designing e-health

Installation der Zertifikate für Google® Chrome[1]

[1] Alle Screenshots wurden mit *Google Chrome Version 94* erstellt. © 2021 Google Inc.
(Weitere Informationen zu Mindestanforderungen und unterstützten Browser-Versionen finden Sie hier: e-Card System Browser und ELGA Browser)
Wesentliche Änderungen zur Vorversion sind gelb markiert.

Installation der Zertifikate

Die Zertifikate finden Sie unter folgendem Link:

→ Download-Zertifikate

(Alternativ navigieren Sie auf www.chipkarte.at zum Bereich „Gesundheitsdiensteanbieter“ → dann im linken Menü: Security & Kompatibilität → Sichere Kommunikation im e-card System (HTTPS) → Zertifikate: Download (Produktionsumgebung)

*Unter dem Punkt „***Zertifikate: Download (Produktionsumgebung)***“ stehen zwei Zertifikatdateien zum Download zur Verfügung.* (Die .cer Dateiversionen sind im Regelfall die richtige Wahl.)

Schritt 1:

Starten Sie den Download durch einen Klick mit der linken Maustaste auf die Datei **„Zert_CA_Root_V02_Prod.cer“**.

Schritt 2:

Ihr Zertifikat erscheint in der Download-Leiste am unteren Bildschirmrand. (Abhängig von den Download-Einstellungen Ihres Browsers werden Sie vor dem Download gebeten, den Ziel-Speicherort der Datei auszuwählen.) Nach abgeschlossenem Download klicken Sie bitte auf die Datei. Etwaige Warnungen können in diesem Fall ignoriert werden.

Schritt 3:

Es wird das entsprechende Zertifikat geöffnet und angezeigt (wie in Abbildung 1). Zum Start der Installation klicken Sie auf „**Zertifikat installieren…**“.

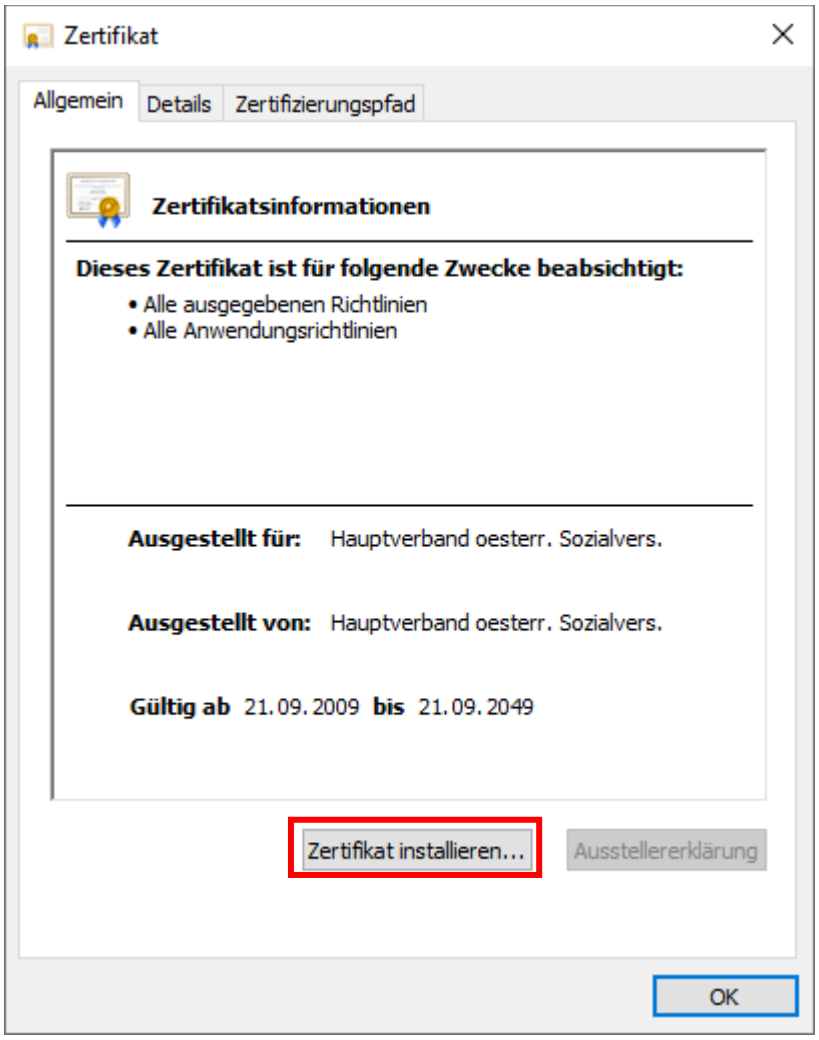

Abbildung 1: Das für die Installation ausgewählte und geöffnete Zertifikat

Schritt 4:

Als Nächstes startet der Zertifikatimport-Assistent (siehe Abbildung 2). Hier haben Sie die Möglichkeit, den relativen Speicherort Ihres Zertifikats zu wählen. **Empfohlen wird 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 die Option „Aktueller Benutzer“ und fahren Sie mit der Installation bei Schritt 6 fort.)

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

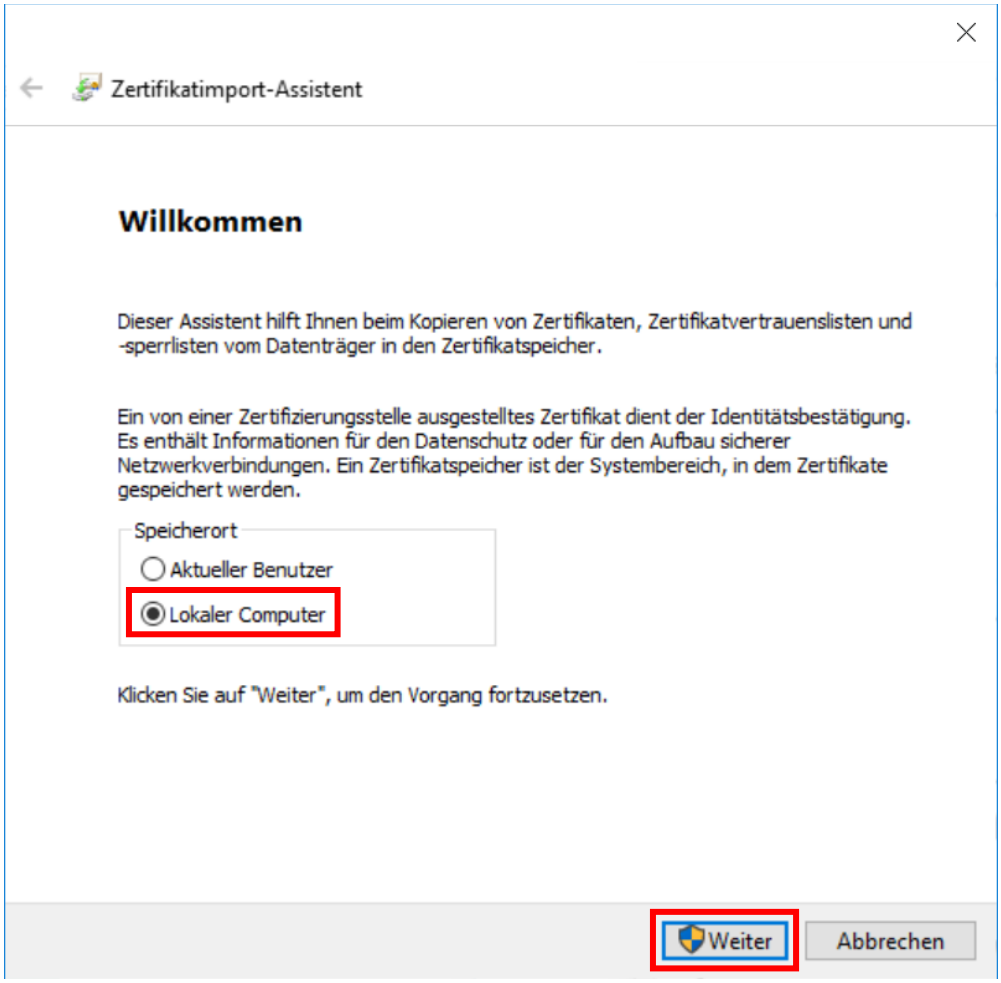

Abbildung 2: Assistent zur Installation der Zertifikate

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 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 3) wählen Sie den Punkt „**Alle Zertifikate in folgendem Speicher speichern**“ und klicken Sie danach auf „**Durchsuchen…**“.

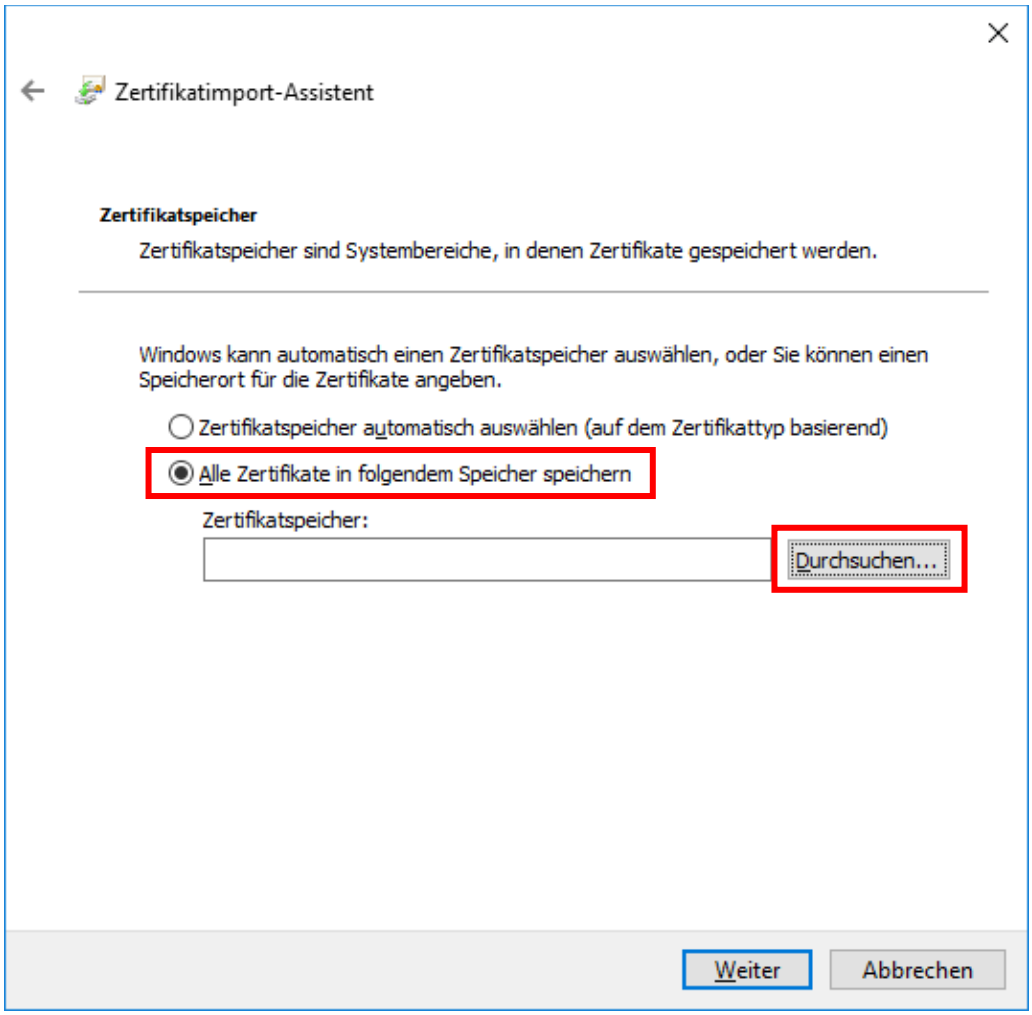

Abbildung 3: Zertifikatimport-Assistent – Zertifikatspeicher

Schritt 7:

Wählen Sie den Ordner „Vertrauenswürdige Stammzertifizierungsstellen“ aus (siehe Abbildung 4), klicken Sie danach auf „**OK**“ und im darauffolgenden Fenster anschließend auf „**Weiter**“.

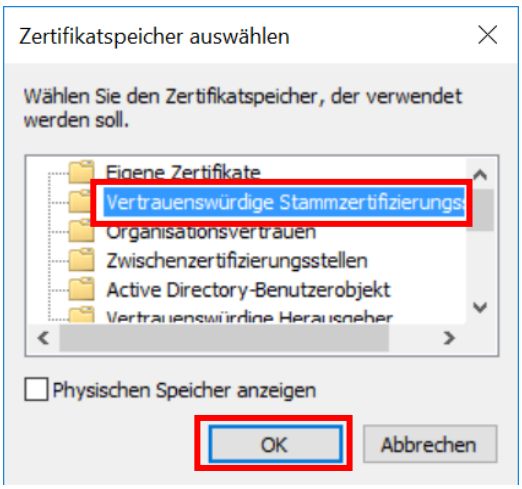

Abbildung 4: Zertifikatspeicher auswählen

Schritt 8:

Im nachfolgenden Fenster „Fertigstellen des Assistenten“ (siehe Abbildung 5) wählen Sie „**Fertig stellen**“.

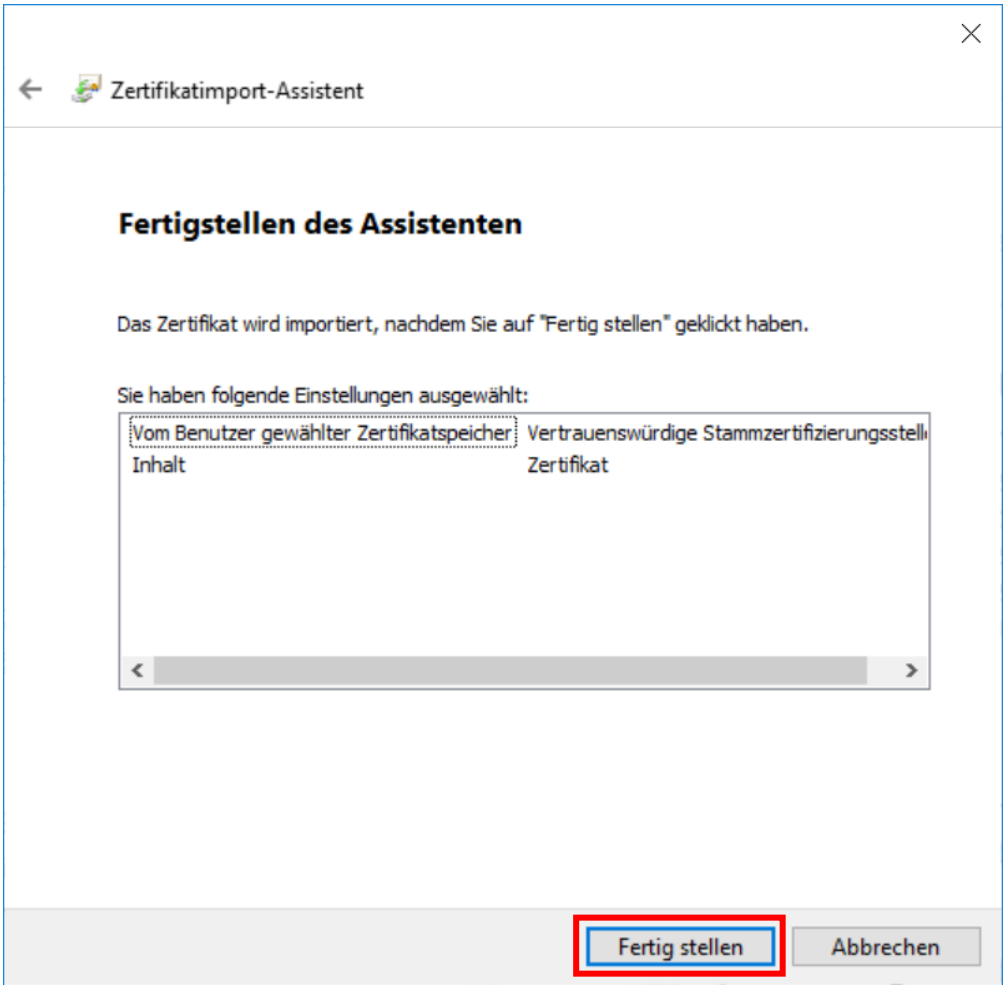

Abbildung 5: Zertifikatimport-Assistent – Fertigstellen des Assistenten

Schritt 9:

Zum Schluss erscheint unter Umständen noch eine „Sicherheitswarnung“ und Sie werden gefragt „*Möchten Sie dieses Zertifikat installieren?“* Klicken Sie 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 im letzten Abschnitt des Dokuments.)

Schritt 10:

Bei der Bestätigungsmeldung über den erfolgreichen Import klicken Sie auf „**OK**“ (siehe Abbildung 6).

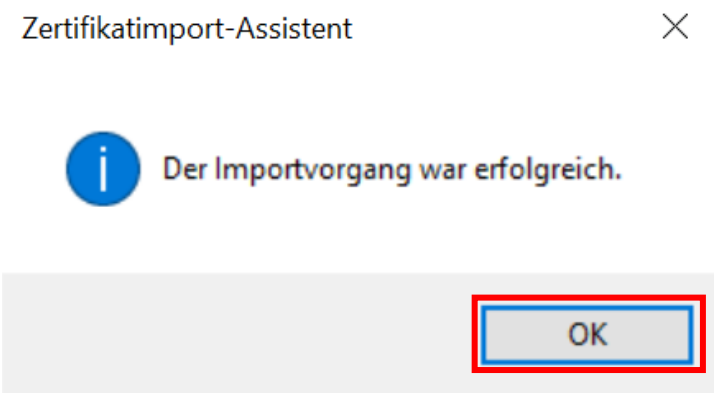

Abbildung 6: Bestätigungsmeldung zur erfolgreichen Installation des Zertifikats

Schritt 11:

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

Der gesamte Vorgang muss auch für das Zertifikat „Zert_CA_ECS_V02_Prod.cer“ wiederholt werden.

Bitte achten Sie jedoch darauf, dass Sie die in Schritt 7 erwähnte Zertifizierungsstelle pro Zertifikat korrekt auswählen. Die Zuordnungen sind in Tabelle 1 aufgelistet.

Für die Verwendung der Testumgebung müssen die Zertifikate „Zert_CA_Root_V02_Test“ und „Zert_CA_ECS_V02_Test“ installiert werden.
Zusätzlich ist auch das „Zert_CA_Root_V02_Prod“ für die Testumgebung notwendig.
Für Gesundheitsdiensteanbieter ohne Zugang zum Testsystem ist diese Funktionalität irrelevant.

Am Ende müssen folgende Zertifikate importiert sein:

- **Zert_CA_Root_V02_Prod (Hauptverband oesterr. Sozialvers.)**
- **Zert_CA_ECS_V02_Prod (Prod ECS CA)**

Für die Verwendung der **Testumgebung** müssen folgende Zertifikate importiert sein:

- **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.)**

Die Zuordnung sollte sein, wie in Tabelle 1 beschrieben:

Umgebung	Vertrauenswürdige Stammzertifizierungsstellen	Zwischenzertifizierungsstellen
PROD	Zert_CA_Root_V02_Prod	Zert_CA_ECS_V02_Prod
TEST	Zert_CA_Root_V02_Test, Zert_CA_Root_V02_Prod	Zert_CA_ECS_V02_Test

Tabelle 1: Übersicht der Zertifizierungsstellen und deren Zertifikate

Die korrekte Zuteilung kann in Google Chrome überprüft werden. Am oberen rechten Fensterrand finden Sie in Google Chrome drei vertikale Punkte, mit denen sich das Chrome-Menü „Anpassungen und Einstellungen“ öffnen lässt. Nachdem Sie es geöffnet haben, sollten Sie die Optionen, wie in Abbildung 7 dargestellt, sehen können. Klicken Sie auf „**Einstellungen**“.

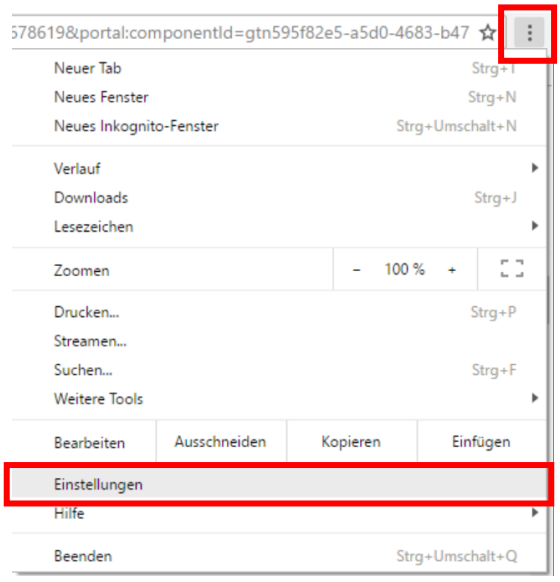

Abbildung 7: Menüpunkt „Einstellungen“ in Google Chrome

Daraufhin wird in Google Chrome ein neuer Tab (Reiter) mit den Einstellungsmöglichkeiten geöffnet. Am linken Rand klicken Sie bitte auf den

Menüpunkt „**Datenschutz und Sicherheit**“, und anschließend auf „**Sicherheit**“ (siehe Abbildung 8).

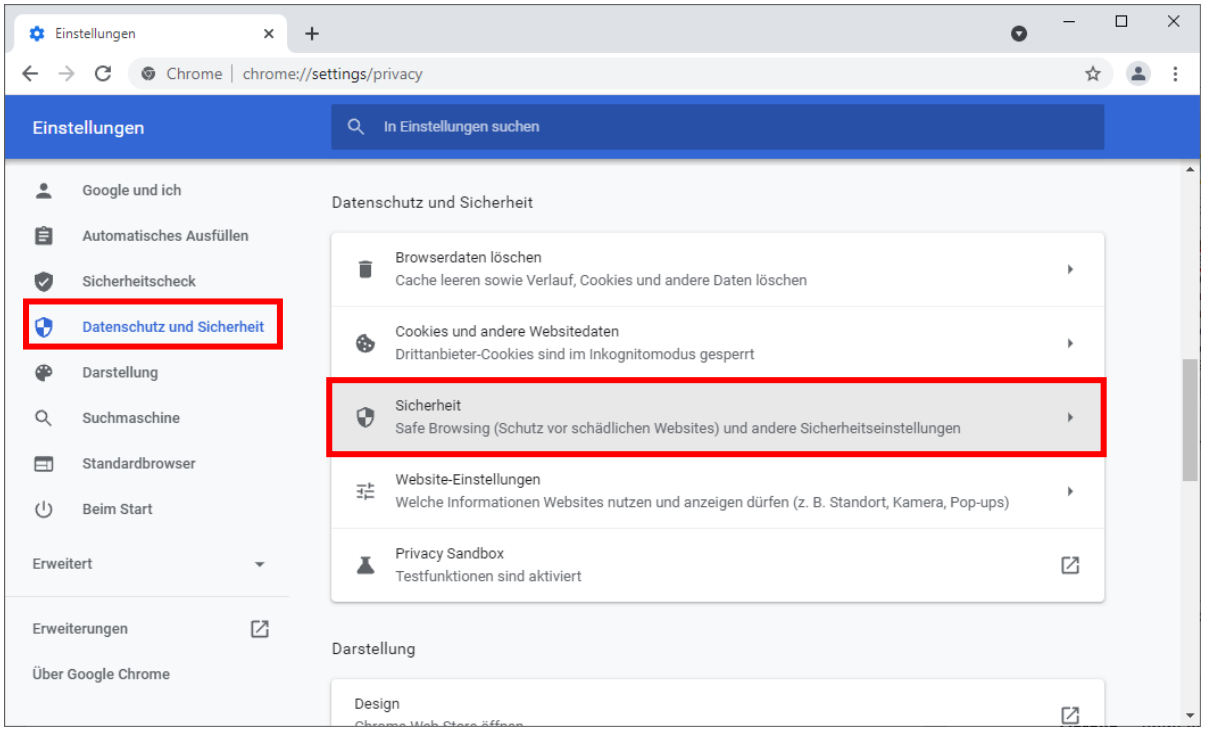

Abbildung 8: Menüpunkt „Datenschutz und Sicherheit“ in Google Chrome

Auf der nun geöffneten Seite „Sicherheit“ scrollen Sie bitte nach unten und klicken Sie auf „**Zertifikate verwalten**“ (siehe Abbildung 9).

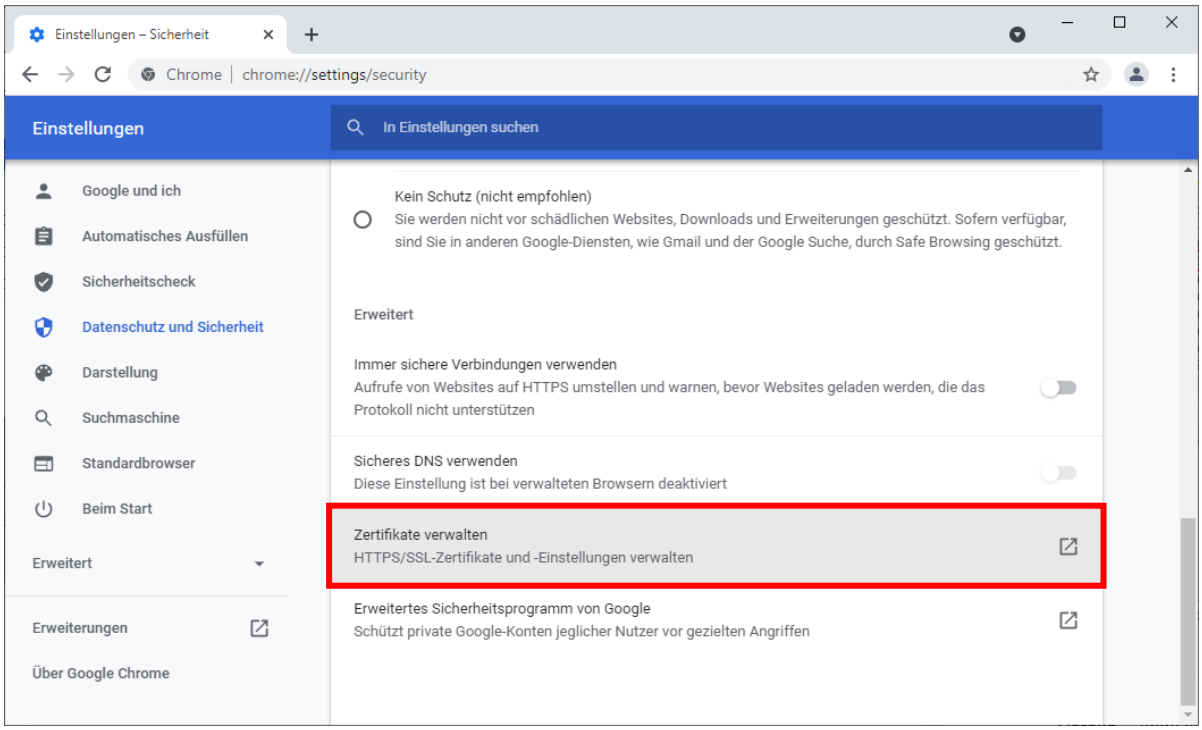

Abbildung 9: Zertifikate verwalten in Google Chrome

Zur Überprüfung kann nun die Übersicht im Fenster „Zertifikate“ herangezogen werden (vgl.
Tabelle 1 und Abbildung 10 bzw. Abbildung 11).

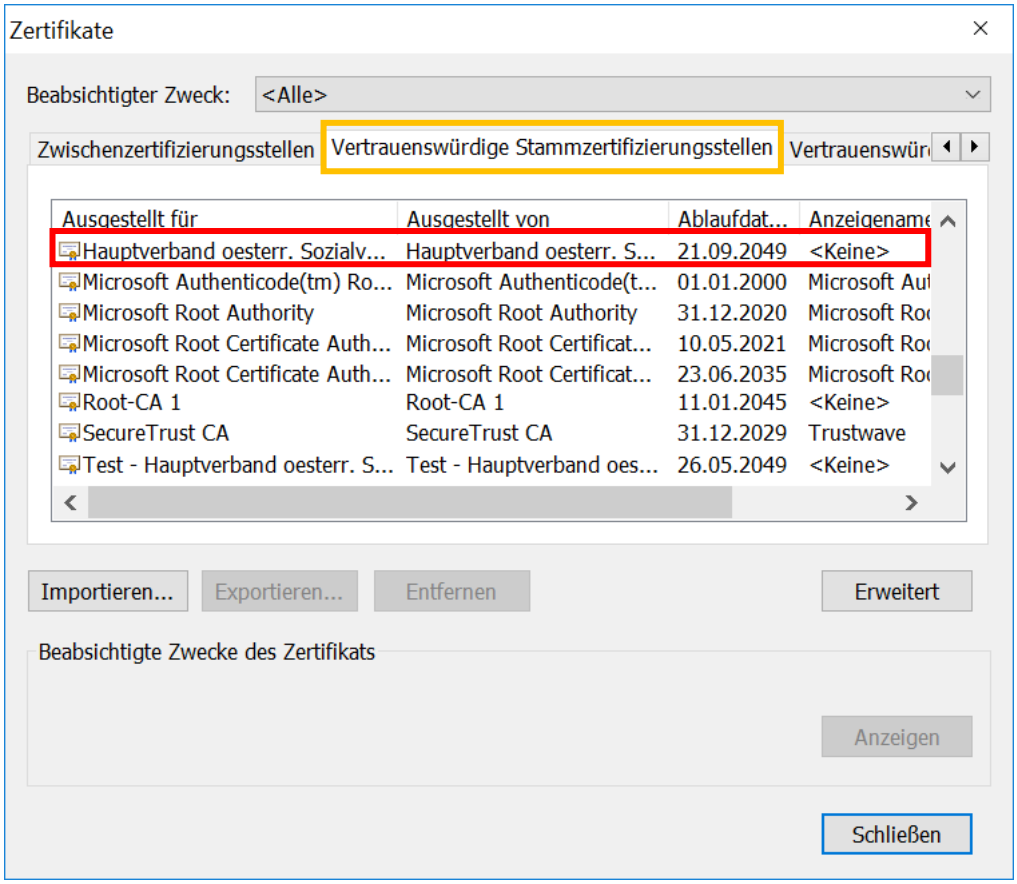

Abbildung 10: Zertifikatsübersicht "Vertrauenswürdige Stammzertifizierungsstellen"

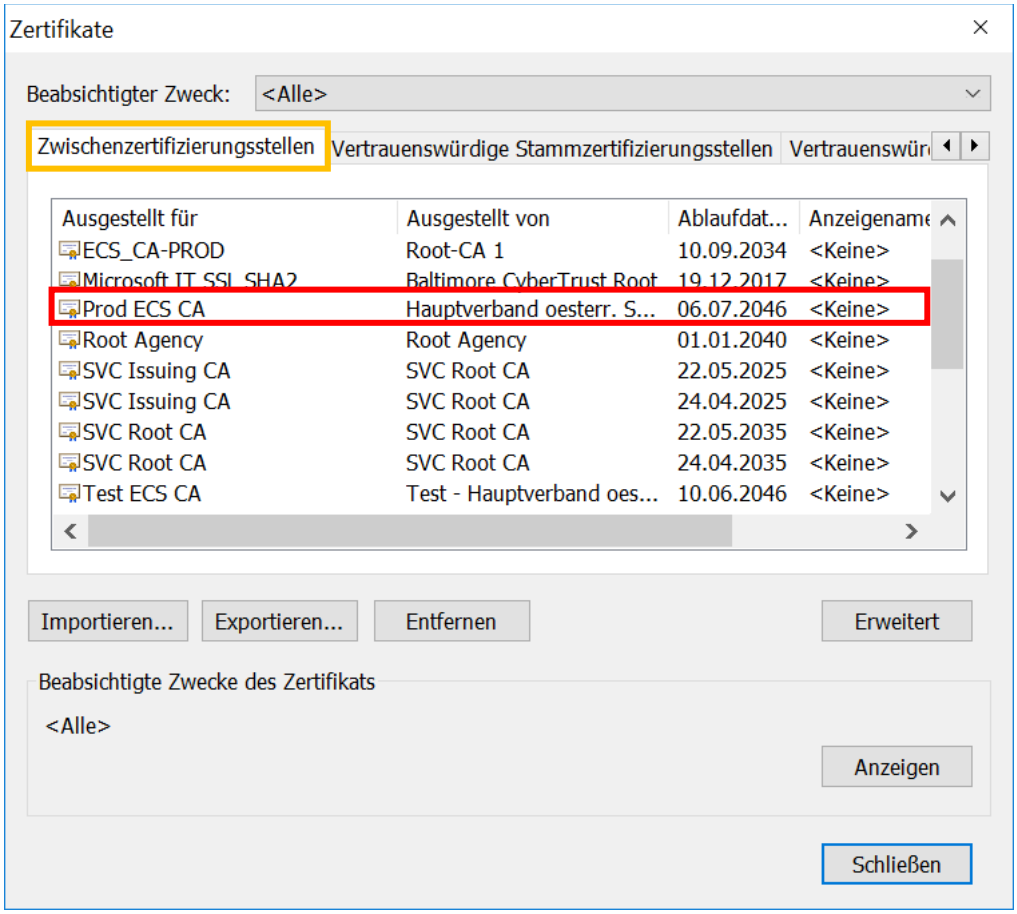

Abbildung 11: Zertifikatsübersicht "Zwischenzertifizierungsstellen"

Durch einen Doppelklick auf das jeweilige Zertifikat – oder auch durch ein Klicken auf „**Anzeigen**“ – wird dieses geöffnet und die Eigenschaften werden in der Registerkarte „**Details**“ angezeigt. Hier sollten Sie die **Signatur (Fingerabdruck)** (grüne Umrandung) überprüfen:

- Hauptverband oesterr. Sozialvers. (siehe Abbildung 12)
- Prod ECS CA (siehe Abbildung 13)

Falls Sie einen Zugang zum Testsystem haben und die zugehörigen Zertifikate installiert haben:

- Test ECS CA (siehe Abbildung 14)
- Test – Hauptverband oesterr. Sozialvers. (siehe Abbildung 15)

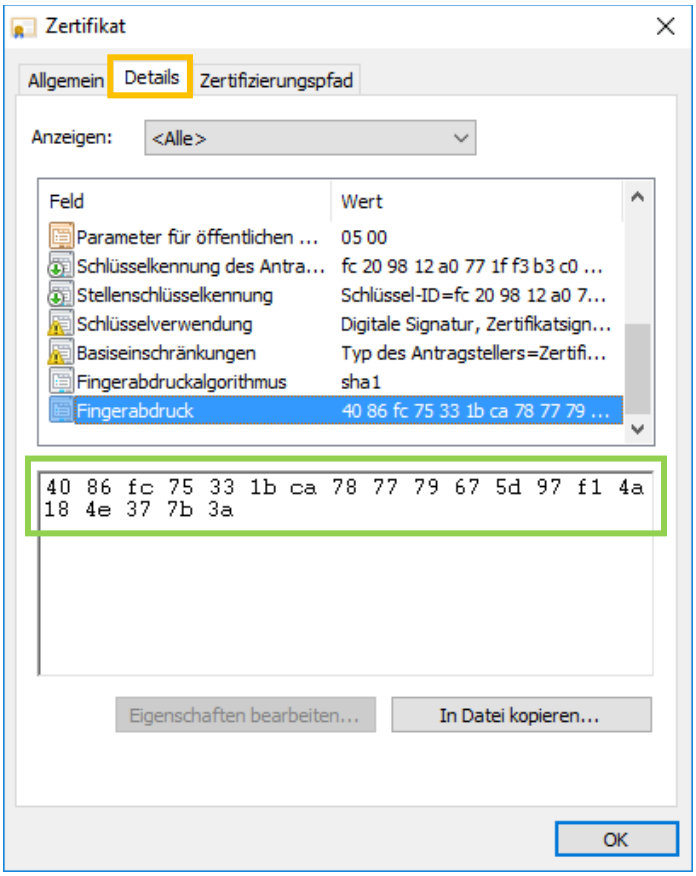

Abbildung 12: Signatur von „Hauptverband oesterr. Sozialvers.“

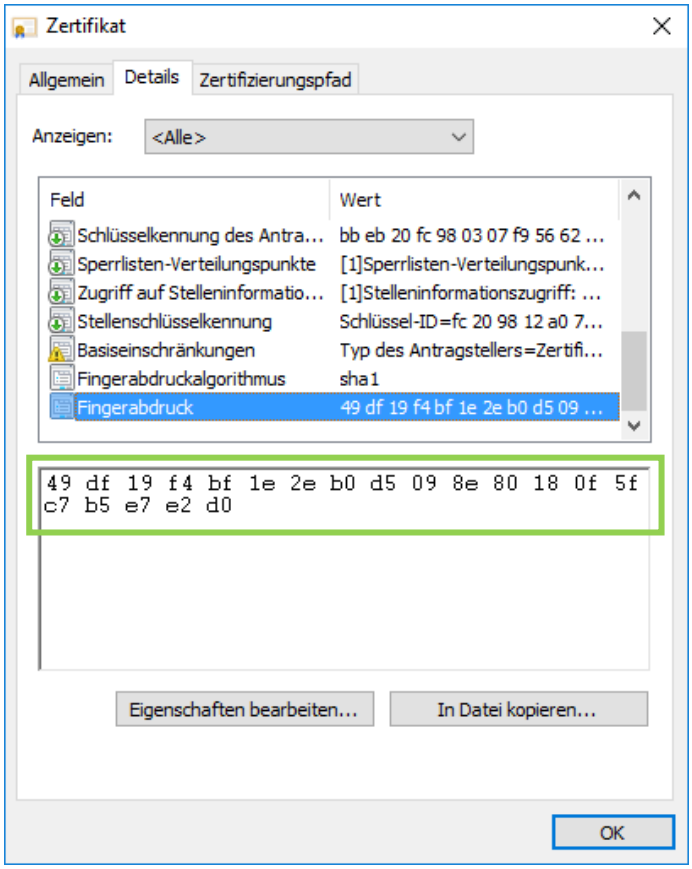

Abbildung 13: Signatur von "Prod ECS CA"

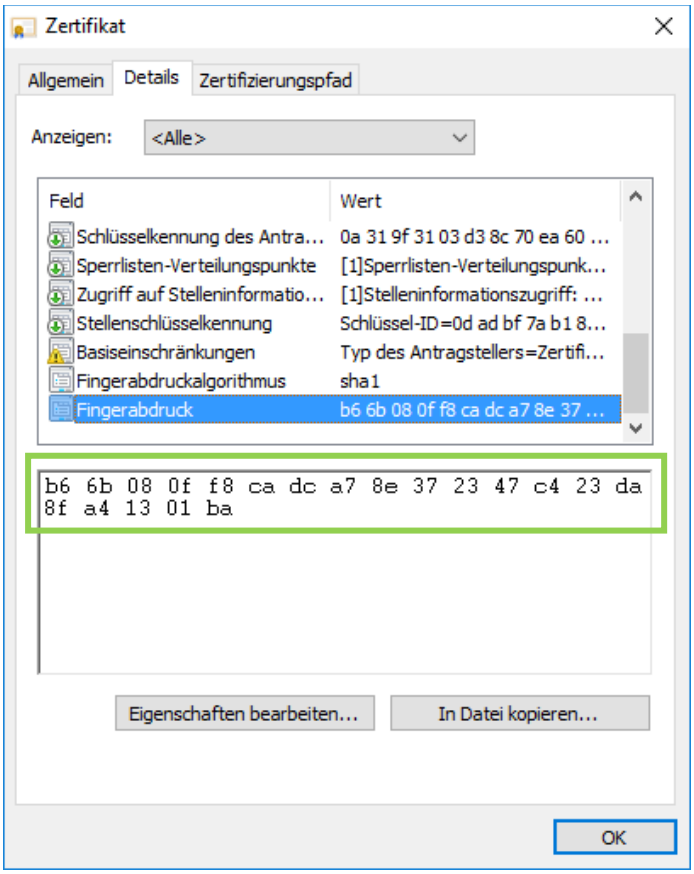

Abbildung 14: Signatur von "Test ECS CA"

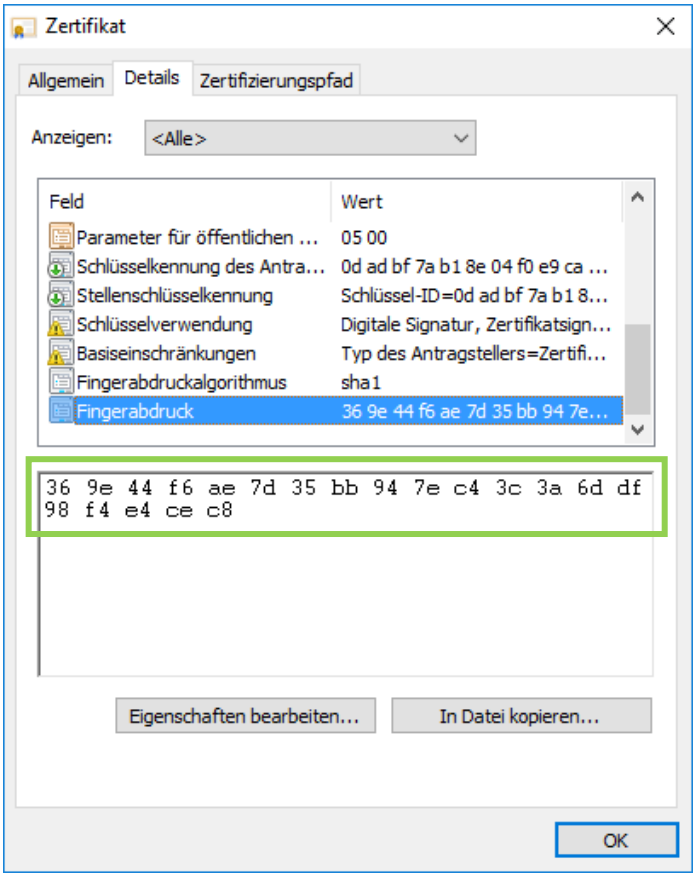

Abbildung 15: Signatur von "Test – Hauptverband oesterr. Sozialvers."