S-T-Dunz GbR
Ewerweg 10, 26723 Emden
Telefon: 04921 / 66772
Telefax: 04921 / 66725
E-Mail: S-T-Dunz@gmx.de

Portierung, Zertifizierung und Installation eines Hardwaretreibers für die Messkarte MeDev-X100 unter dem Betriebssystem Windows Win10

Version 1.0 vom 27. November 2019

Autor: Rolf Andreas Rasenack

Vorwort

Dieses Dokument wird von der Firma STD zur Verfügung gestellt und ist eine Hilfestellung zur Installation des Zertifikates und der anschließenden Installation eines digital signierten Treibers für den Betrieb der Messkarte MeDev-X100 Ver. 2.2.1 unter dem Microsoft Betriebssystem Windows Win10.

Das vorgestellte Verfahren ist ein individueller beispielhafter Lösungsansatz, mit dem ein lokaler Computer mit einem digital signierten Treiber ausgestattet werden kann. Rechte und Pflichten sowie die Einhaltung gesetzlicher Bestimmungen obliegen der Firma EPA GmbH, Bruchköbel.

Emden, den 27. November 2019

Rolf A. Rasenack

Inhaltsverzeichnis:

1. Einleitung

Mit dem neuen Betriebssystem Windows 10 (Win10) von Microsoft werden nicht digital signierte Gerätetreiber bei einem Update aus dem Geräte-Manager entfernt. Daher besteht die Notwendigkeit, Gerätetreiber bei Win10 digital zu signieren, um einen kontinuierlichen Betrieb der Hardware sicher zu stellen.

Diese Beschreibung dient der Dokumentation für die Portierung, das Installieren des Zertifikates und das anschließende Installieren des digital signierten Hardwaretreibers für die Messkarte MeDev-X100 Ver. 2.2.1.

2. Portierung des Hardwaretreibers und deren Zusatzdateien

Der Pfad zum Hardwaretreiber für die Messkarte MeDev-X100 Ver. 2.2.1 des Ableitstrommessystems **LEAK**WATCH sieht wie folgt aus:

C:\Program Files (x86)\EPA Leakwatch\Additional\driver

Unter dem Verzeichnisnamen *driver* befinden sich die bisherigen Treiber. Parallel hierzu wird ein weiterer Verzeichniseintrag erzeugt. Dieser wird mit dem Kürzel DS für Digitale Signierung erweitert, so dass sich dann folgender Pfad ergibt:

C:\Program Files (x86)\EPA Leakwatch\Additional\driver_DS

Damit wird ein neues Verzeichnis geschaffen, ohne dass die „alten Treiber“ weichen müssen. In dem Ordner …*driver_DS* müssen folgende Dateien enthalten sein:

EPA.pfx
stm32f103_win10_epa.inf
stm32f103_win10_epa.cat

Allgemeine Vorgehensweise:

- Der o. a. Pfad mit den Dateien wird auf dem Zielcomputer installiert.
- Die Zertifikat Datei *EPA.pfx* wird danach installiert. Der Vorgang hierzu ist im Kapitel 3. beschrieben.
- Die Installation des Hardwaretreibers wird im Kapitel 4. beschrieben.
- Informationen zum Zertifikat können mit der Microsoft Management Console eingeholt werden (Kapitel 5.).

3. Installation des Zertifikates

Die Installation der Zertifikatdatei wird in diesem Kapitel beschrieben. Mit ihrer Hilfe wird der Hardwaretreiber digital signiert.

- Zunächst öffnet man den Ordner, in dem die Zertifikatdatei (*EPA.pfx*) gespeichert ist. Der folgende Pfad führt zur Zertifikatsdatei:

  C:\Program Files (x86)\EPA Leakwatch\Additional\driver_DS

- Mit Doppelklick auf die Datei *EPA.pfx* kann der Installationsprozess eingeleitet werden. Es öffnet sich das Fenster *Zertifikatimport-Assistent*. Als Speicherort gibt man *Lokaler Computer* an.

Bild 3.1: Zertifikatimport-Assistent Willkommen- Fenster [1]

- Mit *Weiter* gelangt man zum nächsten Fenster (Bild 3.1), in diesem Fenster definiert man den Pfad der zu importierenden Datei. Das ist die Datei *EPA.pfx* mit ihrem entsprechenden Pfad. Mit Weiter folgt das nächste Fenster.

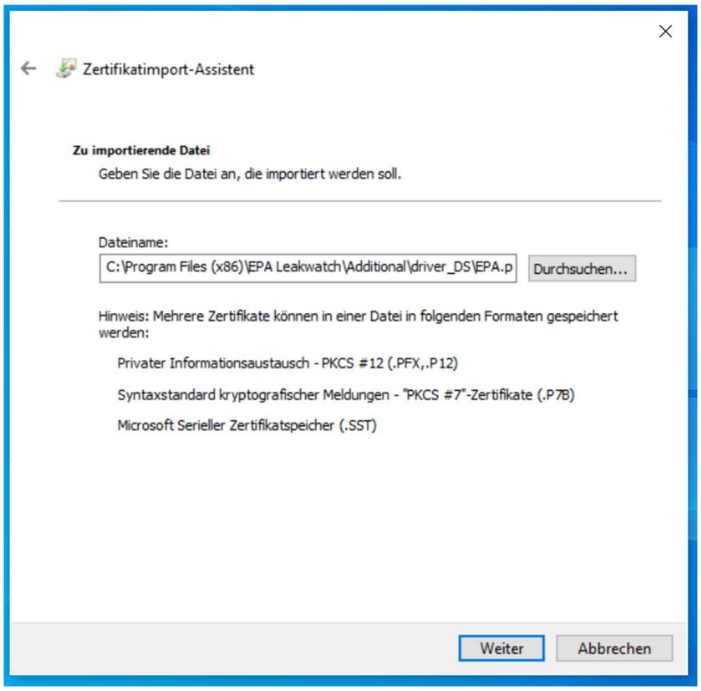

Bild 3.2: Zertifikatimport-Assistent Import- Fenster [1]

- Dieses Fenster (Bild 3.3) dient dem Schutz für den privaten Schlüssel. Daher muss ein Kennwort eingetragen werden. Hier trägt man als Passwort ***EPA_leakwatch*** ein. Als Importoption belässt man es bei der Option *Alle erweiterten Eigenschaften mit einbeziehen*. Anschließend klickt man auf *Weiter*.

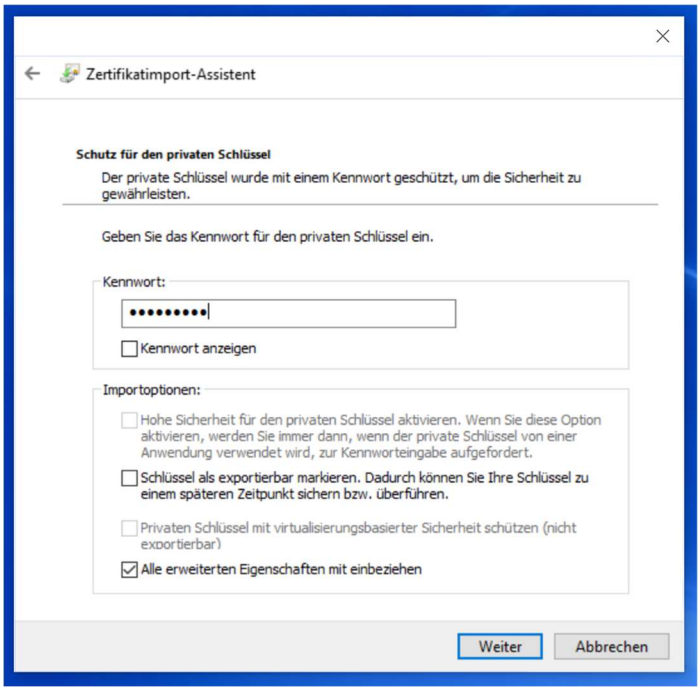

Bild 3.3: Zertifikatimport-Assistent Schutz für den priv. Schlüssel- Fenster [1]

Jetzt wird der Zertifikatspeicher ausgewählt. Dazu wird der Punkt *Alle Zertifikate in folgendem Speicher speichern* ausgewählt. Man klickt auf *Durchsuchen*, um dann als Zertifikatspeicher *Vertrauenswürdige Stammzertifizierungsstellen* auszuwählen.

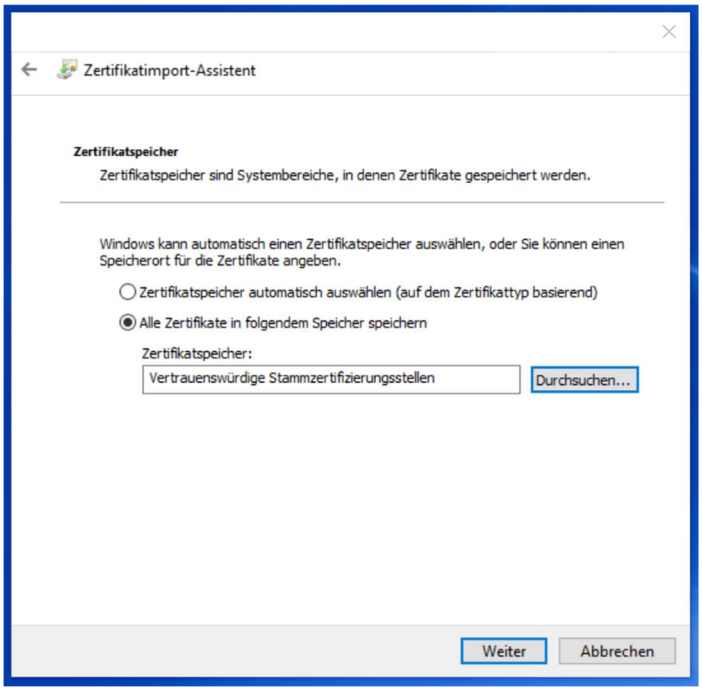

Bild 3.4: Zertifikatimport-Assistent Zertifikatspeicher [1]

Mit dem Klicken auf Weiter gelangt man zu dem Import-Fenster. Hier werden noch einmal die gemachten Angaben gezeigt. Nach dem Klicken auf *Fertig stellen* wird das Zertifikat importiert.

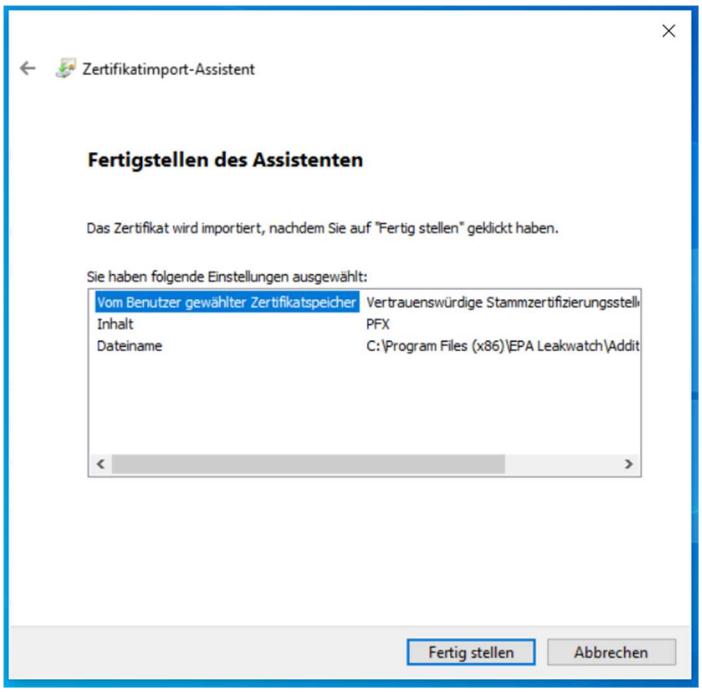

Bild 3.5: Zertifikatimport-Assistent Fertigstellen des Assistenten [1]

- Nach dem Klicken auf *Fertig stellen* wird ein kleines Fenster geöffnet, in dem der erfolgreiche Importvorgang bestätig wird. Dieses Fenster wird durch Klicken auf *ok* abgeschaltet.

Das Zertifikat ist nach diesem Prozess am richtigen Ort importiert worden.

4. Installation des Hardwaretreibers

Um den Hardwaretreiber zu installieren, wird der Computer hochgefahren und die Messkarte MeDev-X100 Ver. 2.2.1 wird an den Computer angeschlossen. Es wird davon ausgegangen, dass der Nutzer Admin-Rechte besitzt.

- Jetzt muss der „alte“ Hardwaretreiber deinstalliert werden. Dazu wird der Geräte-Manager geöffnet, in dem man auf das Windows Symbol links unten in der Ecke des Monitors mit der rechten Maustaste klickt und dann den Geräte-Manager auswählt. Sogleich öffnet sich das Fenster des Geräte-Managers und gibt über die installierte Hardware Auskunft.
- Danach wird auf den „alten“ Treiber mit der rechten Maustaste geklickt, um ein Fenster zu öffnen, das den Prozess zum Deinstallieren einleitet. Man setzt den Haken für *Treibersoftware für dieses Gerät löschen* und klickt dann auf *deinstallieren*. Damit ist dann der „alte“ Hardwaretreiber vom Computer gelöscht.

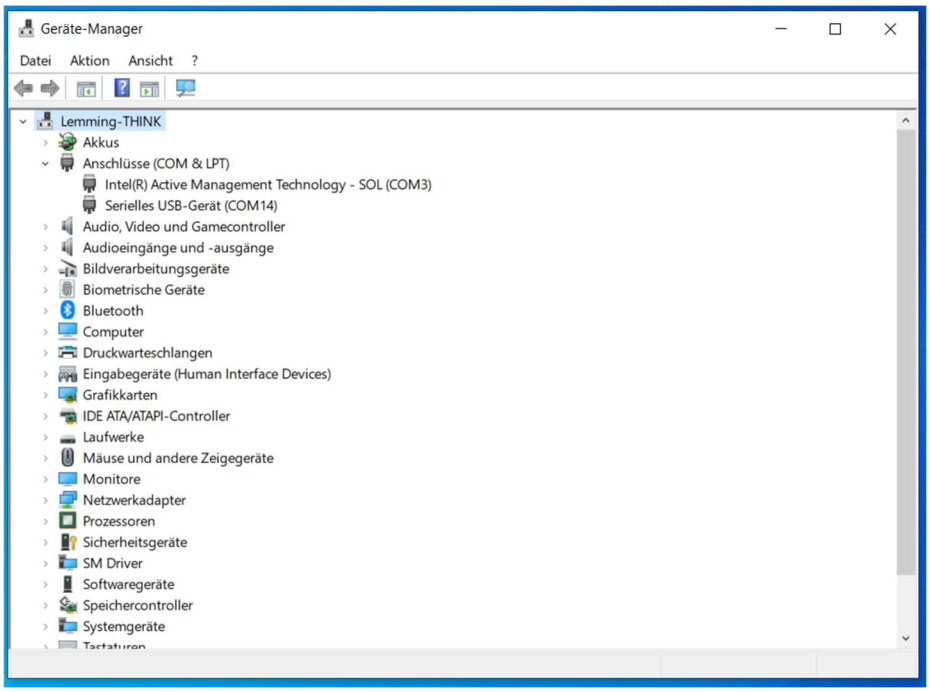

Bild 4.1: Geräte Manager [2]

- Bild 4.1 zeigt die Liste der Hardwarekomponenten im Geräte-Manager. Die Messkarte MeDev-X100 Ver 2.2.1 ist angeschlossen und wird als *Serielles USB-Gerät (hier COM14)* angezeigt. Mit der rechten Maustaste klickt man auf *Serielles USB-Gerät (COM14)* und gelangt dann zu einem weiteren Fenster.

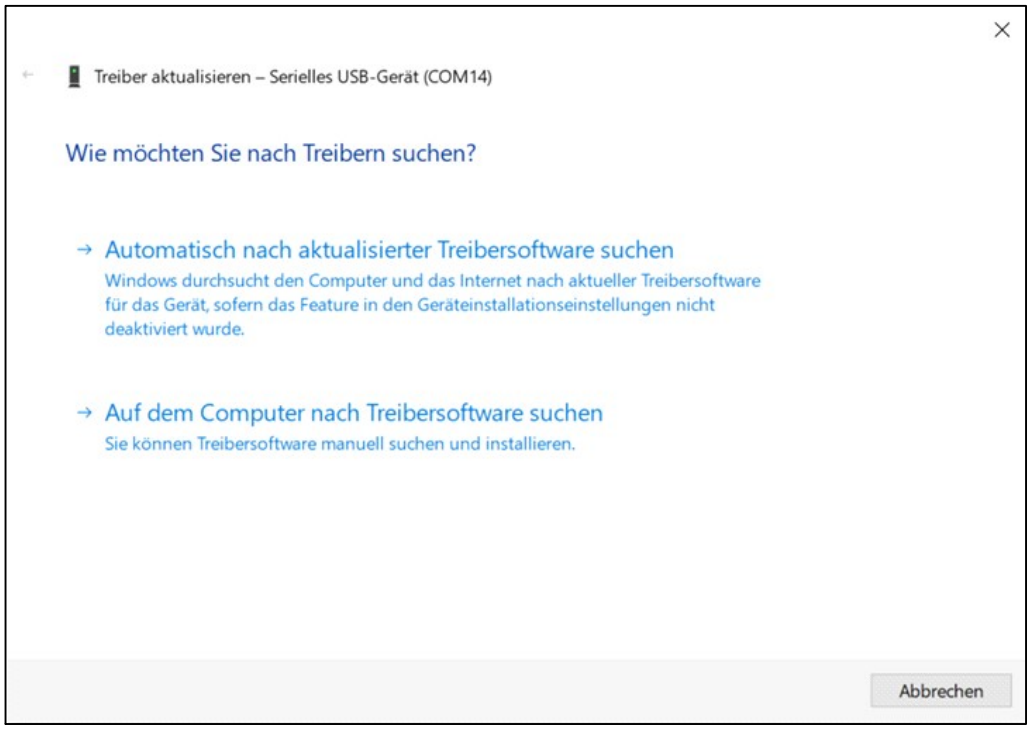

Bild 4.2: Treiber aktualisieren [2]

- Danach wird *Auf dem Computer nach Treibersoftware suchen* (Bild 4.2) geklickt. Von hier aus gelangt man zu einem weiteren Fenster, bei dem man eine Liste der verfügbaren Treiber erhalten kann.

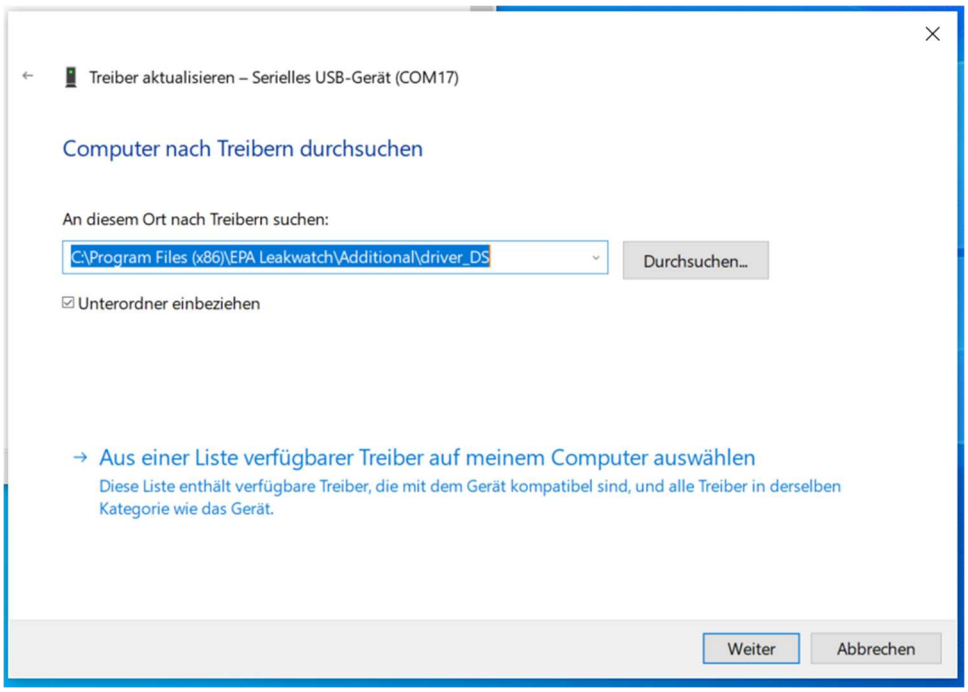

Bild 4.3: Computer nach Treibern durchsuchen [2]

- Nach dem *Aus einer Liste verfügbarer Treiber auf meinem Computer auswählen* gedrückt worden ist, erscheint ein Fenster (Bild 4.4) mit der entsprechenden Treiberliste. Diese Liste ist jedoch zweitrangig. Wichtig ist an dieser Stelle, dass man auf Datenträger drückt um gezielt einen Treiber auswählen zu können.

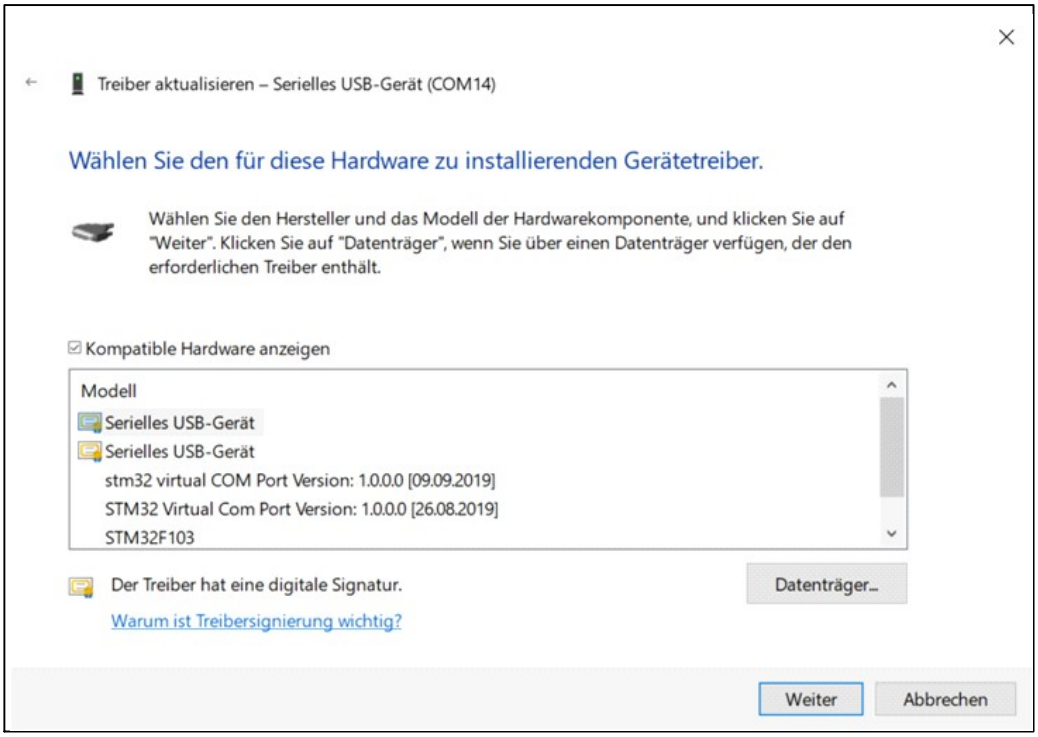

Bild 4.4: Liste verfügbarer Treiber [2]

- Bild 4.5 wird dargestellt und man muss den Pfad zu dem digital signierten Treiber angeben. Hier ist das der folgende Pfad:

C:\Program Files (x86)\EPA Leakwatch\Additional\driver_DS

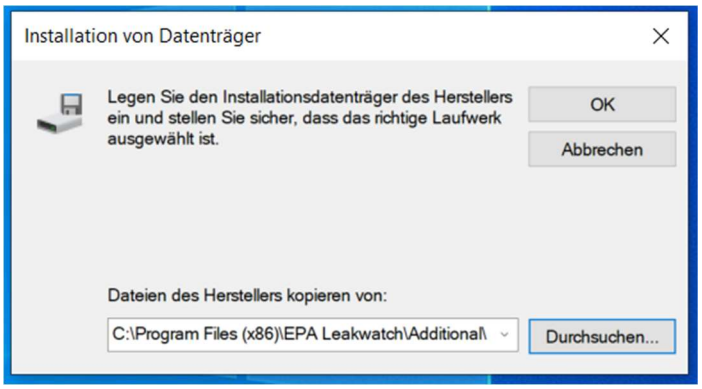

Bild 4.5: Pfad zum digital signierten Treiber [2]

- Mit dem Klicken auf *OK* wird der Pfad bestätigt und es öffnet sich jetzt ein Fenster (Bild 4.6) mit dem aktuell digital signierten Treiber.

- Dieser Treiber *stm32 virtual Com Port* wird ausgewählt und mit *Weiter* installiert.

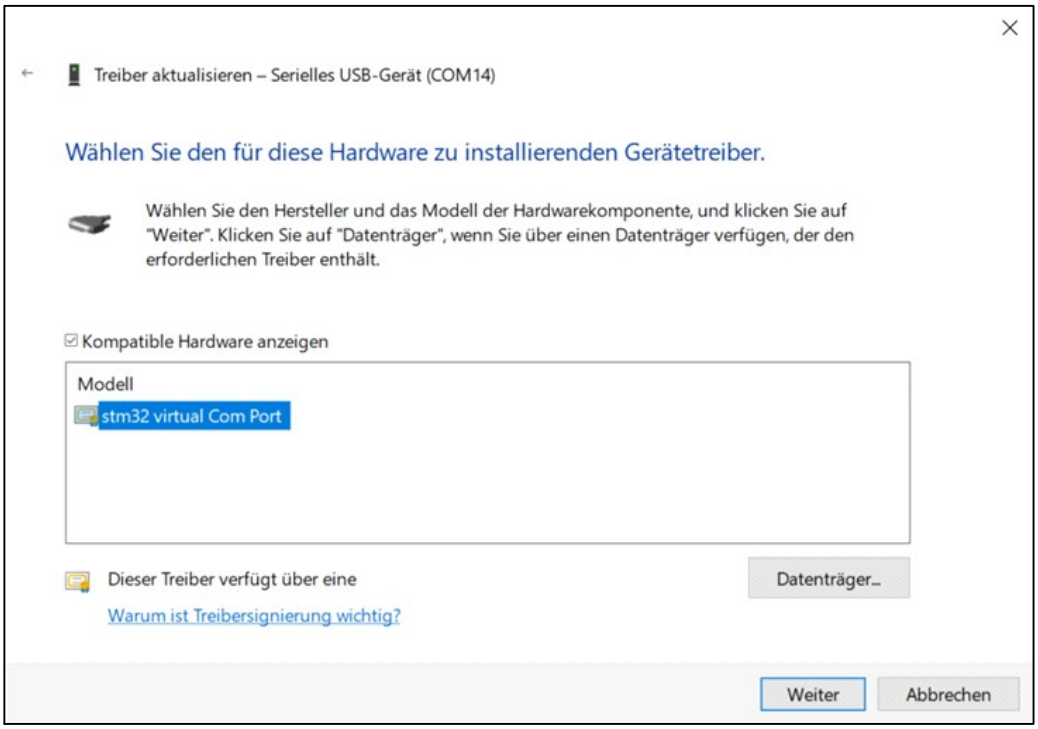

Bild 4.6: Aktueller digital signierter Hardwaretreiber [2]

- Nachdem man *Weiter* geklickt hat, erscheint Bild 4.7. Hier wird mit dem Klicken auf Installieren letztendlich der Hardwaretreiber installiert.

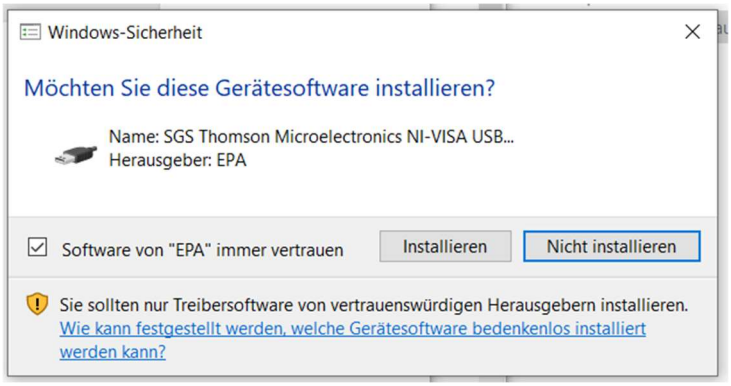

Bild 4.7: Windows Sicherheitsinformation [2]

- Nach der Installation wird das Bild 4.8 als letztes Fenster gezeigt, um den Abschluss der Treiberinstallation zu zeigen.

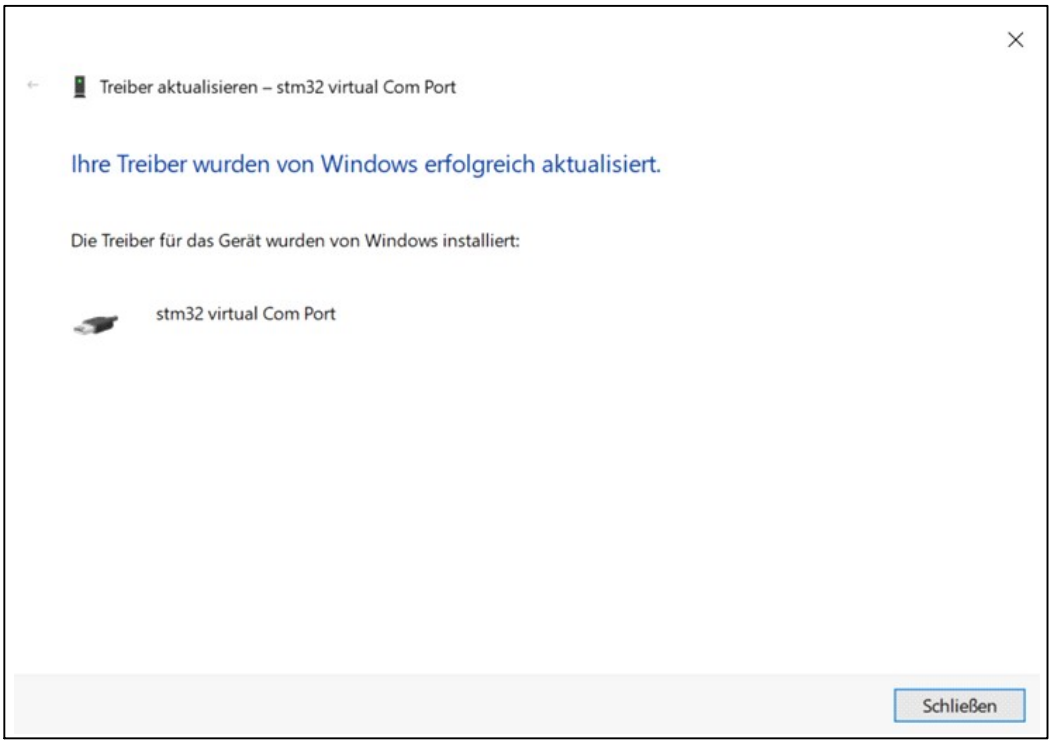

Bild 4.8: Abschluss Treiberinstallation [2]

- Im Geräte Manager wird der neue Treiber als *NI-VISA USB Device* mit dem Namen *stm32 virtual COM Port* angezeigt.

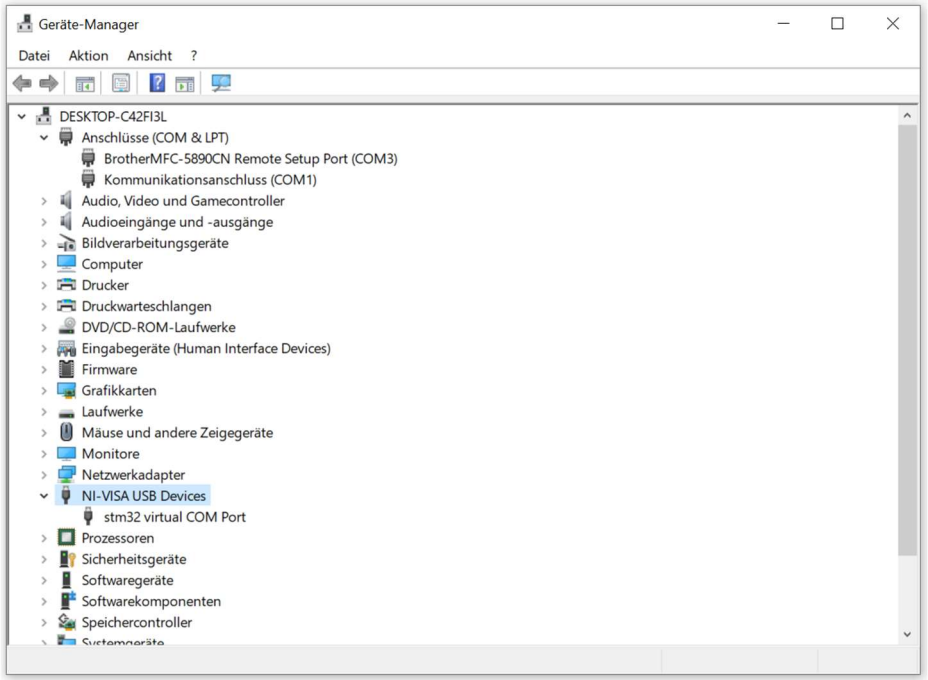

Bild 4.9: Geräte-Manager mit neu installierten Treiber [2]

Damit ist der Treiber erfolgreich installiert und kann jetzt für den angegebenen Zeitraum (siehe Kapitel 5.) benutzt werden. Nach Ablauf dieser Frist muss ein neues Zertifikat erzeugt werden und wieder digital signiert werden.

5. Überprüfung des Gültigkeitszeitraumes für das Zertifikat

In diesem Kapitel wird erläutert, wie man den Gültigkeitszeitraum für das Zertifikat überprüfen kann. Die hier beschriebene Vorgehensweise dient der Information über das Zertifikat. Für die Portierung, Zertifizierung und Installation des Hardwaretreibers für die Messkarte MeDev-X100 unter dem Betriebssystem Windows Win10, wird dies nicht benötigt.

Mit Hilfe der Microsoft Management Console (mmc.exe) kann man die Gültigkeit des Zertifikats überprüfen. Außerdem ist es möglich, verschiedene andere Informationen über das Zertifikat, beispielsweise der Laufzeit, zu erhalten.

Nachfolgend ist das Aufrufen der Microsoft Management Console beschrieben:

- Zunächst wird das Fenster zur Eingabeaufforderung geöffnet. Man drückt die *Windows-Taste* gleichzeitig mit der Buchstabentaste *r*. Danach erscheint dann die Eingabeaufforderung und man kann den Befehl *mmc* eingeben.

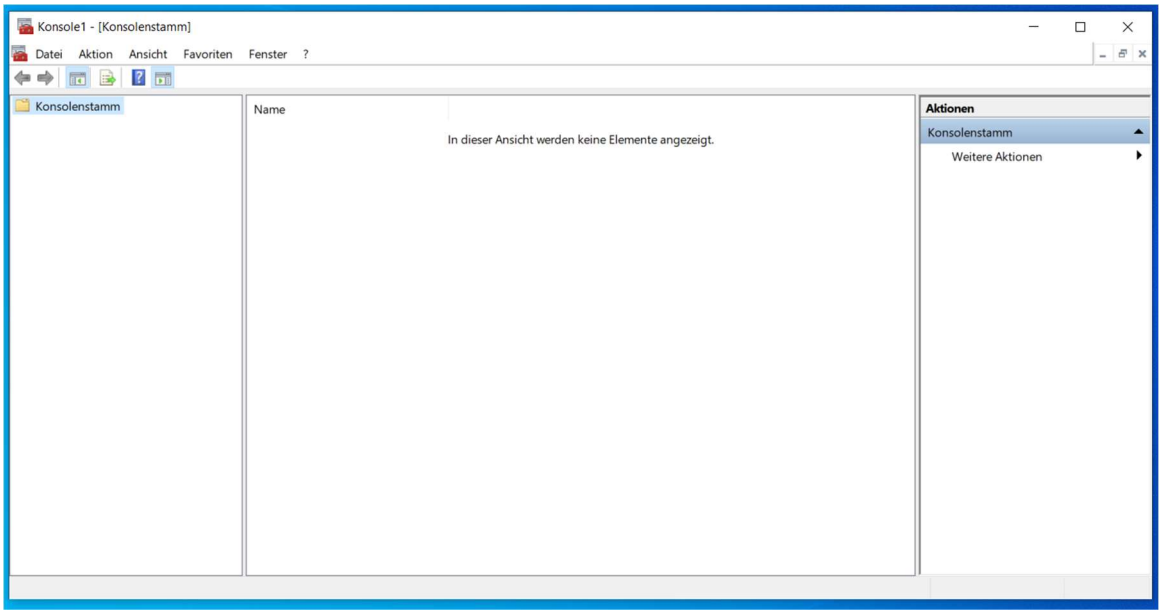

Bild 5.1: Konsolenstamm der mmc ohne Eintrag [3]

- Es öffnet sich der Konsolenstamm (Bild 5.1), ohne dass dort ein Eintrag zu sehen ist.
- Durch Klicken auf *Datei* wird ein Fenster geöffnet, bei dem man die Funktion *Snap-In hinzufügen/ entfernen…* auswählt.

- In dem folgenden Fenster (Bild 5.2) wird dann *Zertifikate* ausgewählt und dann unter der Rubrik *Ausgewählte Snap-Ins:* hinzugefügt.

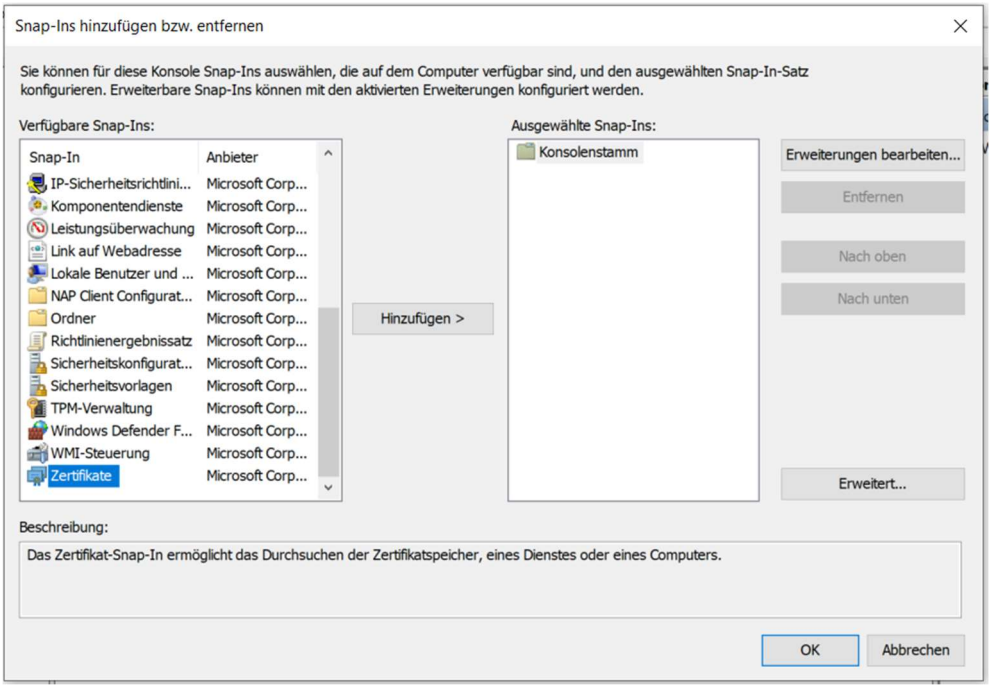

Bild 5.2: Snap-Ins hinzufügen [3]

- Durch klicken auf *Hinzufügen* erscheint dann folgendes Fenster (Bild 5.3). Hier wählt man dann die Option *Computerkonto* und klickt dann auf weiter.

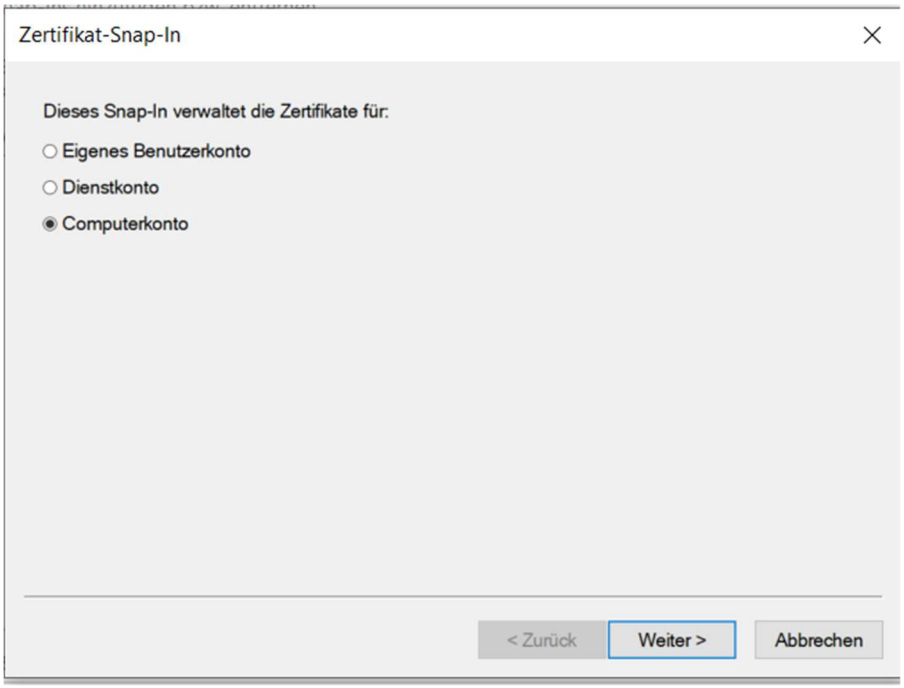

Bild 5.3: Kontoauswahl [3]

- Man belässt die Markierung auf *Lokalem Computer* (…) und klickt dann auf *Fertig stellen* (Bild 5.4).

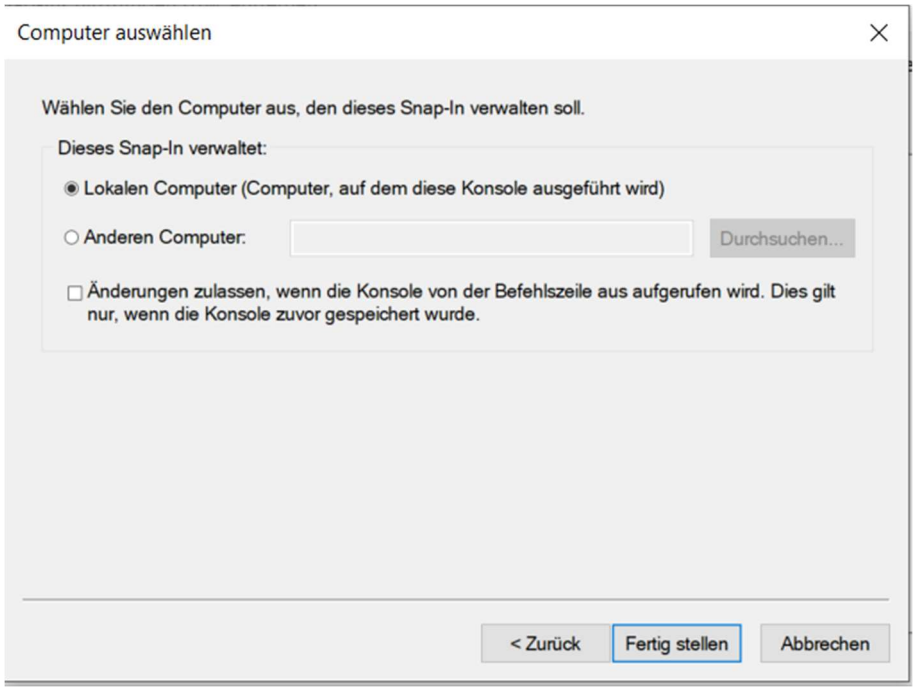

Bild 5.4: Computerauswahl [3]

- Man sieht jetzt den Eintrag *Zertifikate* unter der Rubrik *Ausgewählte Snap-Ins:*. Dieses Fenster (Bild 5.5) verlässt man durch Klicken auf *OK*.

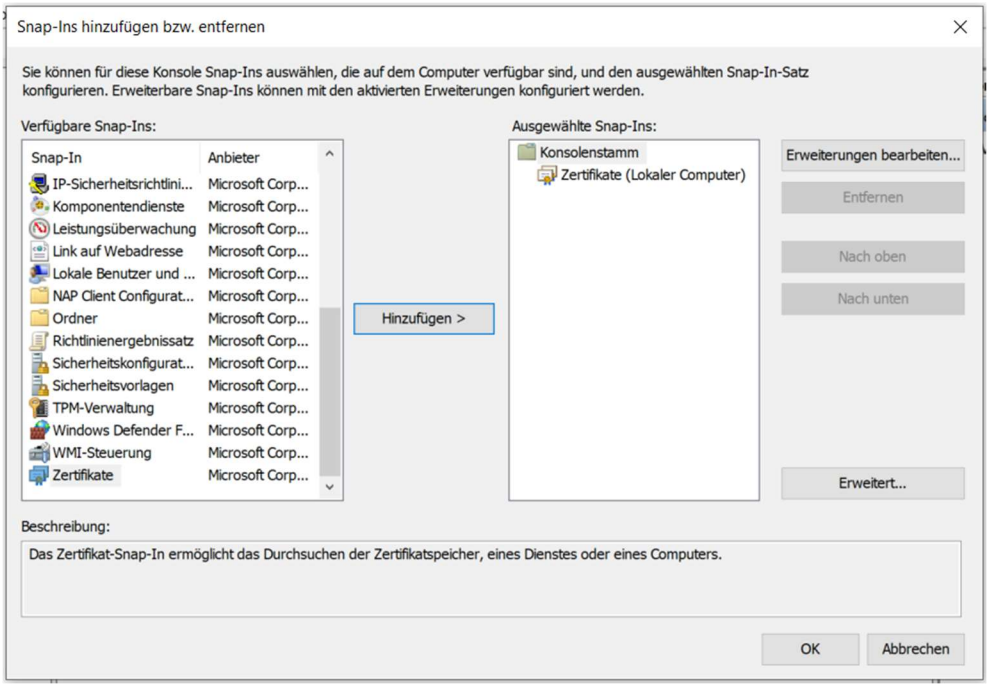

Bild 5.5: Snap-Ins hinzufügen mit Eintrag [3]

- Es zeigt sich wieder der Konsolenstamm von Bild 5.1 jetzt mit dem Eintrag *Zertifikate (Lokaler Computer)* unter der Rubrik *Name*.
- Im Konsolenstamm wird > *Zertifikate* angezeigt. Man klickt auf den Pfeil, der nach rechts zeigt. Danach öffnet sich ein Menü mit einer Liste von verschiedenen Zertifizierungsstellen.

- Man wählt *Vertrauenswürdige Stammzertifizierungsstellen* aus, indem man auch hier den Pfeil nach rechts klickt.
- Es erscheint das Untermenü *Zertifikate*. Durch Klicken auf Zertifikate erscheint dann eine Liste der Zertifikate, die auf dem lokalen Computer gespeichert sind. Das Bild 5.6 wird dann sichtbar.

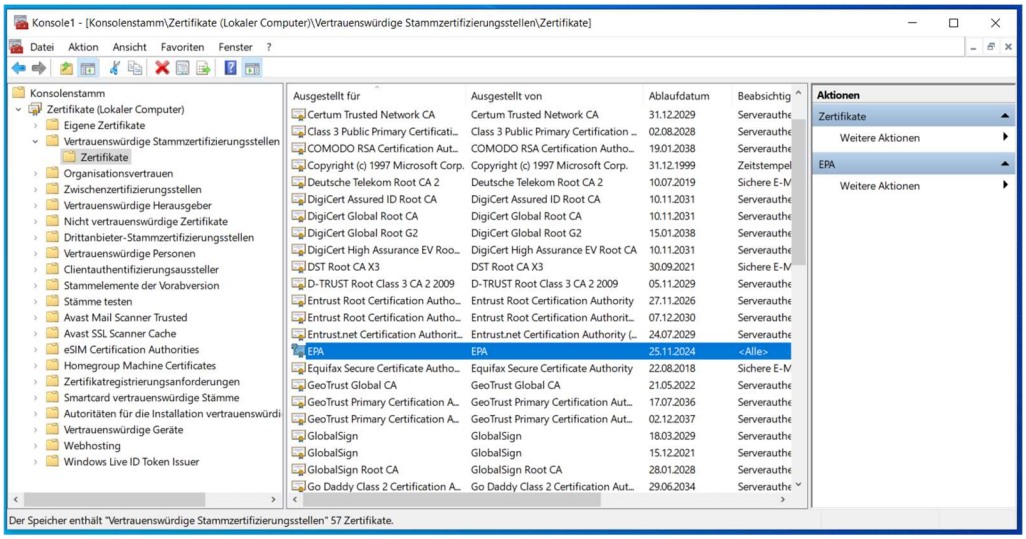

Bild 5.6: Liste der Zertifikate [3]

- Durch scrollen gelangt man dann zum Zertifikat EPA (Bild 3.11). Nach dem Doppelklicken auf EPA zeigt sich dann das Bild 3.12.

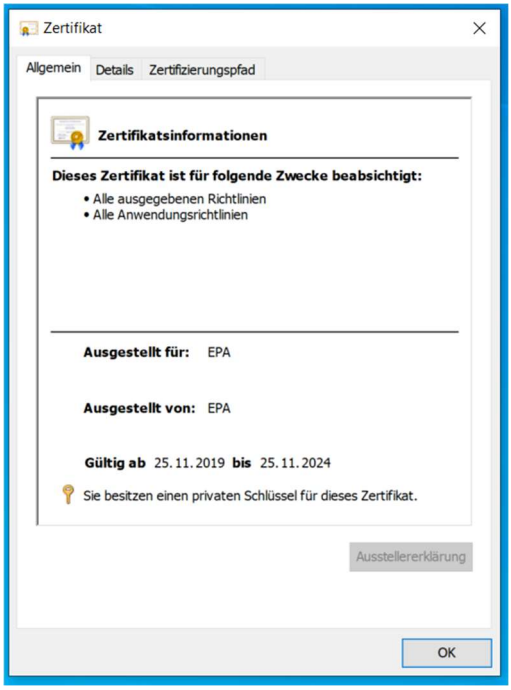

Bild 3.12: Informationen zum Zertifikat LEM [3]

Hier kann man Informationen, wie beispielsweise die Gültigkeit des Zertifikates, abrufen.

6. Quellenverzeichnis

[1] Bilder aus Microsoft Zertifikatimport-Assistent

[2] Bilder aus Microsoft Geräte-Manager

[3] Bilder aus Microsoft Management Console