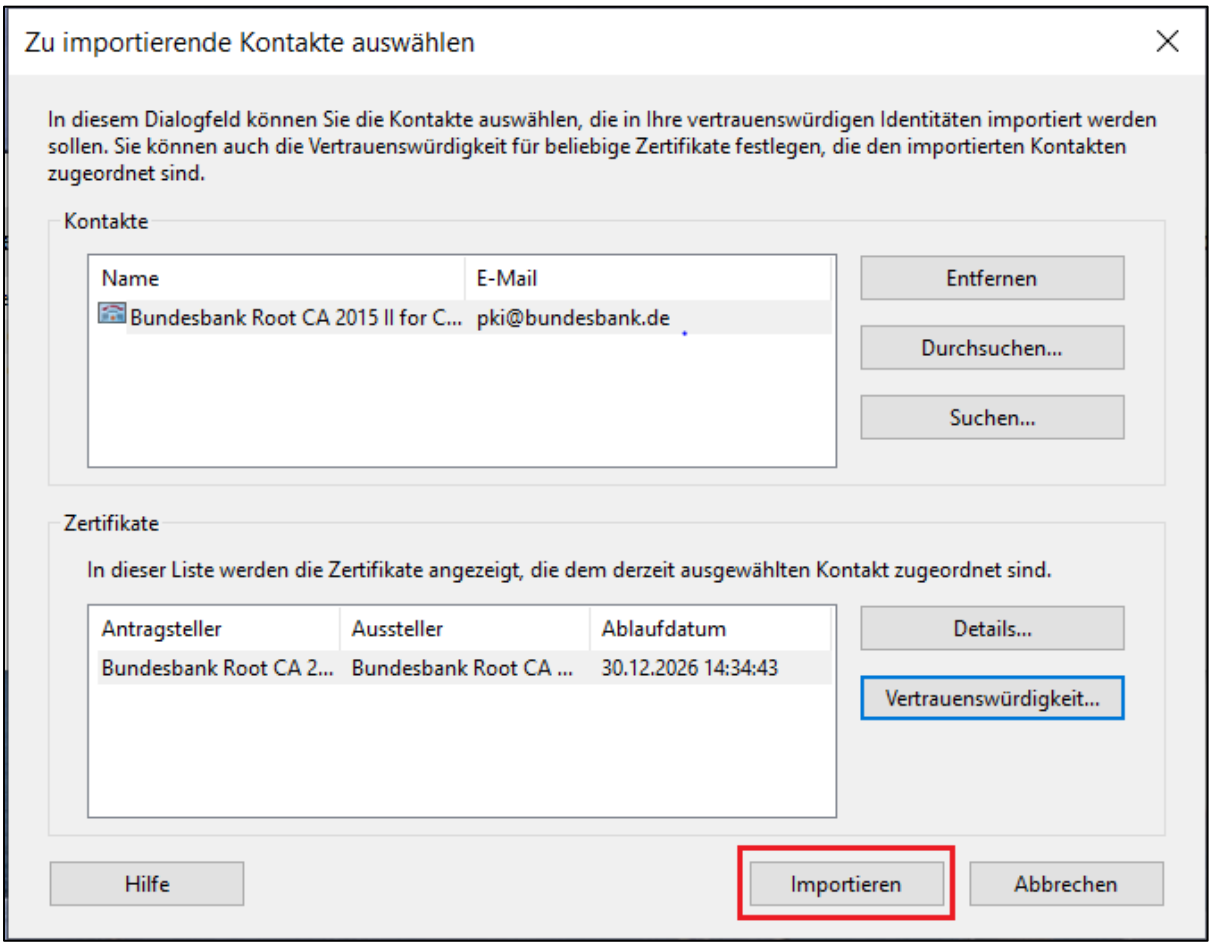


Abbildung 17: Ansicht Auswahl Zertifikat importieren

7. Und bestätigen Sie anschließend die Erfolgsmeldung „Import abgeschlossen“.

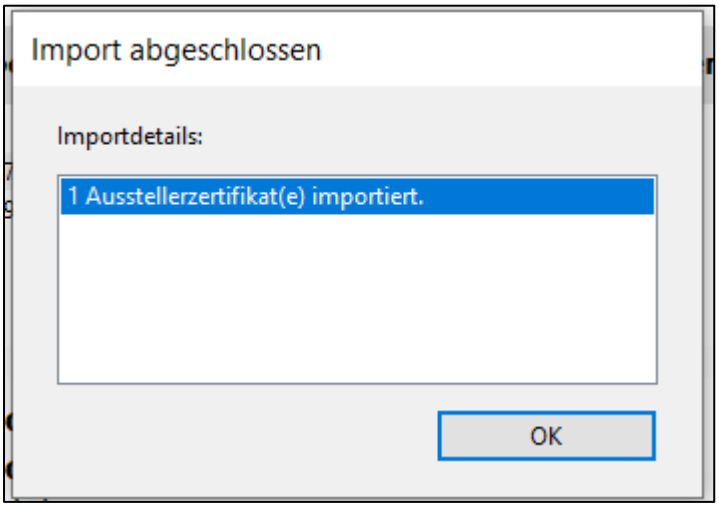


Abbildung 18: Auswahl Bestätigung der Meldung „Import abgeschlossen“

2.3 Das Zertifikat CA for Digital Signature 2019 importieren

Anschließend importieren Sie das zweite Zertifikat wie nachfolgend beschrieben:

1. **Vertrauenswürdige Zertifikate** und anschließend **Importieren** auswählen[2].

Abbildung 19: Ansicht Auswahl Vertrauenswürdige Zertifikate - Importieren

2. Auf **Durchsuchen…** klicken.

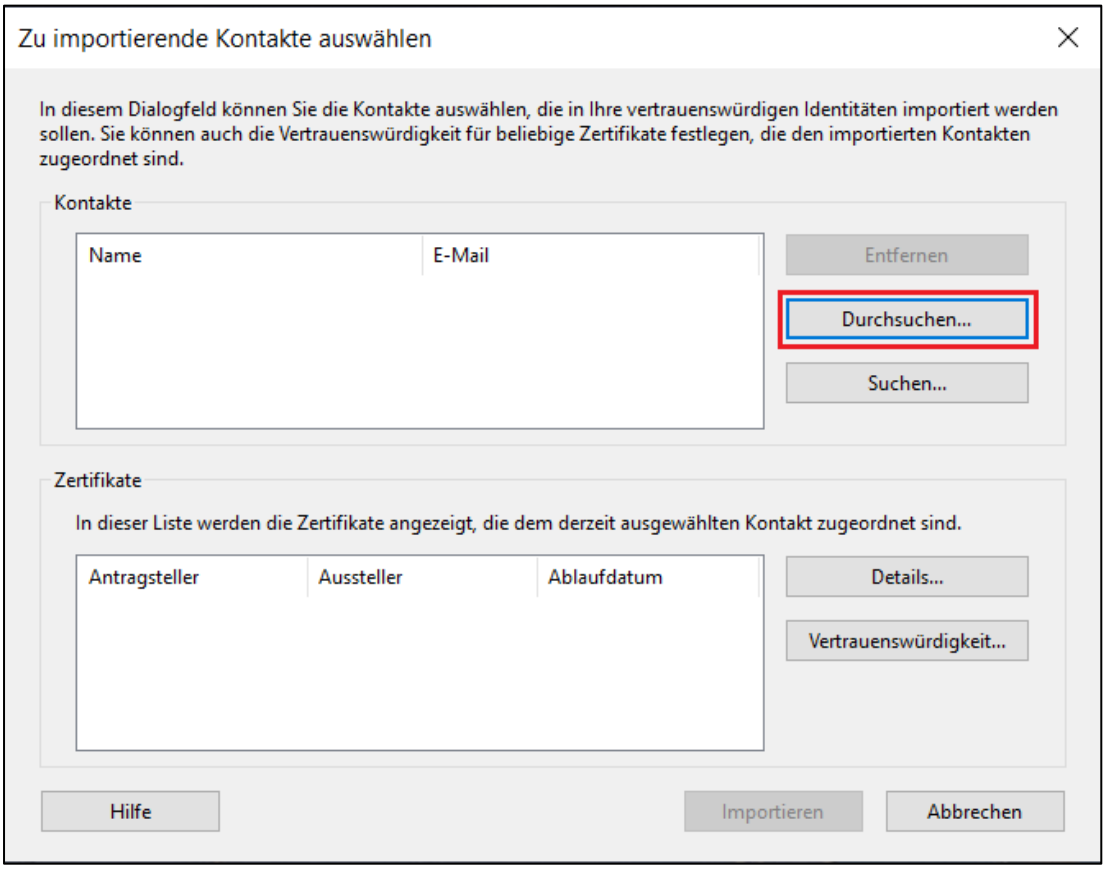


Abbildung 20: Ansicht Auswahl Durchsuchen

3. Anschließend aus dem Verzeichnis, in dem die Zertifikate gespeichert wurden (z. B.: c:\temp oder Desktop), das zweite Zertifikat bundesbank-digital-signature-ca-2019-cer-data.cer mit Doppelklick auswählen oder mit Klick auf **Öffnen**.

Abbildung 21: Ansicht Auswahl Zertifikat bundesbank-digital-signature-ca-2019-cer-data.cer

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

Abbildung 22: Ansicht Auswahl Zertifikat öffnen

4. Klicken Sie auf **Importieren**

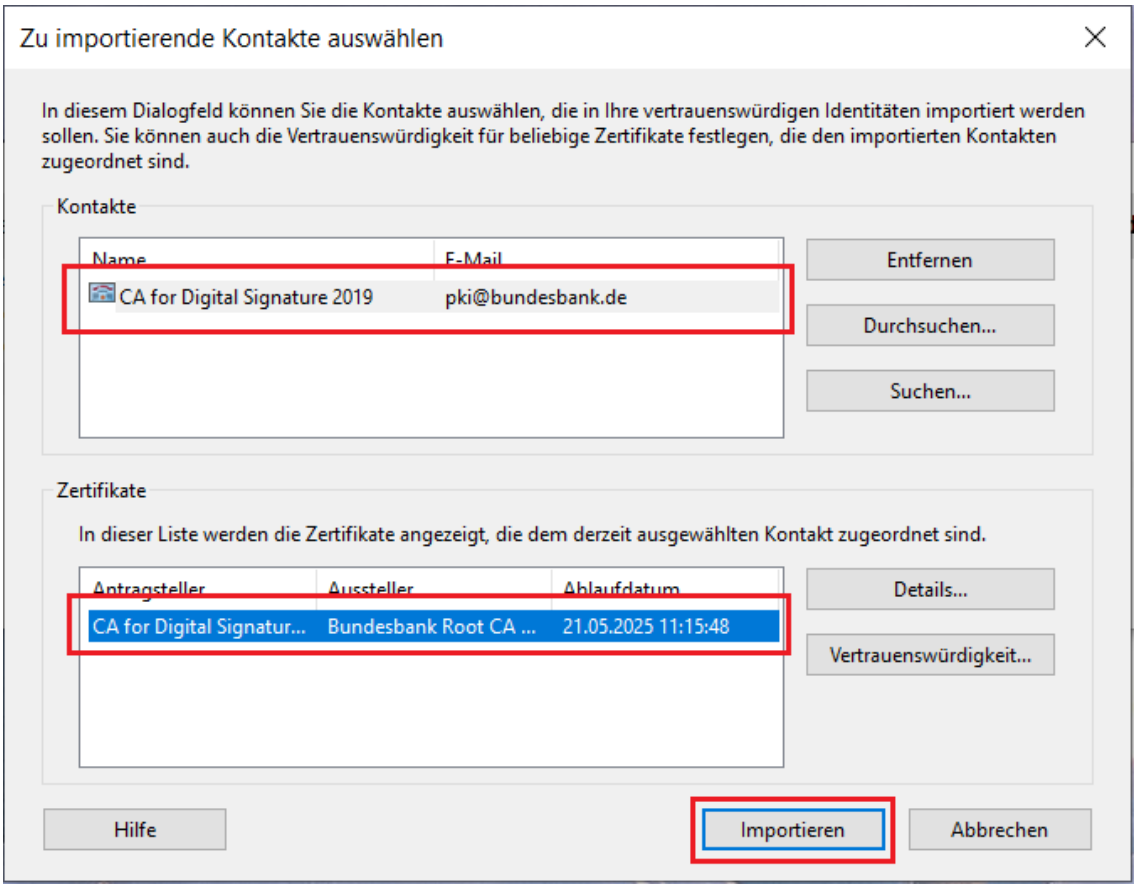


Abbildung 23: Ansicht Auswahl Zertifikat importieren

5. Und bestätigen Sie anschließend die Erfolgsmeldung „Import abgeschlossen“.

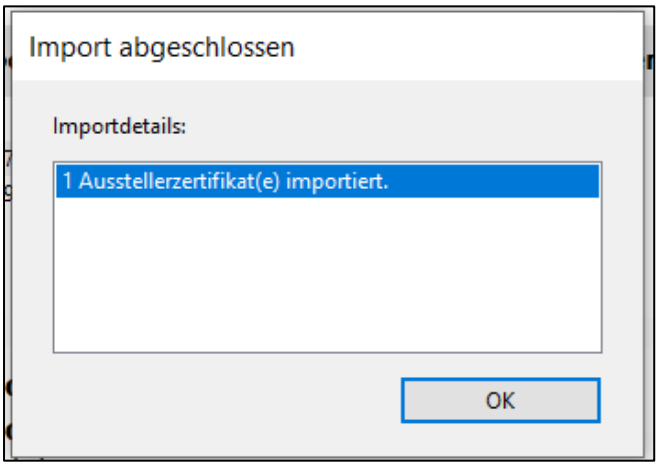


Abbildung 24: Ansicht Auswahl Bestätigung der Meldung „Import abgeschlossen“

2.4 Ergebnis

1. Es werden die importierten Zertifikate angezeigt. Anschließend können Sie dieses Fenster schließen.

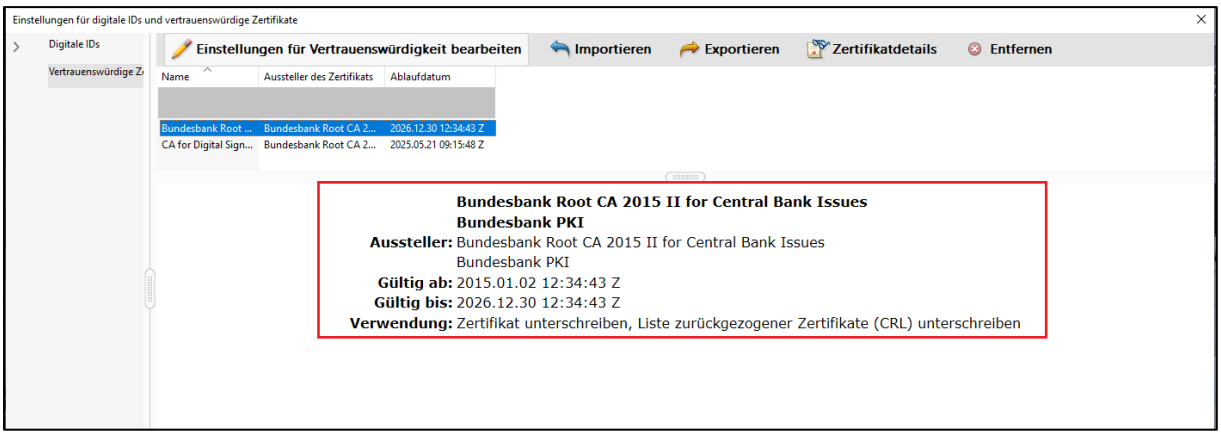


Abbildung 25: Ansicht importiertes Zertifikat Bundesbank Root CA 2015 II

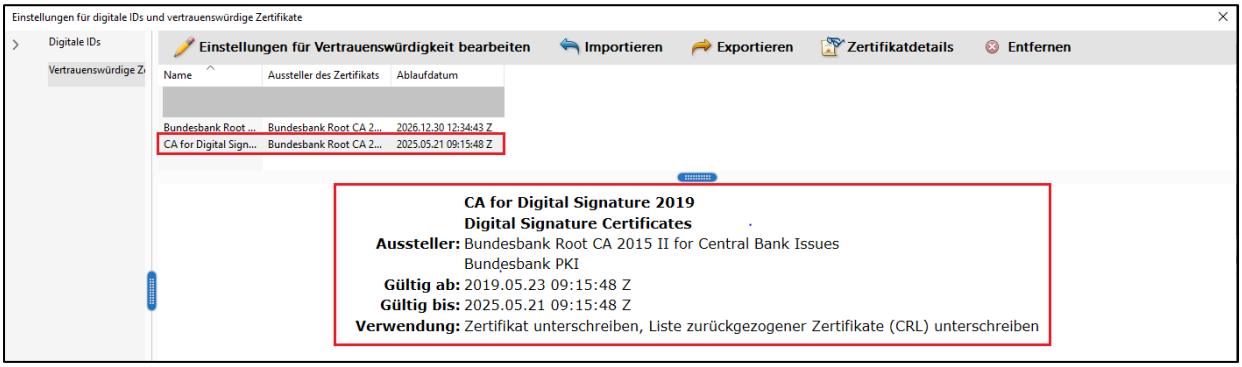


Abbildung 26: Ansicht importiertes Zertifikat CA for Digital Signature 2019

2. Schließen Sie das Fenster „Einstellungen“ mit **OK**

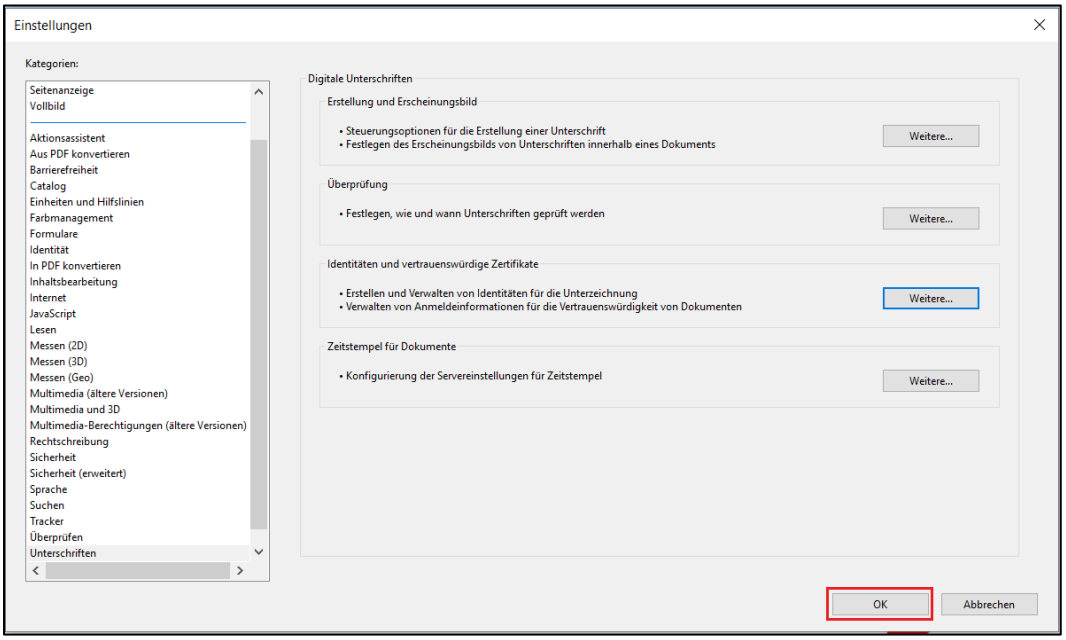


Abbildung 27: Ansicht Fenster „Einstellungen“

3 Überprüfen der Zertifikate

3.1 Allgemeine Prüfung

1. Zur Überprüfung der Signatur im geöffneten Mitteilungsschreiben den Punkt **Zertifikate** auswählen (ggf. muss die Auswahlmöglichkeit **Zertifikate** über die Auswahl **Mehr Werkzeuge** hinzugefügt werden)

Abbildung 28: Ansicht Auswahl Zertifikat

2. **Alle Signaturen prüfen** auswählen.

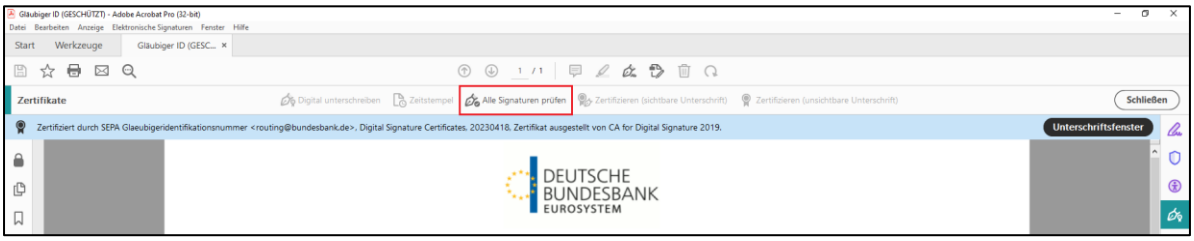


Abbildung 29: Ansicht Auswahl Alle Signaturen prüfen

3. Die Validierung der Signaturen mit **OK** bestätigen.

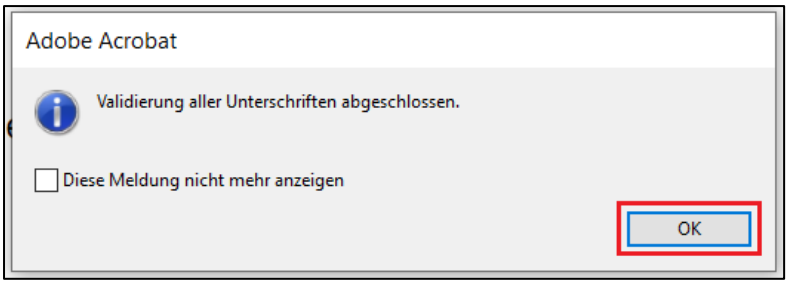


Abbildung 30: Ansicht Bestätigung der Validierung

4. Sie erhalten das Ergebnis der Signaturprüfung:
   Zertifiziert durch SEPA Gläubigeridentifikationsnummer <routing@bundesbank.de>, Digital Signature Certificates, 20230418, Zertifikat ausgestellt von CA for Digital Signature 2019.

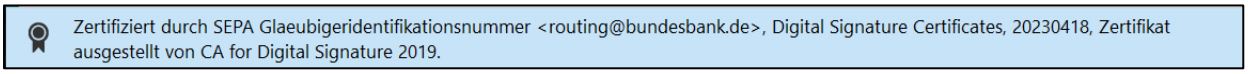


Abbildung 31: Ansicht Ergebnis der Signaturprüfung

3.2 Überprüfung des Unterschriftenfensters

1. Weitere Informationen zur digitalen Unterschrift erhalten Sie mit Klick auf **Unterschriftsfenster**.

Abbildung 32: Ansicht Auswahl Unterschriftsfenster

2. Die Zeile **Zertifiziert von SEPA Glaeubigeridentifikationsnummer <routing@bundesbank.de>** durch Anklicken auswählen.

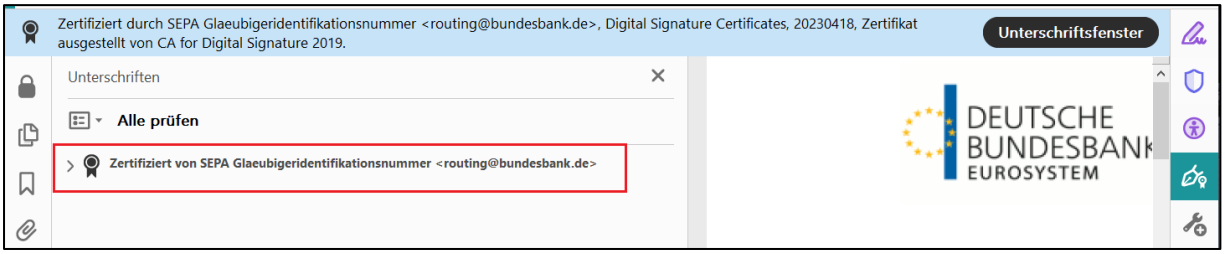


Abbildung 33: Ansicht Auswahl Zertifiziert von SEPA Glaeubigeridentifikationsnummer <routing@bundesbank.de>

Es öffnet sich die folgende Seite:

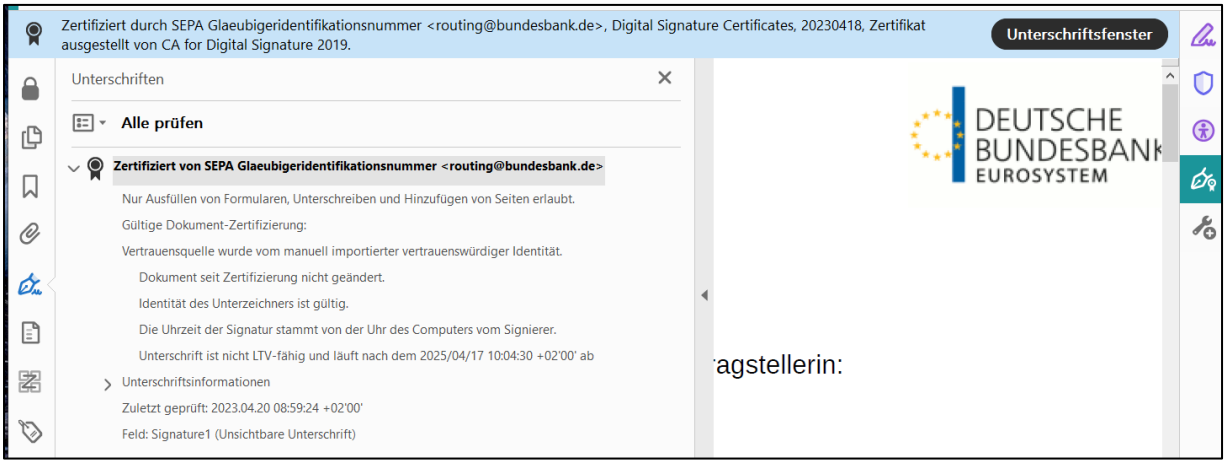


Abbildung 34: Ansicht Zertifiziert von SEPA Glaeubigeridentifikationsnummer <routing@bundesbank.de>

3. Durch Klick auf das Symbol **Optionen** öffnen sich die zugehörigen Auswahlmöglichkeiten:

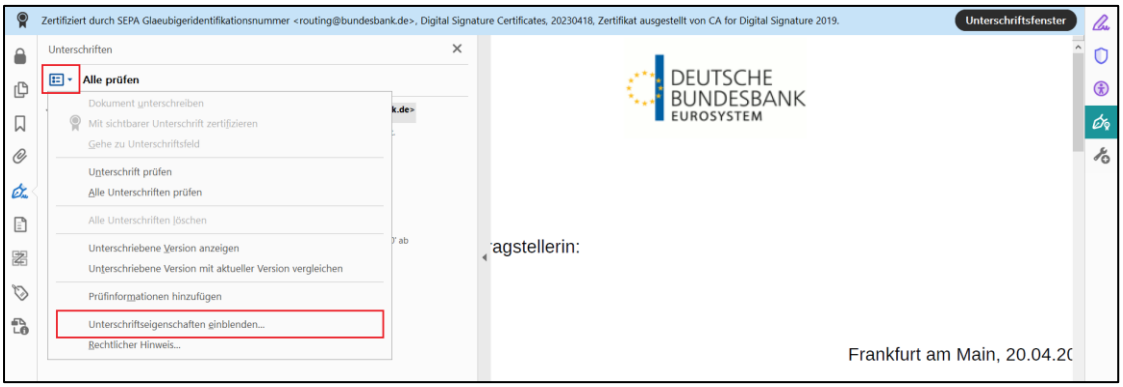


Abbildung 35: Ansicht Auswahl Optionen

4. **Unterschriftseigenschaften einblenden…** auswählen.

   Es müssen folgende Meldungen erscheinen:

Dokument-Zertifizierung ist gültig, von SEPA Glaeubigeridentifikationsnummer <routing@bundesbank.de> unterschrieben.

Dokument seit Zertifizierung nicht geändert. Der Zertifizierer hat festgelegt, dass das Ausfüllen und Unterschreiben von Formularfeldern bei diesem Dokument gestattet ist. Andere Änderungen sind nicht zulässig. Die Identität des Unterzeichners ist gültig.

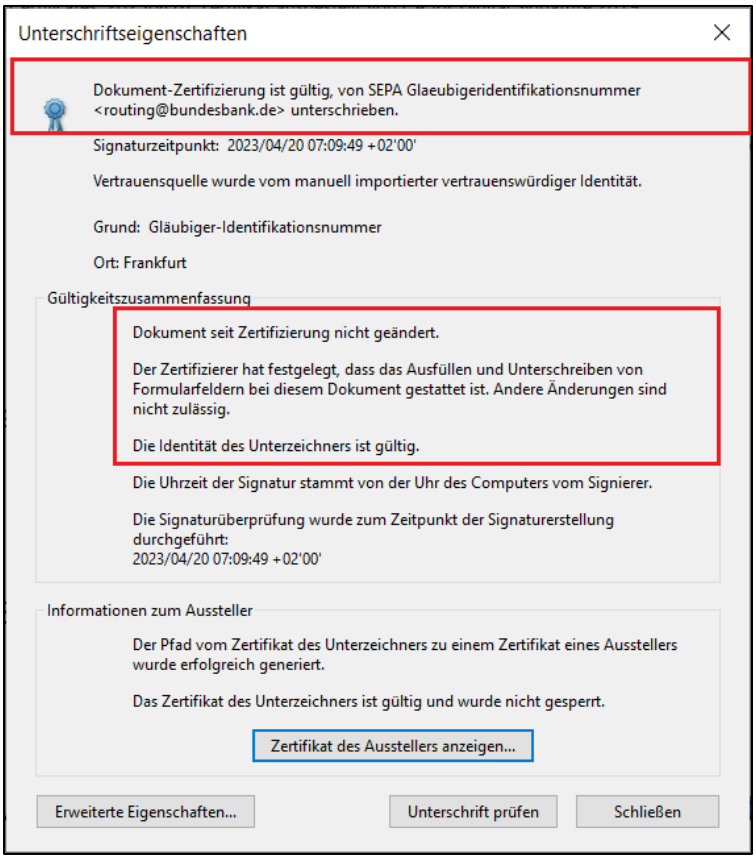


Abbildung 36: Ansicht Ergebnis Unterschriftseigenschaften

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