Sicherer GINA Zugriff mit HTTPS

Installationsanleitung für
Microsoft® Edge[1]

[1] Alle Screenshots wurden mit Microsoft Edge, Version 25.10586.0.0 erstellt. Microsoft Edge ist eine Marke der Microsoft® Corporation. © 2015 Microsoft.
(Weitere Informationen zu Mindestanforderungen und unterstützten Browser-Versionen finden Sie hier: e-Card System Browser und ELGA Browser.)

Installation der Zertifikate

Die Zertifikate finden Sie unter anderem unter folgenden Links:

→ auf www.chipkarte.at/ – Drei Schritte zu einfachen Installation: Schritt 3

→ oder auf https://www.sozialversicherung.at/HTTPS-GINA-ZUGRIFF

(Alternativ navigieren Sie bitte auf www.chipkarte.at zum Bereich „Gesundheitsdiensteanbieter“ → dann im linken Menü: Security & Kompatibilität → Sicherer GINA Zugriff (HTTPS) → Drei Schritte zur einfachen Installation → Schritt 3: Installation der Zertifikate)

Unter dem Punkt „**Schritt 3: Installation der Zertifikate**“ stehen sechs Zertifikatdateien zum Download zur Verfügung.

Schritt 1:
Starten Sie bitte die Installation durch einen Klick mit der linken Maustaste auf die Datei **„LINK 1) Zertifikat RootCA-1“**.

Schritt 2:
Es erscheint am unteren Fensterrand eine Hinweisbox (siehe Abbildung 1). Wählen Sie hier den Punkt „**Öffnen**“.

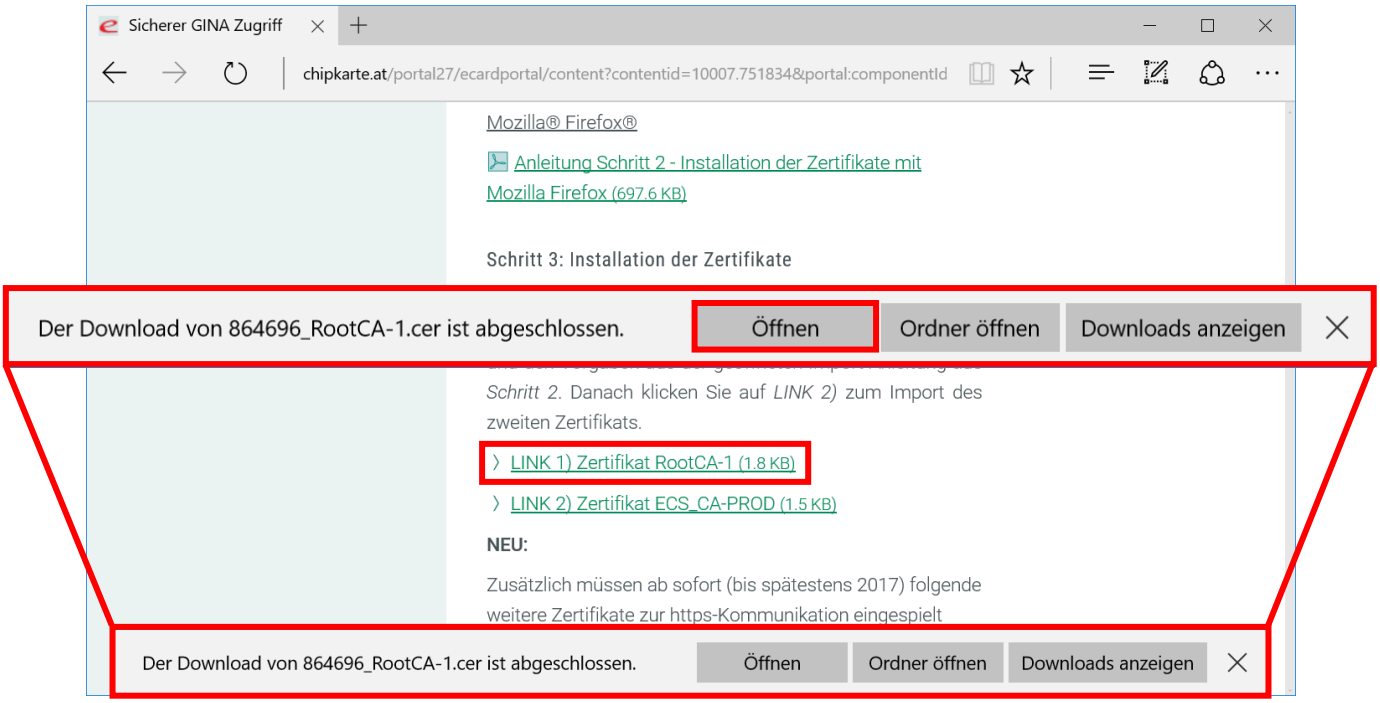

Abbildung 1: Download und Öffnen der Zertifikatsdatei im Microsoft Edge

Schritt 3:

Es wird das entsprechende Zertifikat, wie in Abbildung 2, geöffnet und angezeigt. Zum Start der Installation klicken Sie bitte auf „**Zertifikat installieren…**“.

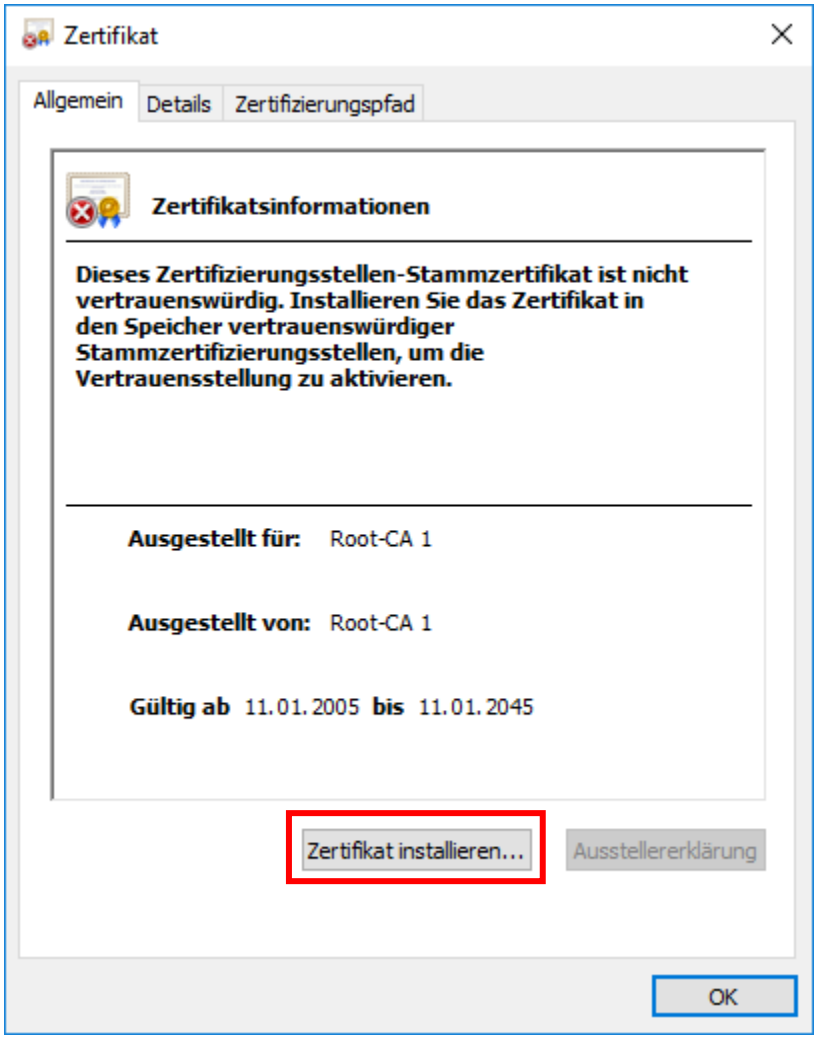

Abbildung 2: Das für die Installation ausgewählte und geöffnete Zertifikat

Schritt 4:

Als Nächstes startet der Zertifikatimport-Assistent (siehe Abbildung 3). Hier haben Sie die Möglichkeit den relativen Speicherort Ihres Zertifikats zu wählen. **Empfohlen wird hierbei die Option „Lokaler Computer“**, da hierbei das Zertifikat für alle Benutzer installiert wird und nicht nur für den jeweiligen, zurzeit angemeldeten Benutzer.

(Sofern Letzteres allerdings gewünscht ist, wählen Sie bitte die Option „Aktueller Benutzer“ und fahren Sie mit der Installation bei Schritt 6 fort.)

Bestätigen Sie Ihre Eingabe mit einem Klick auf „**Weiter**“.

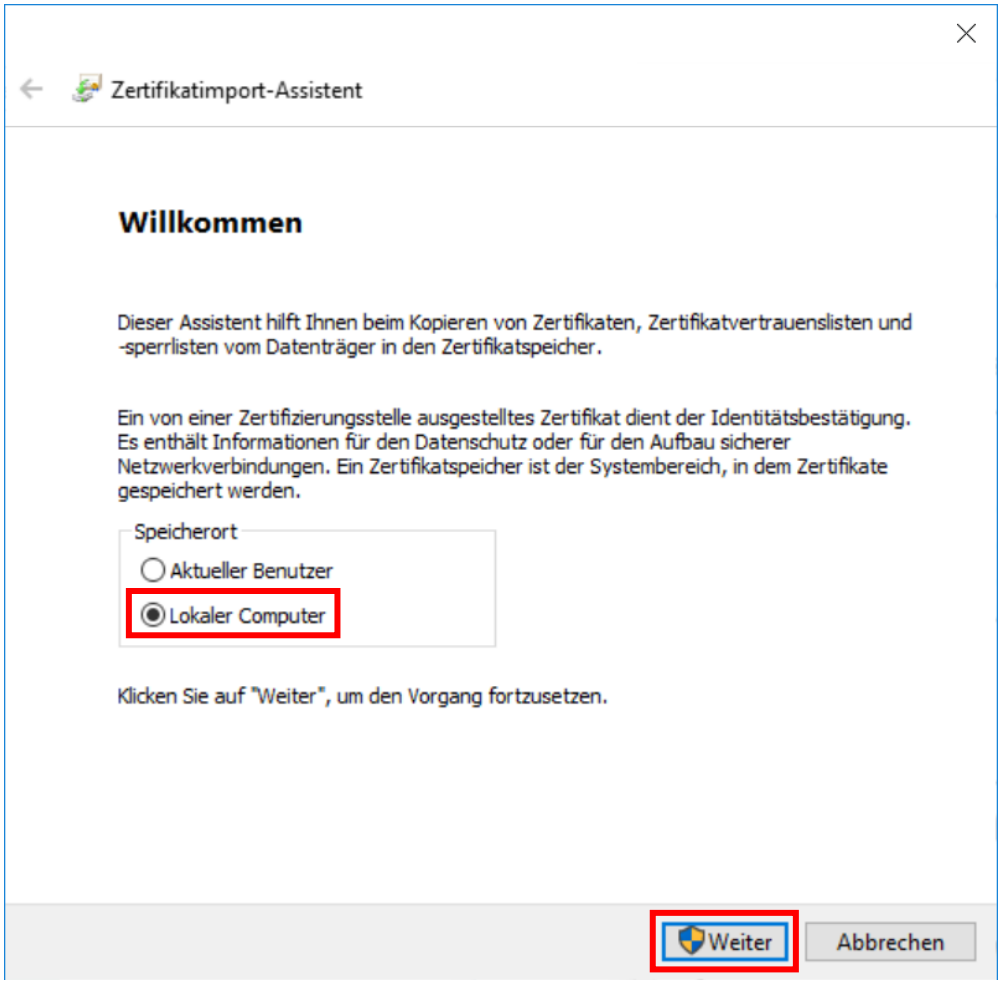

Abbildung 3: Assistent zur Installation der Zertifikate.

Schritt 5:
Als nächstes öffnet sich das Fenster „Benutzerkonten-Steuerung“. Um die Installation des Zertifikats zu erlauben, müssen Sie Administrator-Benutzernamen und –Kennwort Ihres Computers eingeben. Bestätigen Sie mit „**Ja**“.

(Falls Ihnen diese Anmelde-Informationen nicht bekannt sind, klicken Sie bitte auf „Abbrechen“, wählen Sie „Aktueller Benutzer“ und fahren Sie mit Schritt 6 fort. Für weitere Informationen kontaktieren Sie bitte Ihren System-Administrator.)

Schritt 6:
Im folgenden Fenster (siehe Abbildung 4) wählen Sie den Punkt „**Alle Zertifikate in folgendem Speicher speichern**“ und gehen dann auf „**Durchsuchen…**“.

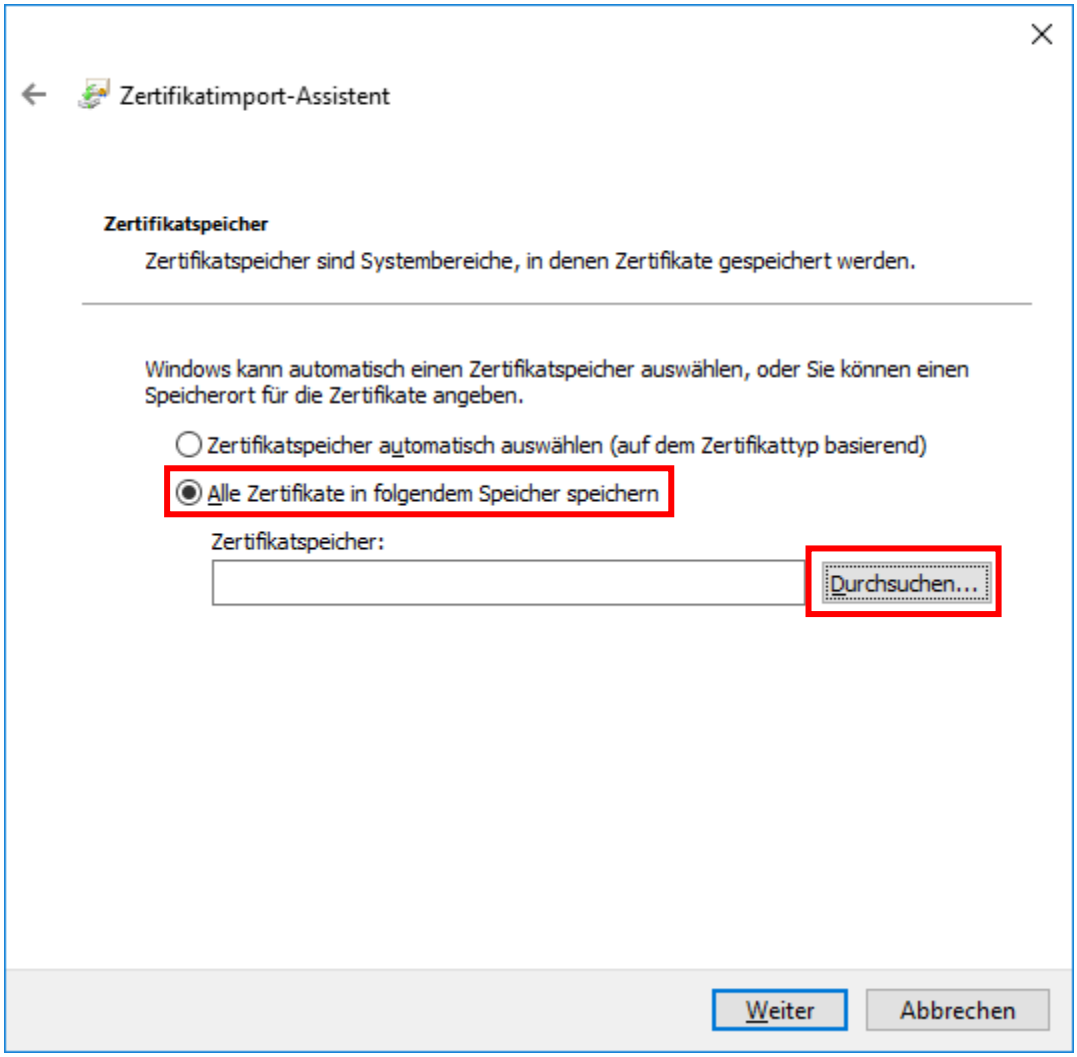

Abbildung 4: Zertifikatimport-Assistent - Zertifikatspeicher

Schritt 7:

Wählen Sie den Ordner „**Vertrauenswürdige Stammzertifizierungsstellen**“ (siehe Abbildung 5) aus, klicken Sie anschließend auf „**OK**“ und im folgenden Fenster auf „**Weiter**“.

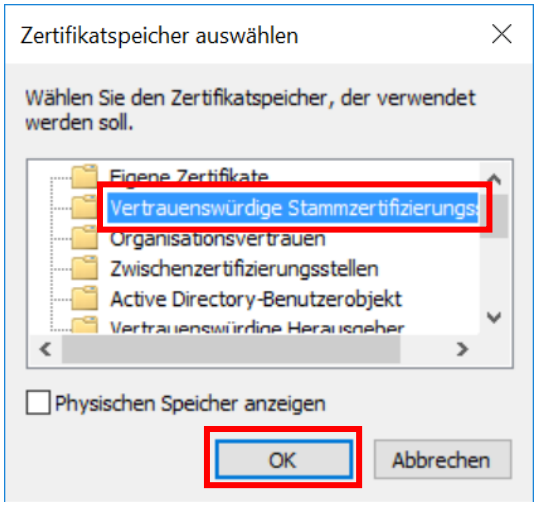

Abbildung 5: Zertifikatspeicher auswählen

Schritt 8:
Im nachfolgenden Fenster „Fertigstellen des Assistenten“ (siehe Abbildung 6) wählen Sie „**Fertig stellen**“.

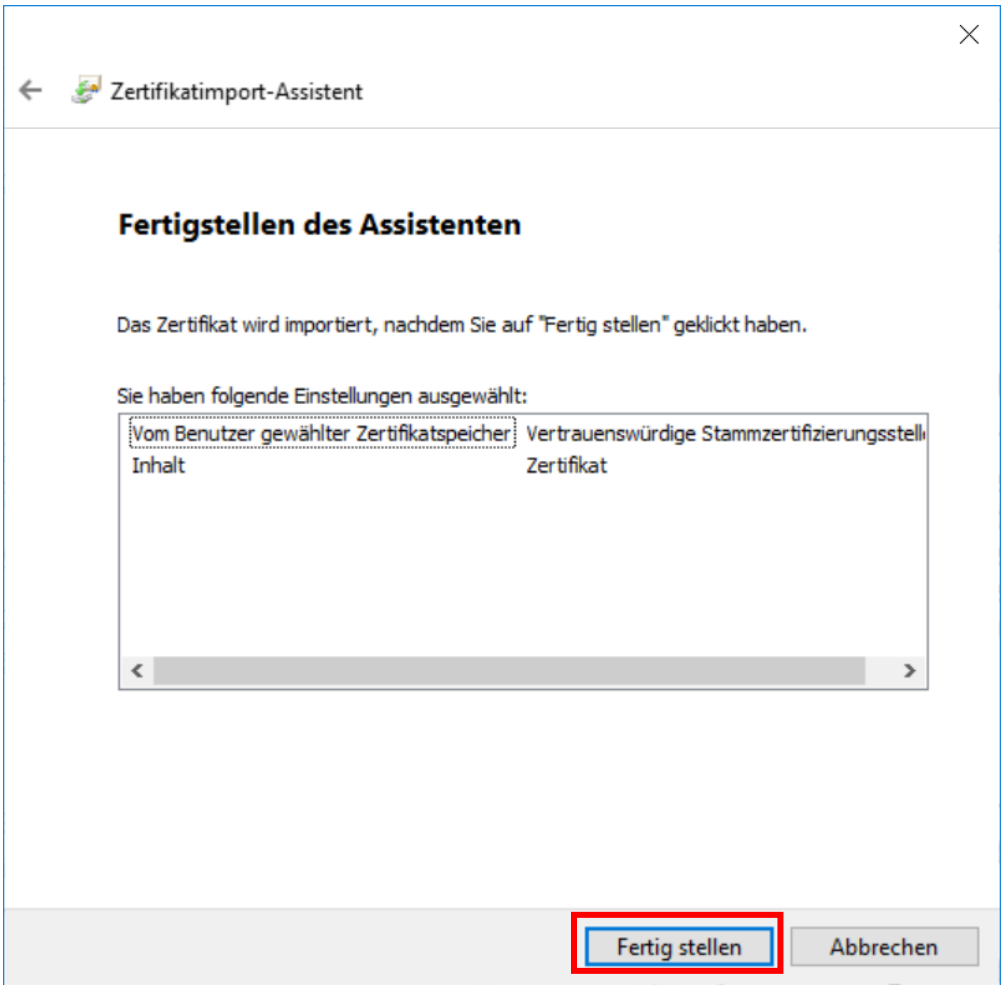

Abbildung 6: Zertifikatimport-Assistent – Fertigstellen des Assistenten

Schritt 9:
Zum Schluss erscheint unter Umständen noch eine „Sicherheitswarnung“ und Sie werden gefragt „*Möchten Sie dieses Zertifikat installieren?“* (siehe Abbildung 7). Hier klicken Sie bitte auf „**Ja**“.

In diesem Fenster finden Sie unter anderem auch die Möglichkeit den Fingerabdruck des Zertifikats unter dem Punkt „Fingerabdruck“ (grüne Markierung) zu kontrollieren. (Eine Auflistung aller Fingerprints finden Sie auch weiter unten in diesem Dokument, ab Seite 9.)

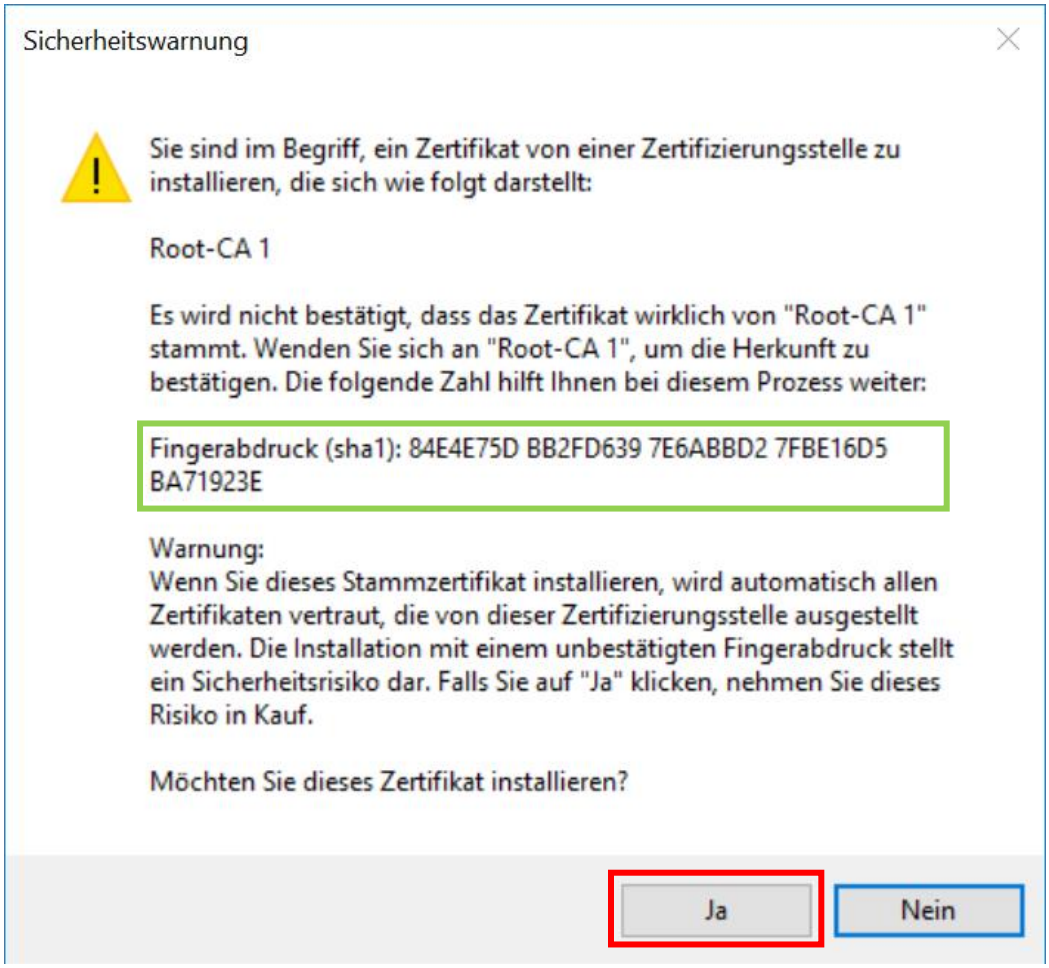

Abbildung 7: Sicherheitswarnung und Kontrollmöglichkeit des „Fingerabdrucks“.

Schritt 10:

Bei der Bestätigungsmeldung über den erfolgreichen Import klicken Sie bitte auf „**OK**“ (siehe Abbildung 8).

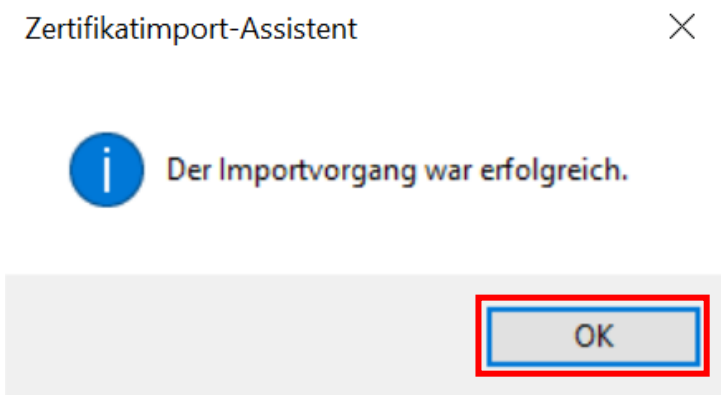

Abbildung 8: Bestätigungsmeldung zur erfolgreichen Installation des Zertifikats.

Schritt 11:
Das Fenster „Zertifikat“ kann nun ebenfalls mit einem Klick auf „**OK**“ geschlossen werden.

Der gesamte Vorgang muss für die fünf weiteren Dateien (Zertifikate LINK 2) – LINK 6)) wiederholt werden!

Bitte achten Sie jedoch darauf, dass Sie die in Schritt 7 erwähnte Zertifizierungsstelle pro Zertifikat korrekt auswählen!

Die Zuordnung sollte sein, wie in Tabelle 1 beschrieben:

Vertrauenswürdige Stammzertifizierungsstellen	Zwischenzertifizierungsstellen
LINK 1) Root-CA 1	LINK 2) ECS_CA-PROD
LINK 3) Zert_CA_Root_V02_Test	LINK 4) Zert_CA_ECS_V02_Test
LINK 5) Zert_CA_Root_V02_Prod	LINK 6) Zert_CA_ECS_V02_Prod

Tabelle 1: Übersicht der Zertifizierungsstellen und deren Zertifikate

Am Ende müssen folgende Zertifikate importiert sein:

- **Root-CA 1** **(Root-CA 1)**
- **ECS_CA-PROD** **(ECS_CA-PROD)**
- **Zert_CA_Root_V02_Test** **(Test – Hauptverband oesterr. Sozialvers.)**
- **Zert_CA_ECS_V02_Test** **(Test ECS CA)**
- **Zert_CA_Root_V02_Prod** **(Hauptverband oesterr. Sozialvers.)**
- **Zert_CA_ECS_V02_Prod** **(Prod ECS CA)**

Um dies zu überprüfen öffnen Sie bitte die „**Einstellungen**“ links unten im Startmenü Ihres Windows 10 Betriebssystems (siehe Abbildung 9).

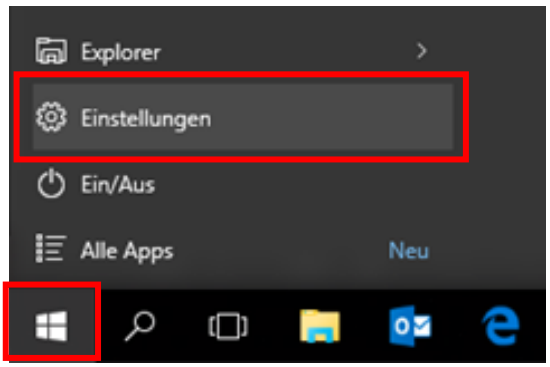

Abbildung 9: Menüpunkt "Einstellungen" in Windows 10

Als nächstes öffnet sich das „**Einstellungen**“-Fenster ihres Betriebssystems. Wie in Abbildung 10 gezeigt, klicken Sie nun bitte in der rechten oberen Ecke in das Such-Feld und tippen Sie „zertifikate“. (Alternativ kann auch „certificate“ getippt werden.)

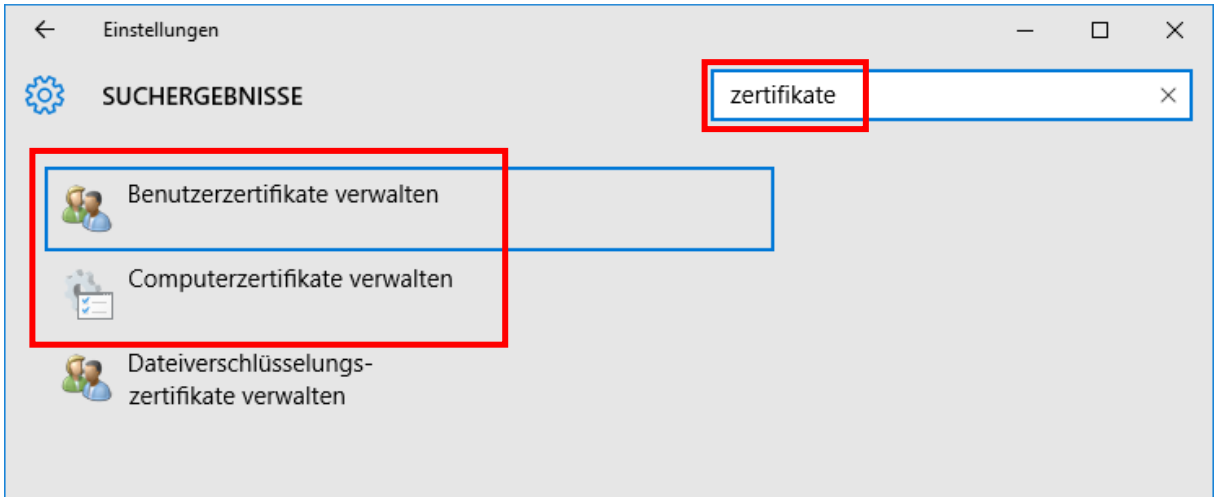

Abbildung 10: Suche der Zertifikat-Verwaltung in den Einstellungen von Windows 10

Das Ergebnis Ihrer Suche sollten zumindest zwei Zertifikat-Verwaltungsstellen sein: „Benutzerzertifikate verwalten“ und „Computerzertifikate verwalten“. Die weitere Vorgehensweise ist abhängig von Ihrer oben getroffenen Speicherortwahl (vgl. Schritt 4 auf Seite 2).
Wenn Sie für Ihre Zertifikate die Option „Aktueller Benutzer“ gewählt haben, klicken Sie bitte auf „Benutzerzertifikate verwalten“. Sollte „Lokaler Computer“ Ihre Option gewesen sein, wählen Sie bitte „Computerzertifikate verwalten“.

Anschließend öffnet sich der Zertifikatmanager – „**certmgr**“ für Benutzerzertifikate oder „**certlm**“ für Computerzertifikate.

Da sich beide Manager in deren Anzeige für die weitere Vorgehensweise nur gering unterscheiden, werden sich die Screenshots im weiteren Verlauf der Einfachheit halber nur auf den Verwaltungsmanager für Benutzerzertifikate („certmgr“) beziehen (siehe Abbildung 11).

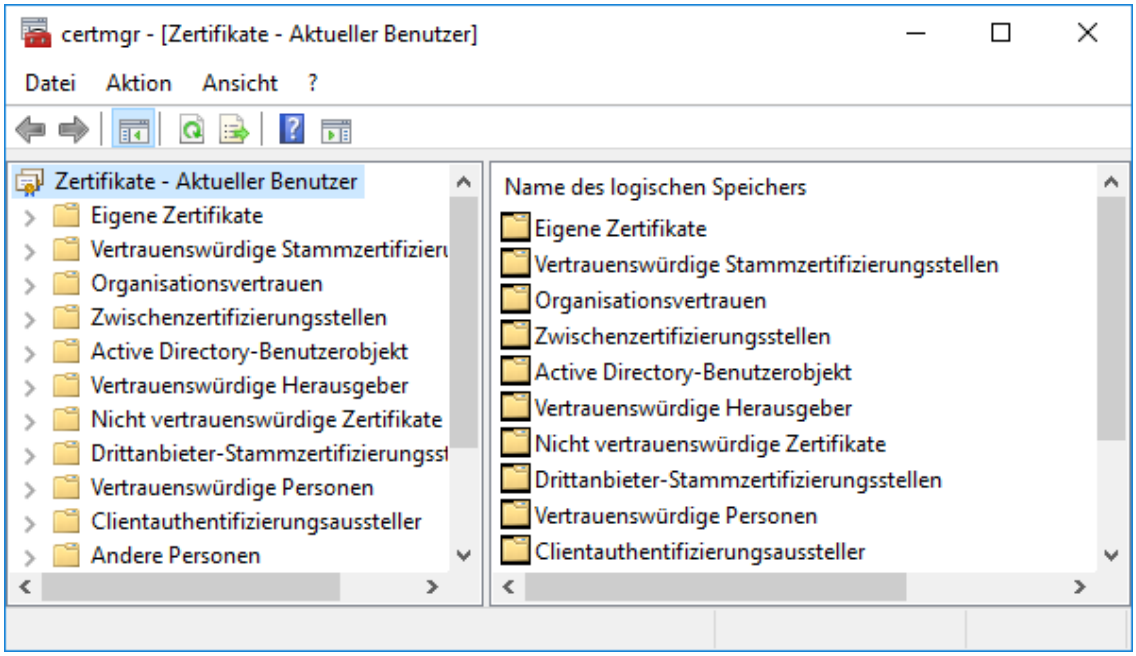

Abbildung 11: Verwaltungsmanager für Zertifikate

Öffnen Sie als nächstes bitte auf der linken Seite den Ordner „**Vertrauenswürdige Stammzertifizierungsstellen**“ und dann den Unterordner „**Zertifikate**“ mit jeweils einem Einfachklick. Dann erscheint eine Liste der Zertifikate in der rechten Fenster-Hälfte (siehe Abbildung 12). Hier sollten Sie die drei Zertifikate vorfinden, wie in Tabelle 1, S.7 beschrieben.

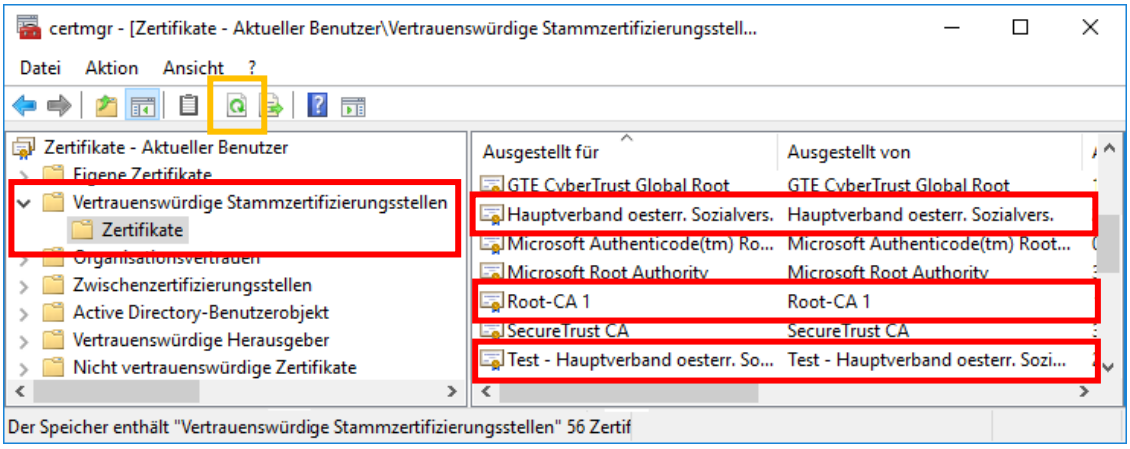

Abbildung 12: Zertifikate im Ordner "Vertrauenswürdige Stammzertifizierungsstellen" – „Zertifikate“

(Für den Fall, dass die Zertifikate bei Ihnen nicht angezeigt werden, ist es womöglich notwendig die Ansicht zu aktualisieren. Dies können Sie mit einem Klick auf dieses Symbol in der oberen Menü-Leiste machen: .)
Durch einen Doppelklick auf das jeweilige Zertifikat wird dieses geöffnet und die Eigenschaften werden in der Registerkarte „**Details**“ angezeigt. Hier sollten Sie die **Signatur (Fingerabdruck)** (grüne Umrandung) überprüfen:

- Root-CA 1 (siehe Abbildung 13)
- Test – Hauptverband oesterr. Sozialvers. (siehe Abbildung 14)
- Hauptverband oesterr. Sozialvers. (siehe Abbildung 15)

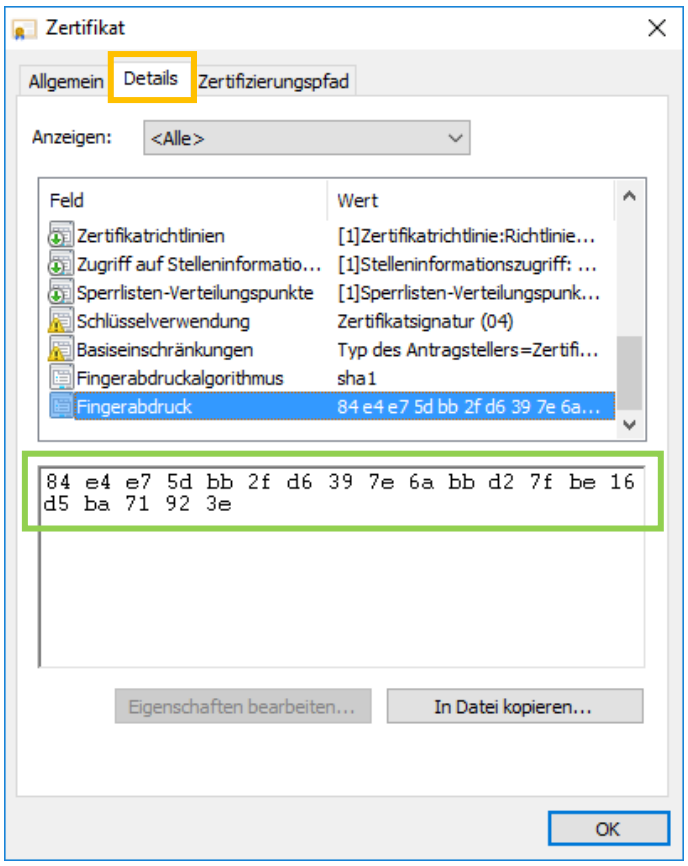

Abbildung 13: Signatur von "Root-CA 1"

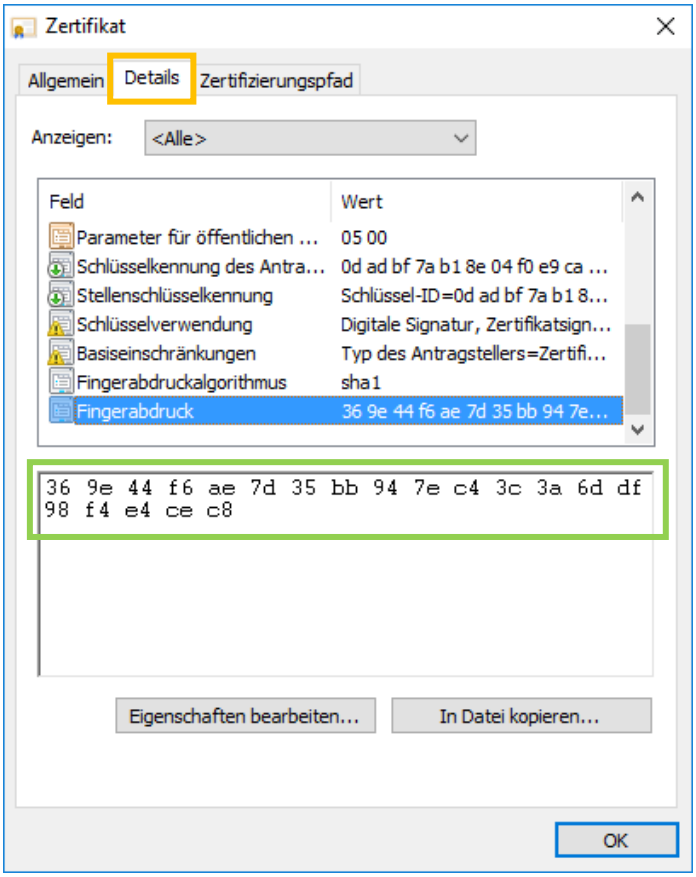

Abbildung 14: Signatur von "Test – Hauptverband oesterr. Sozialvers."

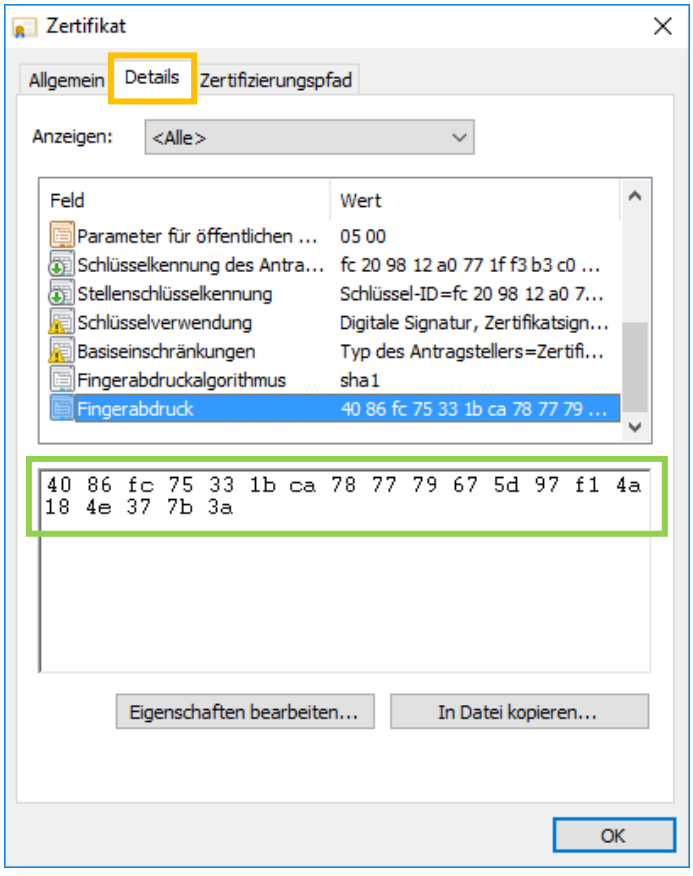

Abbildung 15: Signatur von "Hauptverband oesterr. Sozialvers."

Wiederholen Sie den letzten Schritt auch für die Zertifikate im Ordner „Zwischenzertifizierungsstellen“, Unterordner „Zertifikate“ (siehe Abbildung 16).

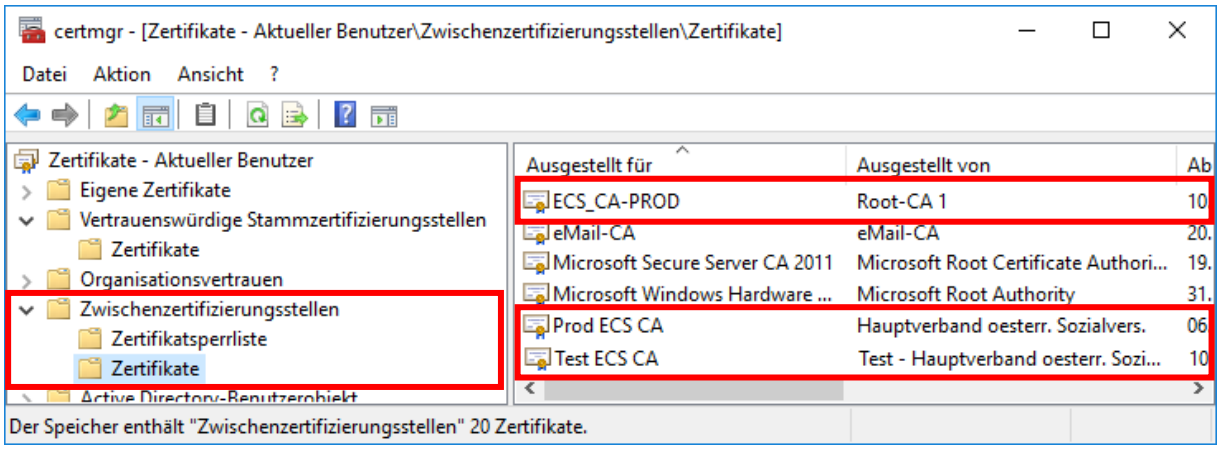

Abbildung 16: Zertifikate im Ordner "Zwischenzertifizierungsstellen" – „Zertifikate“

Durch einen Doppelklick auf das jeweilige Zertifikat kann dieses wieder geöffnet und die Eigenschaften in der Registerkarte „**Details**“ angezeigt werden. Überprüfen Sie nun bitte die **Signatur (Fingerabdruck)** (grüne Umrandung) folgender Zertifikate:

- ECS_CA-Prod (siehe Abbildung 17)
- Prod ECS CA (siehe Abbildung 18)
- Test ECS CA (siehe Abbildung 19)

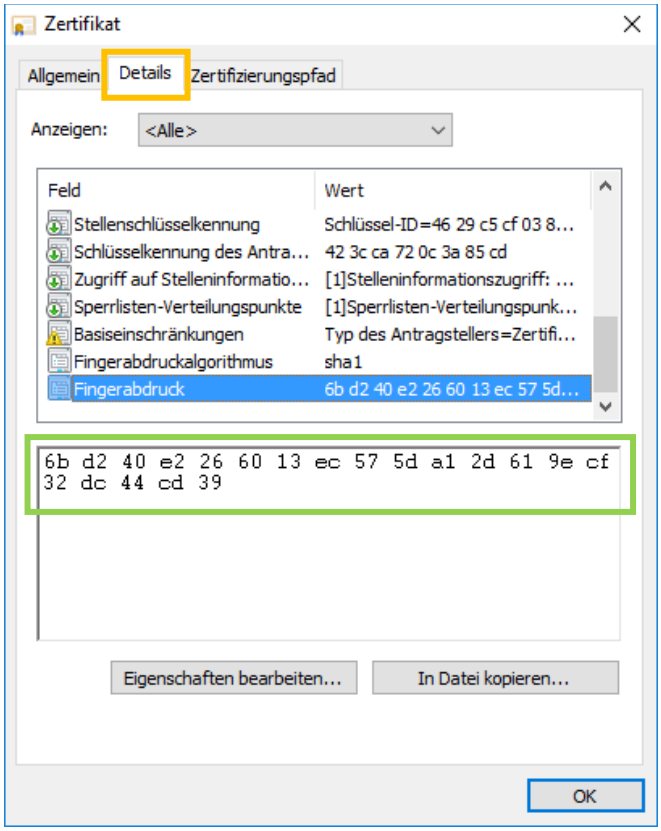

Abbildung 17: Signatur von "ECS_CA-Prod"

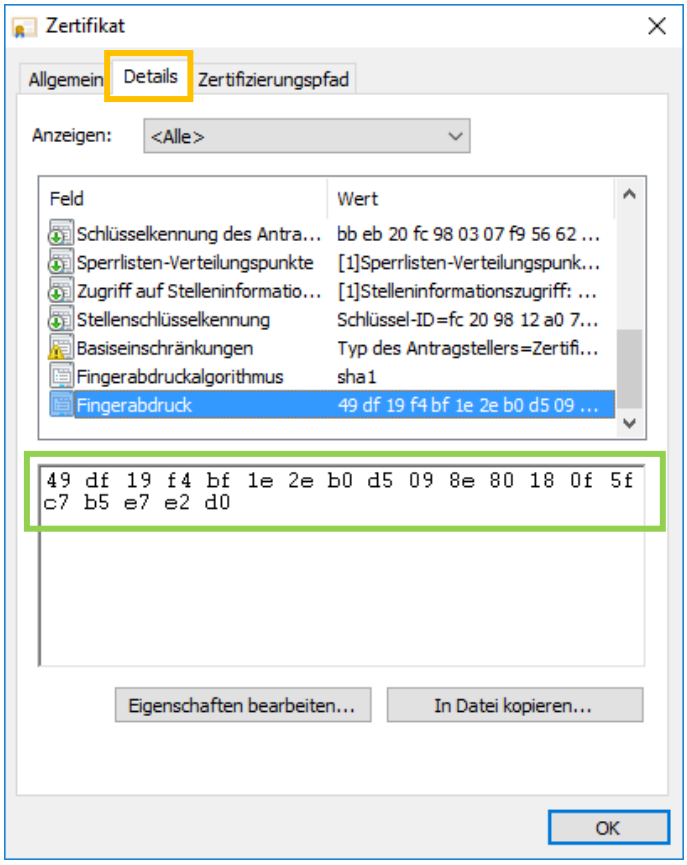

Abbildung 18: Signatur von "Prod ECS CA"

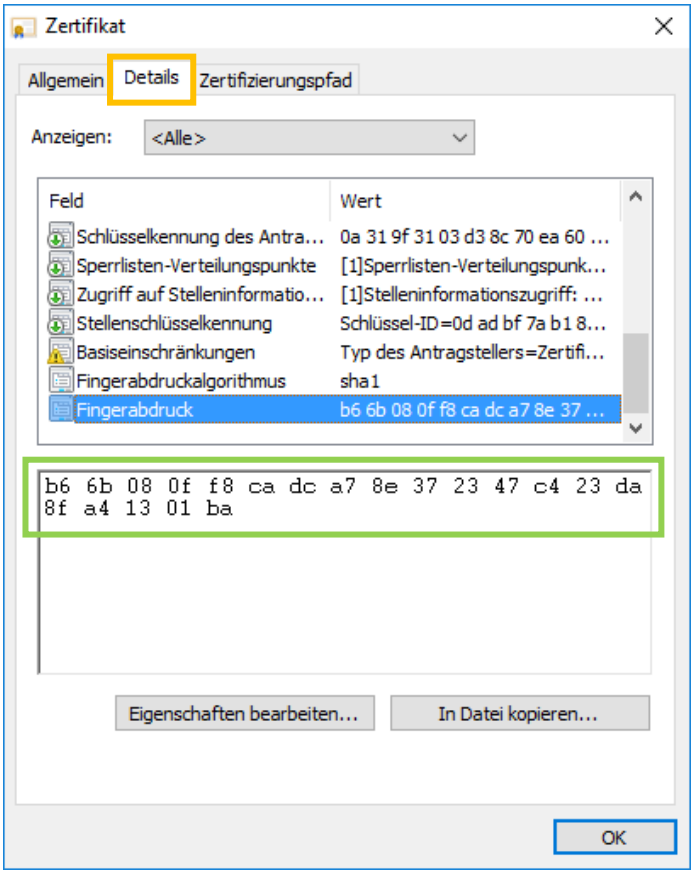

Abbildung 19: Signatur von „Test ECS CA“