Anleitung

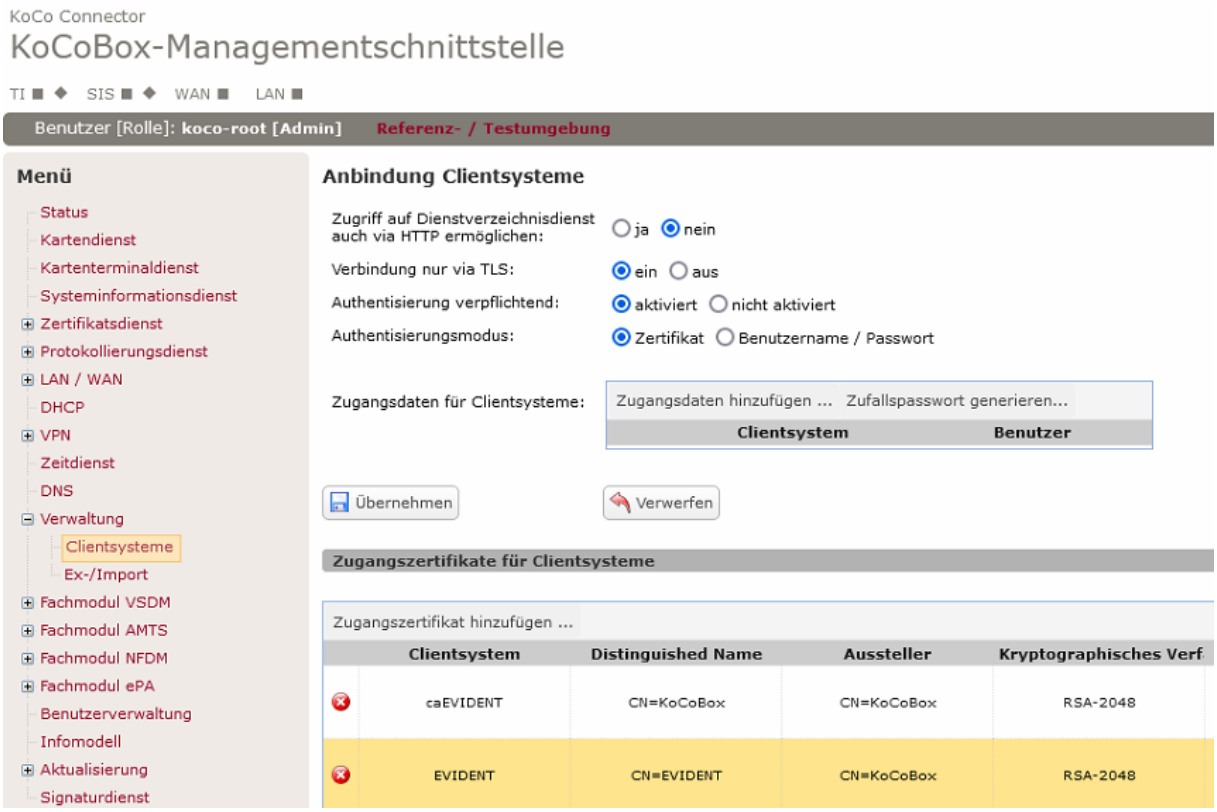
In dieser Anleitung ist beschrieben, wie Sie in der KoCoBox ein neues Clientzertifikat generieren und in allen relevanten Programmteilen einspielen. Diese Schritte sollte auf jeden Fall Ihr DVO (Dienstleister vor Ort) durchführen.

Die Anleitung unterteilt sich in insgesamt 5 Schritte:

1. Clientzertifikat in der KoCoBox generieren und herunterladen
2. Clientzertifikat in den Konnektor Manager importieren
3. LDAP und WCS/ECS
4. Clientzertifikat für das eRezept hinterlegen
5. Einspielen des neuen Clientzertifikats in den KIM Client

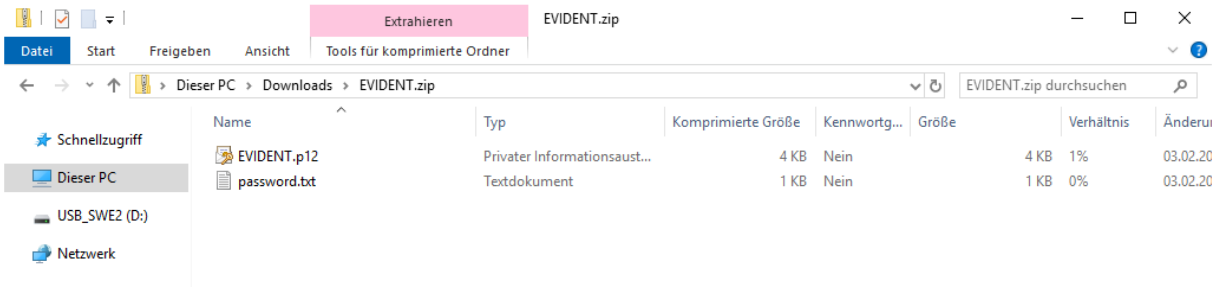
1. Clientzertifikat in der KoCoBox generieren und herunterladen

Wichtiger Hinweis: Beachten Sie bitte, dass in Verbindung mit EVIDENT derzeit bei allen Konnektoren **ausschließlich RSA-Clientzertifikate** erstellt und verwendet werden können.
Das Zertifikat für die TLS-Verbindung wird innerhalb der **KoCoBox-Managementschnittstelle** erzeugt. Verwenden Sie für diesen Schritt bitte ausschließlich den Browser **Mozilla Firefox**, wie von der **CompuGroup** empfohlen.



Im Bereich **Verwaltung Clientsysteme** wählen Sie die Option **Zugangszertifikat hinzufügen....** Damit werden Sie aufgefordert die im Infomodell hinterlegte Clientsystem-ID anzugeben, diese entspricht in unserem Fall immer **EVIDENT**.

Danach wird für diese Clientsystem-ID ein TLS-Zertifikat generiert und anschließend startet der Download automatisch. Das hierbei erzeugte Dateiarchiv, mit der Zertifikatsdatei und einer Textdatei mit dem automatisch generierten Passwort, landet üblicherweise im Ordner **Downloads**.

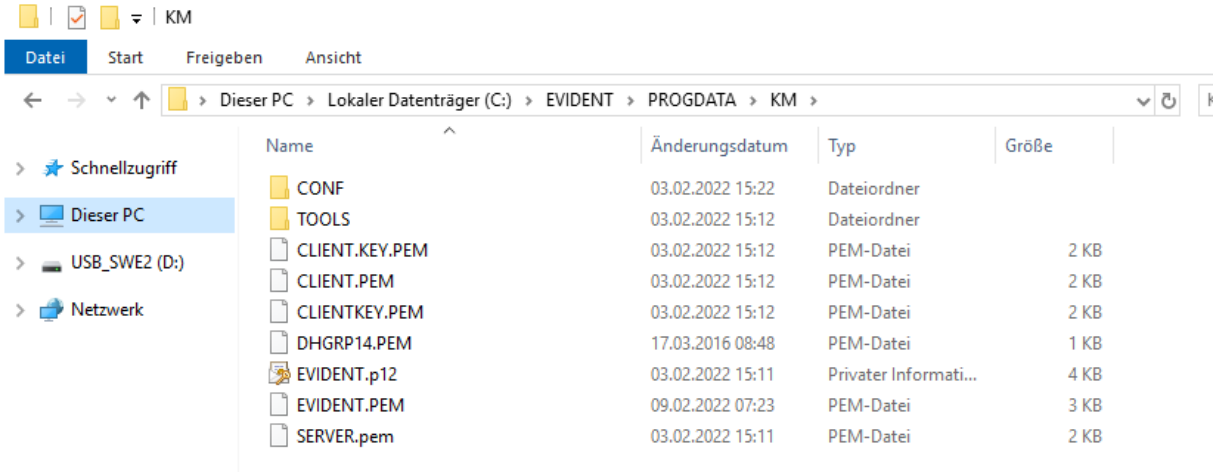


Legen Sie das Dateiarchiv am besten an einem zentralen Ort im EVIDENT-Verzeichnis ab z.B. \\SERVER\EVIDENT\ZERTIFIKATE. Wenn noch nicht vorhanden, bitte den Ordner **ZERTIFIKATE** erstellen.

Sie benötigen das Clientzertifikat nicht nur für unseren Konnektormanager, sondern auch für die LDAP und eRezept Anbindung im EVIDENT und für den KIM Client.

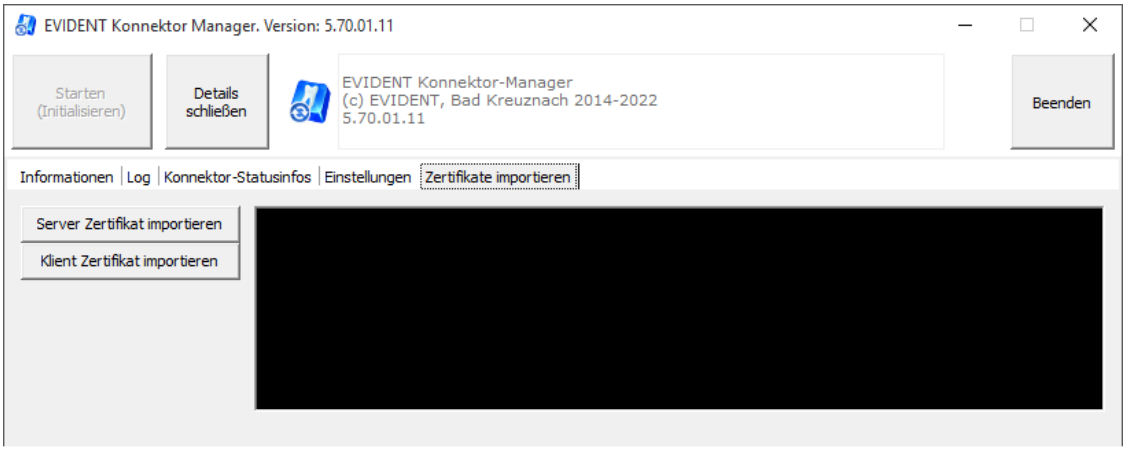
2. Clientzertifikat in den Konnektor Manager importieren

Bevor Sie das neue Clientzertifikat wieder in den **Konnektor Manager** importieren, müssen Sie erst noch eine bestimmte Datei im EVIDENT-Verzeichnis löschen. Greifen Sie am besten über die **EVIDENT-Verknüpfung** auf dem Desktop mit **Rechtsklick**->**Dateipfad öffnen** auf die **EVIDENT-Freigabe** auf dem Server zu. In der EVIDENT-Freigabe gehen Sie bitte in das Verzeichnis **PROGDATA** und dort ins Verzeichnis **KM**. Wie Sie in folgendem Screenshot sehen, befindet sich darin die **EVIDENT.PEM**, diese ist zu löschen.

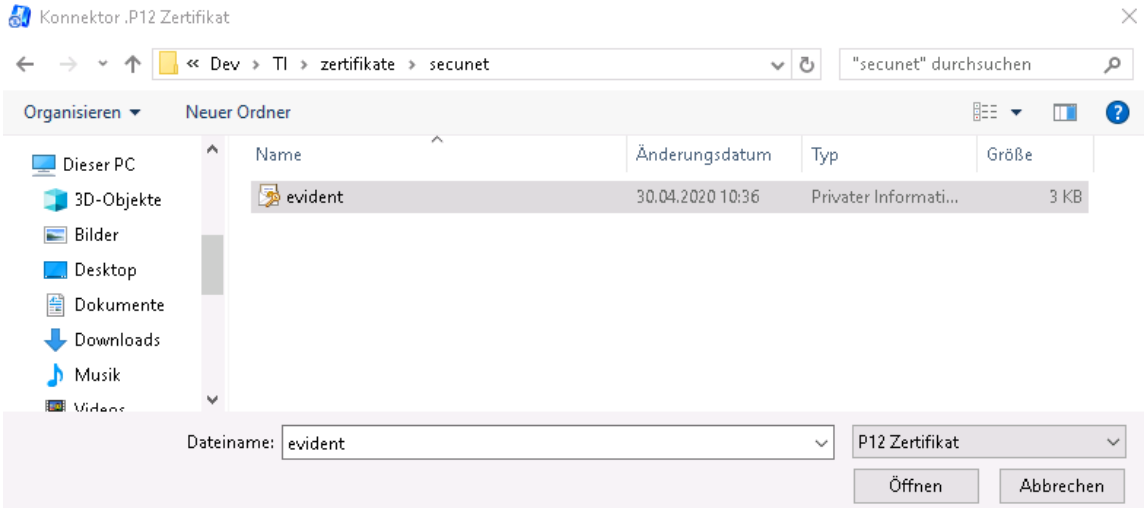


Als nächstes müssen Sie das neu generierte Clientzertifikat in den Konnektor Manager einspielen, um das schon vorhandene, aber abgelaufene Clientzertifikat, zu ersetzen.

Öffnen Sie dazu bitte zuerst den Konnektor Manager, dann auf **Details öffnen** und wechseln Sie dort auf die Registerseite **Zertifikate importieren**.

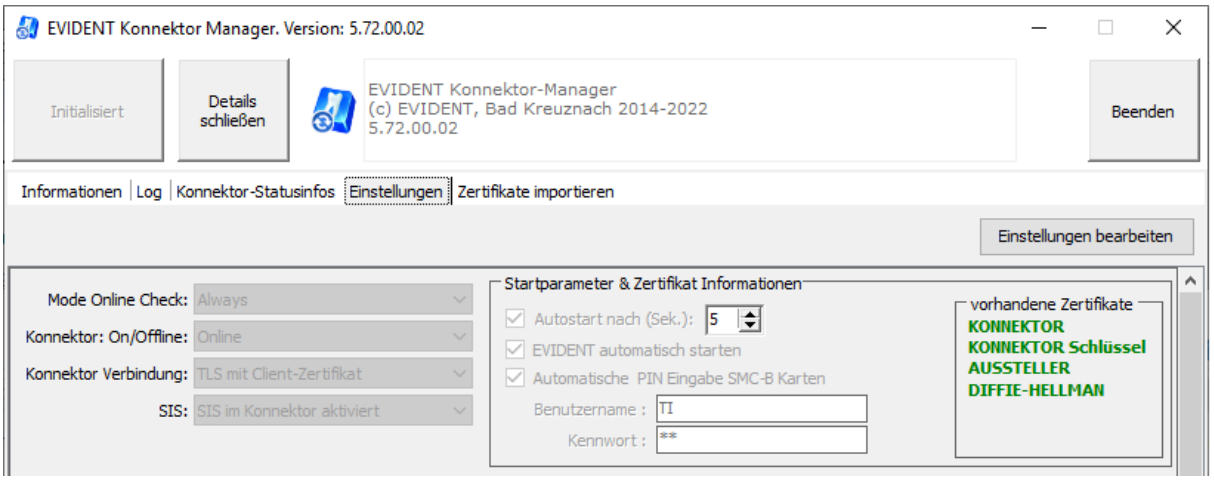


Als nächstes wird das Clientzertifikat (**.p12** Datei) über die Schaltfläche **Klient Zertifikat importieren** importiert.



Nach Öffnen der **.p12** Datei erscheint die Passwortabfrage, hier ist das automatisch generierte Passwort aus der passwort.txt einzugeben.

Per Bestätigung mit OK wird das Zertifikat importiert. Als Ergebnis sollten im Register **Einstellungen**, wie nachfolgend abgebildet, sämtliche Zertifikate grün sein.



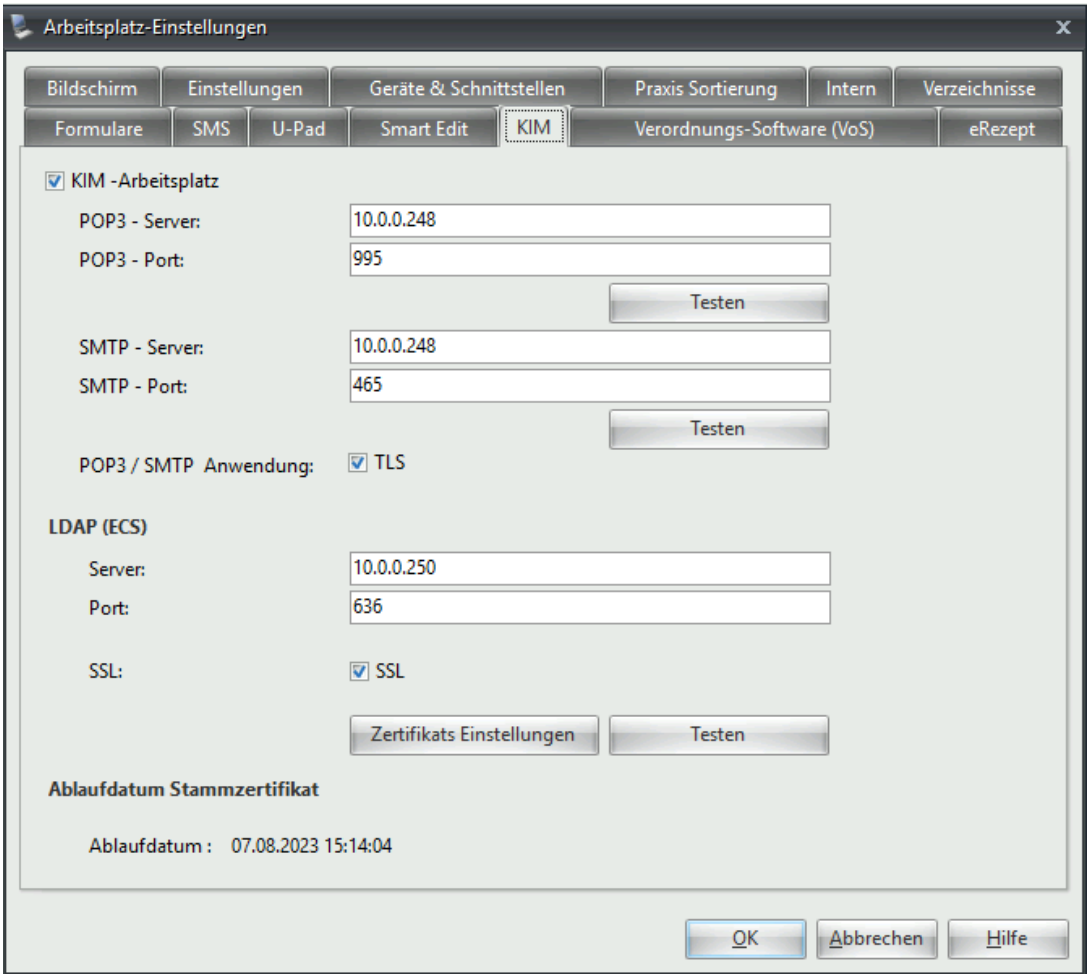
Achten Sie bitte darauf, dass nach dem erneuten Einspielen des Clientzertifikats, die Einstellungen für **Konnektor Verbindung** und **SIS** auf der linken Seite leer sind. Dort müssen Sie dann wieder, wie im Screenshot zu sehen, **TLS mit Client-Zertifikat** auswählen. Was Sie bei **SIS** auswählen, hängt davon ab, ob SIS in der KoCoBox aktiviert oder eben deaktiviert ist.

Nachdem Sie das Clientzertifikat in den Konnektor Manager importiert haben, ist der Konnektor Manager zu beenden und neu zu starten, damit die Änderungen wirksam werden.

Der Konnektor Manager sollte sich dann wieder an der KoCoBox anmelden können. Anschließend kann die Praxis wieder Chipkarten einlesen, alle weiteren Schritte betreffen die KIM-Anbindung.

3. LDAP und WCS/ECS

Durch den Ablauf des Clientzertifikats ist das Empfangen und versenden von **KIM-Mails ebenfalls nicht mehr möglich**. In diesem Schritt erfahren Sie, wie Sie den Zugriff auf das **LDAP** wieder ermöglichen können. Starten Sie dazu bitte **EVIDENT**, die Einstellungen für LDAP finden Sie im Menü **Praxis**->**Arbeitsplatz** auf der Registerseite **KIM**.



Der Bereich **LDAP (WCS** oder **ECS)** (Lightweight Directory Access Protocol, Windows oder EVIDENT Zertifikat Store) beschreibt die Verbindung zu dem zentralen Adressbuch, in dem alle Teilnehmer an diesem Kommunikationsdienst per spezieller KIM-E-Mail-Adresse gelistet sind.

Bitte prüfen Sie mit der Testen-Schaltfläche, dass ein Verbindungsaufbau tatsächlich nicht funktioniert. Wenn ECS verwendet wird, ist es durchaus möglich, dass der Zugriff auf LDAP durch die vorherigen Schritte bereits wieder möglich ist. Bei positivem Testergebnis ist mit Schritt 4 fortzufahren.

a) Automatische Aktivierung EVIDENT Zertifikatsverwaltung

Die in diesem Abschnitt a) beschriebene Vorgehensweise bildet den Standard. D. h., wenn diese funktioniert, dann übernehmen Sie diese Einstellung bitte und die unter b) und c) beschriebenen Optionen entfallen. Nach Anwahl der **Zertifikats-Einstellungen** öffnet sich ein Dialogfenster, in welchem sofort automatisch geprüft wird, ob der EVIDENT Cert Store (ECS) verwendet werden kann.
Im Erfolgsfall erkennen Sie das positive Ergebnis an den beiden grünen Haken vor den Anzeigen **PEM Zertifikate vorhanden** und **LDAP Verbindung herstellen**.

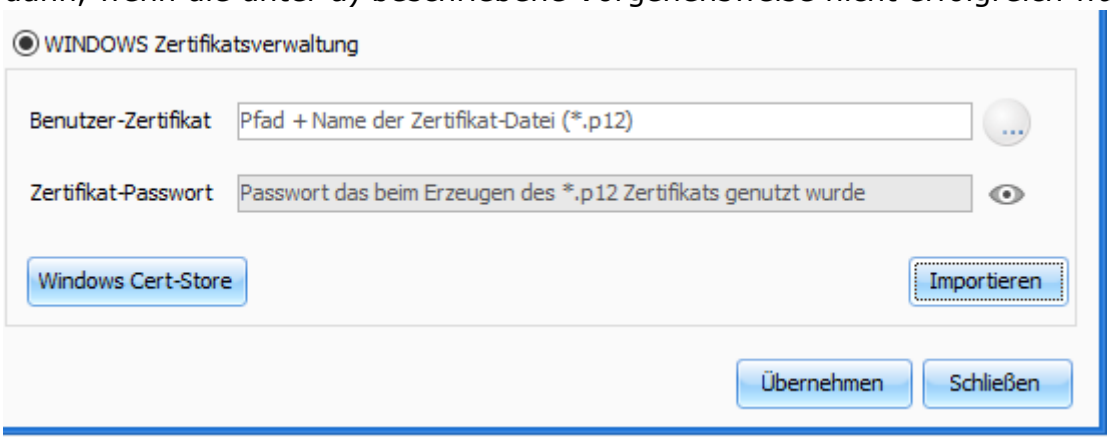
Das Textfeld unterhalb der angehakten Optionen beinhaltet das Live-Protokoll der Überprüfung. An dessen Ende steht die Information, für welche Variante sich die Überprüfung entschieden hat, in unserem Fall: Verbindung per SSL möglich. Um diese Einstellung zu **sichern**, klicken Sie bitte auf die Schaltfläche **Übernehmen**.

Konnte die **EVIDENT Zertifikatsverwaltung erfolgreich** aktiviert werden, dann entfallen, wie bereits erwähnt, die Punkte b) und c). Sie können mit **Schritt 4** fortfahren.

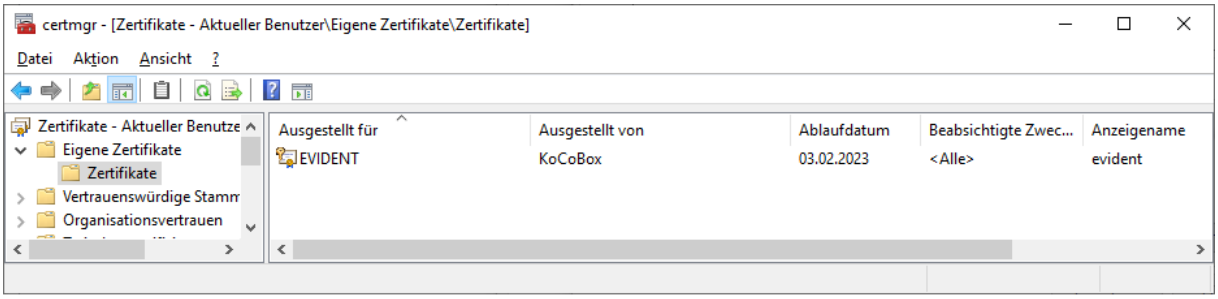
Hinweis: Wenn die Aktivierung der EVIDENT Zertifikatsverwaltung an einem Arbeitsplatz erfolgreich war, ist dies grundsätzlich aus technischer Sicht auch für weitere Arbeitsplätze zu erwarten. Spezielle Firewalleinstellungen an bestimmten Stationen könnten dies allerdings verhindern. Sollte eine der beiden Prüfungen nicht erfolgreich abgeschlossen werden, wird statt des grünen Hakens ein rotes Kreuz angezeigt. Das bedeutet die EVIDENT Zertifikatsverwaltung ist nicht möglich. In diesem Fall kann im unteren Teil des Fensters mit der Windows Zertifikatsverwaltung fortgefahren werden.

b) Verwendung der Windows Zertifikatsverwaltung

Wichtig: Nachfolgende Vorgehensweise ist an **jedem Arbeitsplatz** erforderlich, an dem ein LDAP-Abgleich durchführbar sein soll, allerdings nur dann, wenn die unter a) beschriebene Vorgehensweise nicht erfolgreich war.

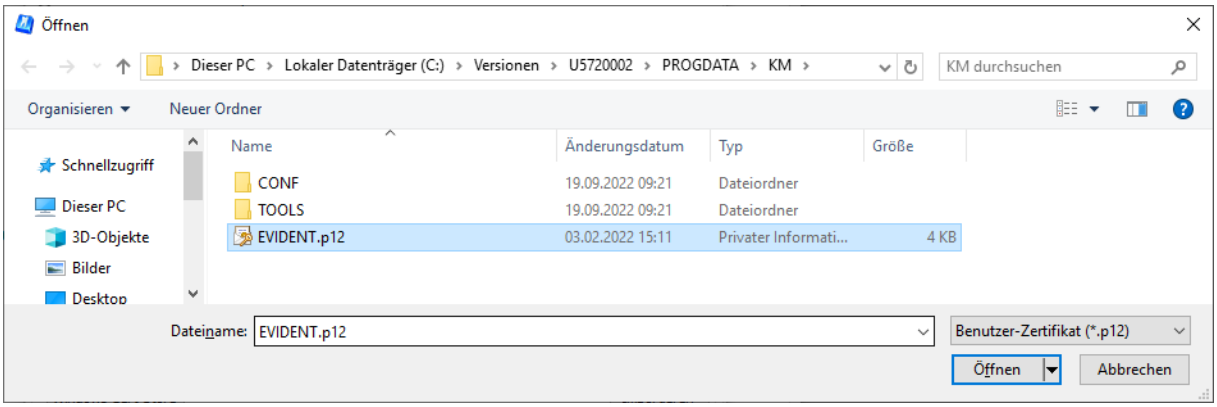


Öffnen Sie bitte über den Button **Windows Cert-Store** die **Windows Zertifikatsverwaltung**. Klicken Sie dort auf der rechten Seite auf **Eigene Zertifikate** und dann auf **Zertifikate**. Anschließend sollten Sie das schon vorhandene, aber abgelaufene Clientzertifikat sehen können.

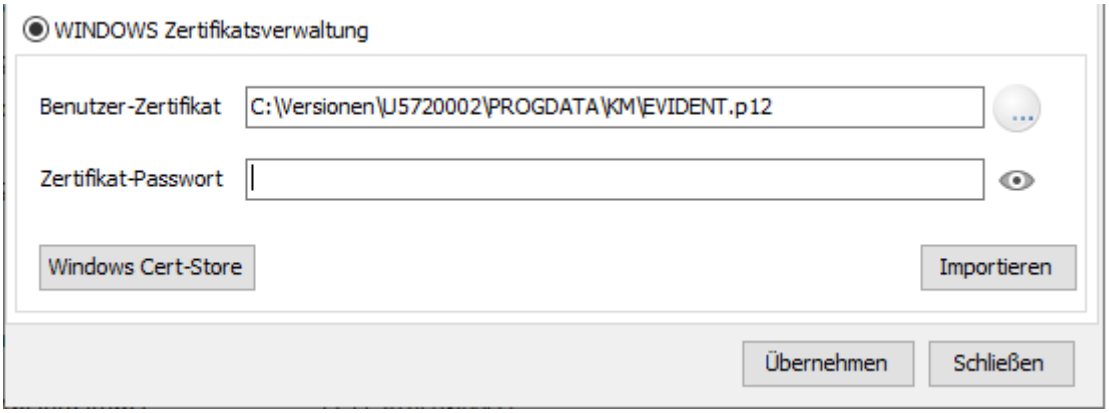


Machen Sie darauf bitte einen Rechtsklick und klicken Sie dann auf **Löschen**. Danach können Sie die **Windows Zertifikatsverwaltung** wieder schließen und im EVIDENT weitermachen.

Per Klick auf das Symbol rechts neben dem Feld **Benutzer-Zertifikat** lässt sich das **Clientzertifikat** auswählen.
Der Dateiauswahldialog gibt das Verzeichnis der EVIDENT-Installation sowie PROGDATA\KM\ vor. Hier liegt das **Clientzertifikat**, das zuvor erfolgreich in den **Konnektor Manager** importiert wurde. Der Dateiendungsfilter des Dateiauswahldialogs ist fix auf ***.p12** eingestellt.



Nach Auswahl des gewünschten Zertifikats und **Bestätigen** der **Öffnen** Schaltfläche wird der komplette Pfad der gewählten Zertifikatsdatei in den Import-Dialog übernommen.

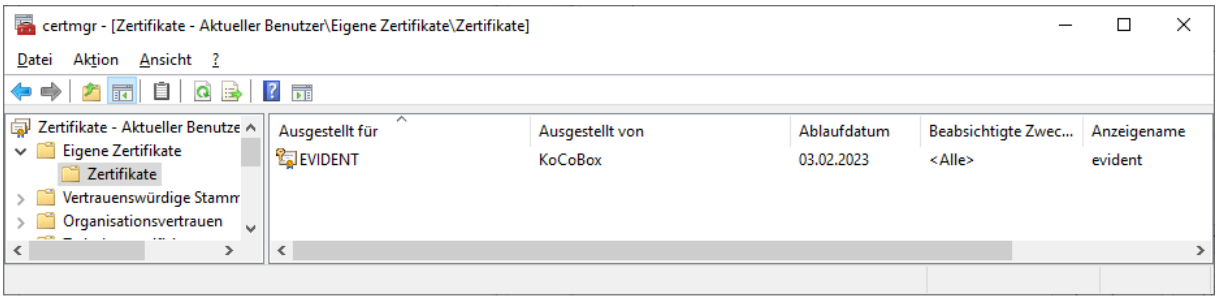


Zum Importieren des gewählten Clientzertifikats ist das **Passwort nötig**, das bei Export des Zertifikats aus dem jeweiligen Konnektor generiert wurde. Um diese Einstellung zu **sichern**, klicken Sie bitte auf die Schaltfläche **Übernehmen**.

c) Automatikimport

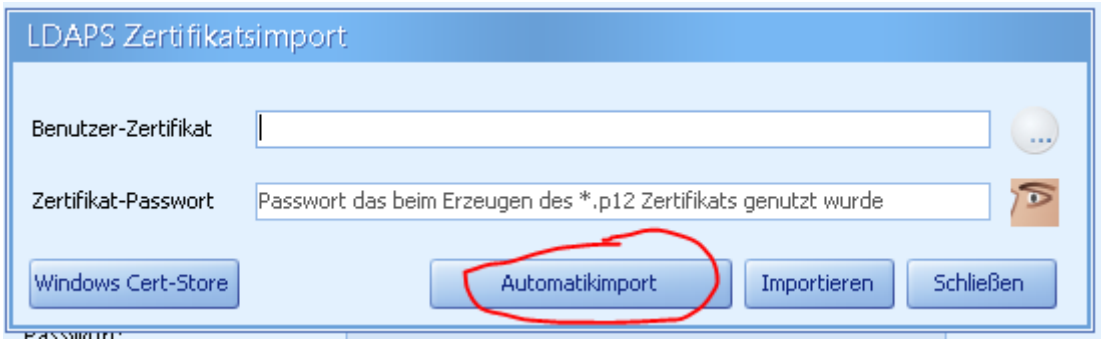
Beim Import der Zertifikate erzeugt der Konnektor Manager Importscripte für den LDAP-Zertifikatsimport. Über diese **Scripte** kann das Clientzertifikat wie zuvor beschrieben importiert werden, ohne dass die Zertifikatsdatei ausgewählt oder das Passwort eingegeben werden muss.
Findet das Importprogramm also beim Aufruf das erwähnte Importscript, wird im Importprogramm eine **Schaltfläche Automatikimport** verfügbar.

Öffnen Sie aber bitte zuerst über den Button **Windows Cert-Store** die **Windows Zertifikatsverwaltung**. Klicken Sie dort auf der rechten Seite auf **Eigene Zertifikate** und dann auf **Zertifikate**. Anschließend sollten Sie das schon vorhandene, aber abgelaufene Clientzertifikat sehen können.



Machen Sie darauf bitte einen Rechtsklick und klicken Sie dann auf **Löschen**. Danach können Sie die **Windows Zertifikatsverwaltung** wieder schließen und im EVIDENT weitermachen.

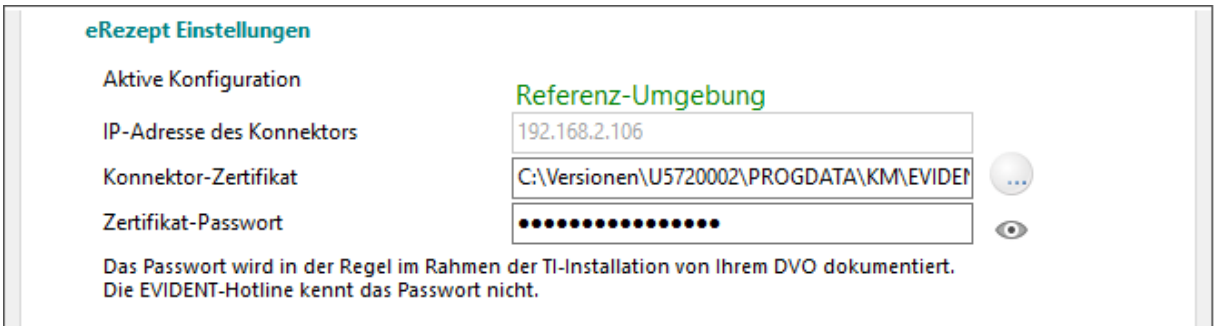
Klicken Sie anschließend auf den Button **Automatikimport**.



Das Bestätigen der Schaltfläche liest die benötigten Informationen aus dem Importscript aus und installiert das **Clientzertifikat** in die **Windows Zertifikatsverwaltung**. Auch hier gilt: Um diese Einstellung zu **sichern**, klicken Sie bitte auf die Schaltfläche **Übernehmen**.

4. Clientzertifikat für das eRezept hinterlegen

Die letzte Stelle, an der EVIDENT das Clientzertifikat benötigt, ist das **eRezept**. Öffnen Sie bitte das entsprechende Menü über **Praxis->Arbeitsplatz->eRezept**. In der unteren Hälfte sehen Sie unter anderem **Konnektor-Zertifikat** (damit ist das Clientzertifikat gemeint) und **Zertifikat-Passwort**. Es reicht hier, wenn Sie einfach nur rechts neben dem Feld für **Konnektor-Zertifikat** auf den runden Button mit den drei Punkten klicken. EVIDENT liest dann eine **Script-Datei** aus, die beim einspielen des Clientzertifikats in den Konnektor Manager, generiert wurde und trägt automatisch das richtige Passwort in das Feld darunter ein.



5. Einspielen des neuen Clientzertifikats in den KIM Client

Damit das **Versenden** und **Empfangen** von **KIM-Mails** ebenfalls wieder funktioniert, müssen Sie das neu generierte **Clientzertifikat** als letzten Schritt auch noch in den Ihren **KIM Client** einspielen. Hierbei können wir leider keine weitere Hilfe zur Verfügung stellen, da wir für die Einrichtung keines der auf dem Markt angebotenen KIM Clients befugt sind. Das Einrichten und der Support des KIM Clients erfolgt immer durch den DVO.
Es gibt in jedem KIM Client auch ein Feld um das Clientzertifikat zu importieren, immerhin muss sich der KIM Client damit ebenfalls am Konnektor anmelden. Im **KIMplus Clientmodul** finden Sie das zugehörige Feld im Menü **TLS**: