



Beschreibung zur Weitergabe an den DVO, Stand 08.09.2022

Gültig seit EVIDENT Version 5.68

Sehr geehrte Damen und Herren,

in Kürze werden Sie KIM in unserer Praxis installieren.

Damit KIM mit unserer Praxissoftware EVIDENT einwandfrei funktioniert, ist es wichtig, dass die praxisindividuellen und technischen Einstellungen zu KIM von Ihnen in unsere EVIDENT-Software eingetragen werden. Um Ihnen die Eintragungen möglichst einfach zu machen, hat EVIDENT diese Kurzbeschreibung für Sie erstellt.

! Bitte laden Sie unmittelbar vor der Installation den neuen Versionsstand der Anleitung unter www.evident.de/ti.html herunter !

Schritt 1: Installieren Sie bitte das eHealth-Update für unseren Konnektor. Danach nehmen Sie an dem Arbeitsplatz, an dem KIM-Nachrichten versendet und empfangen werden sollen die technische Einrichtung im Menü **Praxis, Arbeitsplatz**, Registerseite **KIM** vor.

Das folgende Beispiel zeigt eine Installation mit einem secunet-KIMplus-Client.

The screenshot shows the 'Arbeitsplatz-Einstellungen' dialog box with the 'KIM' tab selected. The settings are as follows:

Category	Field	Value
KIM - Arbeitsplatz	<input checked="" type="checkbox"/> KIM - Arbeitsplatz	
	POP3 - Server:	10.0.0.248
	POP3 - Port:	995
	Testen	
SMTP	SMTP - Server:	10.0.0.248
	SMTP - Port:	465
	Testen	
	POP3 / SMTP Anwendung:	<input checked="" type="checkbox"/> TLS
LDAP (ECS)	Server:	10.0.0.250
	Port:	636
	SSL:	<input checked="" type="checkbox"/> SSL
	Zertifikats Einstellungen	
Testen		
Ablaufdatum Stammzertifikat		
Ablaufdatum :		07.08.2023 15:14:04

Buttons at the bottom: OK, Abbrechen, Hilfe

Bitte beachten Sie:
Gemäß Vorgabe der gematik ist die **Einstellung TLS/SSL mit Zertifikat verpflichtend!**

Diese Einstellung hat im Konnektor selbst zu erfolgen.

Bei Bedarf erfahren Sie im **Anhang** wie Zertifikate erstellt werden.

Wie die Abbildung zeigt, können an dieser Stelle die entsprechenden IP-Adressen (Pop3-Server/ SMTP- Server) und Ports erfasst werden.

Der Bereich **LDAP** (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 den Test-Schaltflächen, dass ein Verbindungsaufbau tatsächlich funktioniert. Bei negativem Testergebnis ist mit Schritt 3 fortzufahren.**

Schritt 2: LDAP Verbindung per SSL/TLS mit Zertifikat-Einstellung


Voraussetzungen:

- Ein funktionstüchtiger Konnektor-Manager (KM), in den alle Zertifikate korrekt importiert wurden. Das bedeutet: alle Zertifikate sind grün angezeigt im Konnektor-Manager.
- EVIDENT Programmversion ab 5.68.
- Vom KM erzeugte Importskripte unter PROGDATA\KM\TOOLS (nur für Scriptimport)

Sie starten in voriger Abbildung per Klick auf die **Schaltfläche Zertifikats Einstellungen**. Diese ist nur sicht- und benutzbar, wenn zuvor die **Checkbox SSL angehakt** wurde.

Automatische Aktivierung EVIDENT Zertifikatsverwaltung

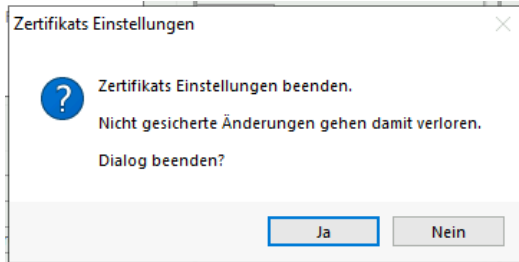
Nach Anwahl der Zertifikats-Einstellungen öffnet sich ein Dialogfenster, in welchem sofort automatisch geprüft wird, ob der EVIDENT Cert Store (ECS) verwendet werden kann.

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, im o. a. Fall: Verbindung per SSL möglich. Um diese Einstellung zu **sichern**, muss die Schaltfläche **Übernehmen** gedrückt werden. Klickt man stattdessen auf die Schaltfläche

Schließen, erfolgt diese Abfrage:



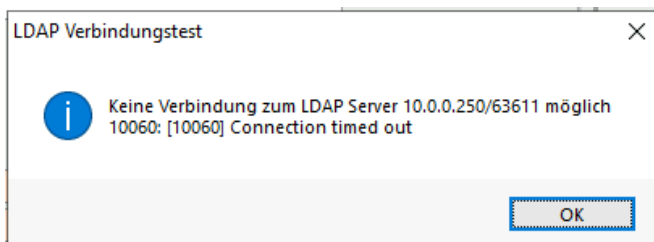
Hinweis: Wenn die Aktivierung der EVIDENT Zertifikatsverwaltung an einem Arbeitsplatz erfolgreich war, ist dies grundsätzlich aus technischer Sicht auch für weitere Arbeitsplätze zu erwarten. Spezielle Firewall-Einstellungen an bestimmten Stationen könnten dies allerdings verhindern.

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.

Schritt 3: Negatives Testergebnis



Konnte bereits beim Anklicken des Testen Buttons keine Verbindung hergestellt werden, erhalten Sie eine Fehlermeldung.



Nur dann erscheint hinter der Zeile mit der Porteinstellung ein Zahnrad.

LDAP (ECS)

Server: 10.0.0.250

Port: 63611

SSL: SSL

Zertifikats Einstellungen Testen



Nach Anklicken des Zahnrad-Symbols erscheint folgendes Fenster:

Zertifikats Einstellungen

LDAP Einstellungen

Nur nach Rücksprache Änderungen vornehmen!

StartMode: Automatic

InternalAPI:

SupportedGroup: z.B. ecclhe_secp256r1

Base: dc=data,dc=vzd

Authentifizierungs Methode: 0

LDAP Version: 3

Testen

Zurücksetzen

Übernehmen Schließen

Bitte beachten: Halten Sie sich an die im Fenster angezeigte Meldung, d. h. nehmen Sie **Änderungen** auf jeden Fall **nur nach Rücksprache** mit EVIDENT vor.

Schritt 4: Zur Anbindung der Ärzte an KIM die Daten der Personalakte vervollständigen und prüfen

Die Ärzte, die von Ihnen eine KIM-Mailadresse erhalten, haben wir für Sie in der Personalakte bereits angelegt. Das notwendige Passwort zum Ergänzen der Arztdaten liegt Ihnen vor oder Sie erhalten es von uns bei der Installation.

Übers Menü **Orga-Manager, Personalakte** gelangen Sie in die Verwaltung aller Praxis-Mitarbeiter, auch der Ärzte. Bitte tragen Sie dort im Register **Allgemein** die KIM-Zugangswerte in der EVIDENT-Personalakte folgender Ärzte ein.

Arzt 1: _____ Arzt 2: _____

Arzt 3: _____ Arzt 4: _____

Personalakte - Testpraxis - Benutzer: Mustermann, Max (MAX)

Mitarbeiter Archivierte anzeigen

Mustermann, Max (MAX)

Stammdaten Allgemein Soll-Arbeitszeiten Abwesenheit Medizin-Check Dokumente

zusätzliche Daten

Kürzel* MAX

Personalnummer

Dienstliche E-Mail

KIM E-Mail 1 evident@arv.kim.telematik-test

KIM E-Mail 2

Dienstlich Mobil

Zuordnung

Stammpraxis Testpraxis

Personengruppe* Zahnärzte

Praxis-Zuordnung

Arbeitsplätze Synchronisieren

Tätigkeiten Synchronisieren



Behandlerverwaltung

Technikverwaltung

Arztverwaltung

TIS-Behandlerverwaltung

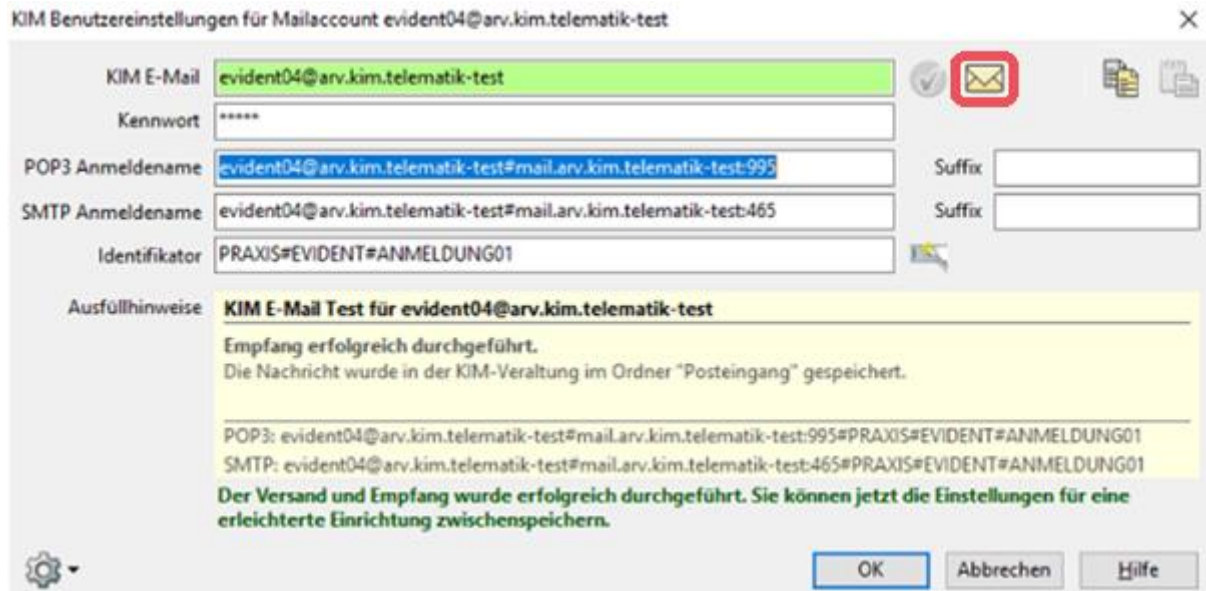
Benutzerprofil

Über das Schloss  gelangen Sie in die Benutzereinstellungen. Wurde die Mailadresse dort über  im LDAP-Verzeichnis gefunden, dann können Sie diese mit KIM verbinden und geben hier die KIM-Zugangsdaten ein.

Schritt 5: Einrichten der KIM-Zugangsdaten und das Versenden einer Testmail


Bitte tragen Sie die KIM-Zugangsdaten in untenstehendes Fenster ein.

Die Testmail kann einfach per Klick auf das aktivierte Briefumschlag-Symbol versendet werden und führt im Erfolgsfall zu folgendem Ergebnis.



Eingesehen werden kann die Testmail im **Posteingang** der **KIM-Verwaltung**, die sich im Menü Kommunikation befindet. Bitte lassen die Mail dort als Nachweis des erfolgreichen Tests liegen.

Unser Tipp für Sie:

An der zuvor beschriebenen Programmstelle, also innerhalb der Benutzereinstellungen, können Sie die getesteten Einstellungen über das Symbol  in die Zwischenablage kopieren. Dies ist hilfreich, wenn Sie weitere KIM E-Mailadressen anlegen, da sich dort dann die Einstellungen einkopieren lassen und nicht mehr händisch erfasst werden müssen. Lediglich der Benutzername ist dann jeweils anzupassen.

Herzlichen Dank!

Sollte es Ihnen **nicht** möglich sein, die o.g. Daten in EVIDENT zu erfassen, dann **senden** Sie uns diese bitte anhand folgendem Erfassungsbogen zu:

Technische KIM-Zugangswerte:

KIM-Client der Firma: _____

POP3 Server: _____

POP3 Port: _____

SMTP-Server: _____

SMTP-Port: _____

SSL: Ja Nein

SSL mit Zertifikat: Ja Nein

Technische LDAP-Zugangswerte:

Server: _____

Port: _____

SSL: Ja Nein

SSL mit Zertifikat: Ja Nein

Bitte senden Sie uns das LDAP-Benutzerpasswort vertraulich, verschlossen und schriftlich.

KIM-Mailadressen und Zugangsdaten Arzt

KIM-Fachdienstanbieter: VisionmaxX anderer: _____

KIM-Mailadresse Arzt1: _____

KIM-Mailadresse Arzt2: _____

KIM-Mailadresse Arzt3: _____

KIM-Mailadresse Arzt4: _____

Bitte senden Sie uns die KIM-Passwörter vertraulich, verschlossen und schriftlich. Besten Dank.



ANHANG

Erstellen, Exportieren und Importieren von Zertifikaten

Um Angriffe auf die Sicherheit zwischen zwei kommunizierenden Systemen zu verhindern, gibt es die sogenannte TLS/SSL gesicherte Verbindung. **TLS** steht dabei für **Transport Layer Security**, also eine gesicherte Transportschicht für Datenpakete.

Damit im konkreten Fall die sichere Kommunikation zwischen Konnektor und Konnektor Manager (KM) gewährleistet werden kann, kommen in dieser Transportschicht sogenannte Zertifikate zum Einsatz. Dabei kann der KM das vom Konnektor erstellte **Clientzertifikat** (im Falle des **RISE** Konnektors) verwenden, oder ein eigenes Zertifikat (im Falle des **secunet** Konnektors ist sowohl das **Server-** als auch das **Clientzertifikat** möglich) erstellen. Dieses Zertifikat müsste im Konnektor pro Clientsystem importiert werden.

Nachfolgend wird nun die Vorgehensweise beschrieben, wie im Falle der Konnektoren RISE und secunet das jeweilige Zertifikat erzeugt wird.

Wichtiger Hinweis: Beachten Sie bitte, dass in Verbindung mit EVIDENT derzeit bei allen Konnektoren **ausschließlich RSA-Clientzertifikate** erstellt und verwendet werden können.

1. Zertifikat für RISE erstellen

Im Managementservice (Konfigurationsmenü) des RISE Konnektors befindet sich unter der Rubrik **Dienste**, der Menüpunkt **Clientsysteme**. Dieser Menüpunkt präsentiert sich wie folgt:

[Anbindung der Clientsysteme](#)

The screenshot shows a configuration window with three tabs: 'Konfiguration', 'Passwörter', and 'Zertifikate'. The 'Konfiguration' tab is active. The main heading is 'Kommunikation mittels TLS absichern'. There are two checkboxes: 'Verpflichtend TLS verwenden' (checked) and 'Als Ausnahme den Dienstverzeichnisdienst trotzdem ohne TLS zugänglich machen' (unchecked). Below this is the section 'Authentifizierung von Clientsystemen' with a checked checkbox 'Verpflichtende Authentifizierung von Clientsystemen'. A dropdown menu is set to 'Zertifikats-basierte Authentifizierung'. At the bottom is an orange 'Speichern' button.

Im Register **Konfiguration** sind folgende Einstellungen vorzunehmen:

- **Verpflichtend TLS verwenden** per Haken aktivieren
- Als Ausnahme den Dienstverzeichnisdienst ohne TLS zugänglich machen muss deaktiviert werden
- **Verpflichtende Authentifizierung von Clientsystemen** – per Haken aktivieren
- In der Auswahlbox die Option **Zertifikats-basierte Authentifizierung** wählen

Im Register **Zertifikate** wählen Sie **Neues Zertifikat generieren**.

Konfiguration Passwörter **Zertifikate**

Zertifikats-basierte Authentisierung von Clientsystemen

Clientsystem	Aktionen
Keine Daten gefunden	

+ Neues Zertifikat generieren... + Zertifikat importieren...

Damit gelangen Sie zur nachfolgenden Abfrage:

Neues Zertifikat generieren ✕

Bitte geben Sie den Namen des Clientsystems an, für welches das Zertifikat erzeugt werden soll.

Clientsystem *

* Pflichtfeld

Abbrechen 1/3 Weiter

Als **Clientsystem** selektieren Sie **EVIDENT** und gehen auf **Weiter**.

Das neue Zertifikat wird erzeugt. Das Ergebnis erscheint etwa wie folgt:

Neues Zertifikat generieren ✕

Zertifikat erzeugt.

[Laden Sie das Zertifikat hier im PKCS12 Format herunter.](#)

Zertifikatspasswort **XMO?}YZCuwVG<lyP**

Notieren Sie sich das Zertifikatspasswort sorgfältig. Nach dem Beenden dieses Schritts wird Ihnen das Passwort nicht mehr angezeigt.

Abbrechen 3/3 Fertigstellen

Wichtig: Nur an dieser Stelle kann das Zertifikat heruntergeladen werden.

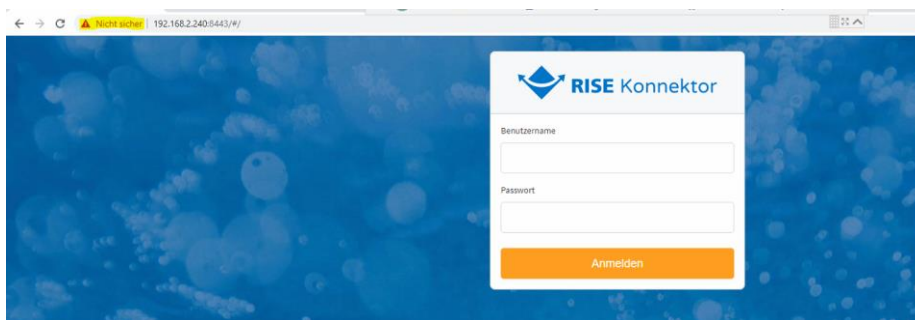
Wie in der Meldung am Bildschirm angezeigt, **notieren** Sie sich **unbedingt** das angezeigte **Zertifikatspasswort** bzw. kopieren Sie es zur korrekten Verfügbarkeit z. B. in Notepad **bevor** Sie auf **Fertigstellen** klicken.

Empfehlung: Das heruntergeladene Zertifikat und das Passwort sichern Sie am besten in einem separaten Ordner (Name: RISE Zertifikat).

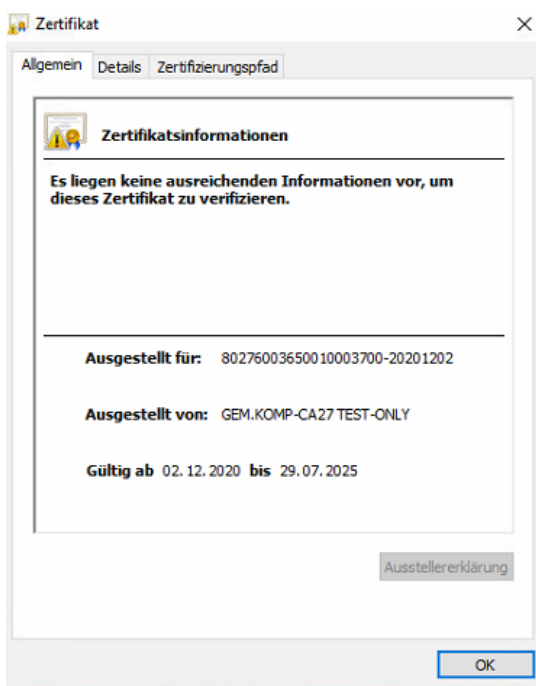
2. Konnektor-Zertifikat für RISE exportieren

Das Konnektor Zertifikat **exportieren** Sie wie folgt:

Klicken Sie mit einem Rechtsklick auf den gelb markierten Bereich und wählen im Kontextmenü den Punkt **Zertifikat**



Sie gelangen in das folgende Fenster:



Verzweigen Sie nun auf die Registerkarte **Details** und dann unten rechts auf **In Datei kopieren**.

Bestätigen Sie das folgende Fenster mit **Weiter**.

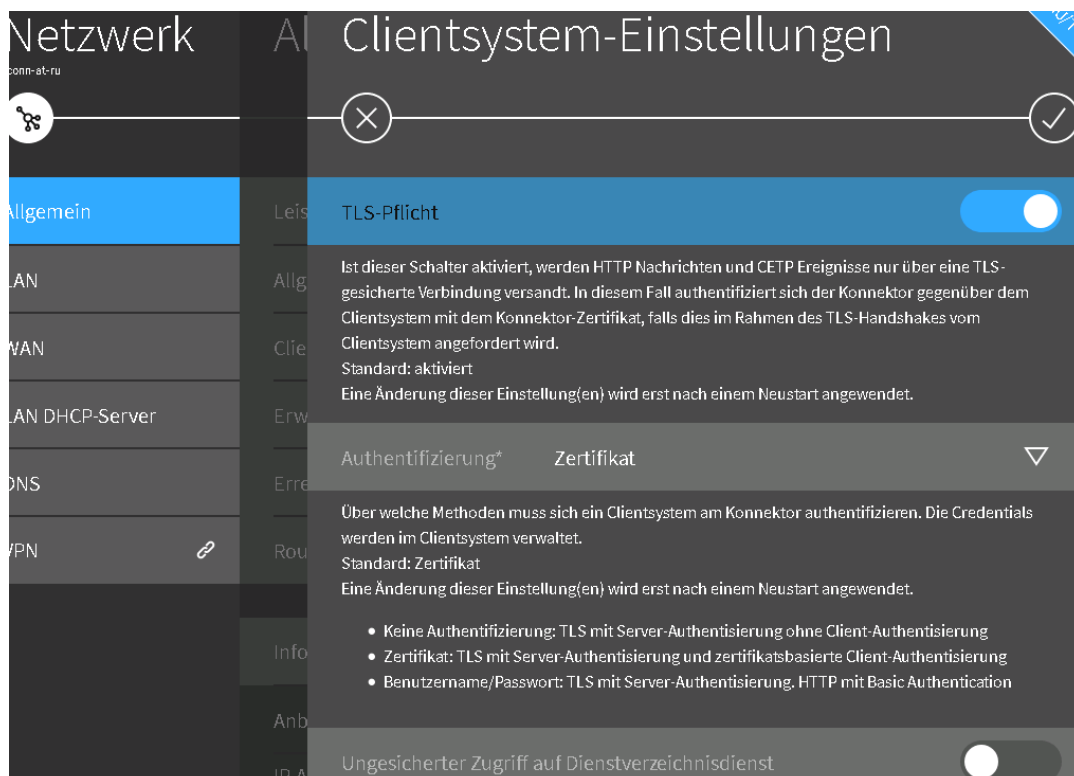
Lassen Sie in dem darauffolgenden Fenster die Auswahl bitte bei **DER-codiert-binär X.509 (.CER)** stehen und bestätigen mit **Weiter**.

Wählen Sie nun einen Dateinamen sowie den gewünschten Speicherort aus und bestätigen mit **Weiter** und dann mit **Fertigstellen**.

3. Zertifikate für Secunet erstellen

Im Management (Konfigurationsmenü) des secunet Konnektors befindet sich unter **Praxis**, der Menüpunkt **Clientsysteme**.

Über den dortigen Menüpunkt **Clientsystem Einstellungen** gelangt man zu den allgemeinen **Netzwerkeinstellungen**.

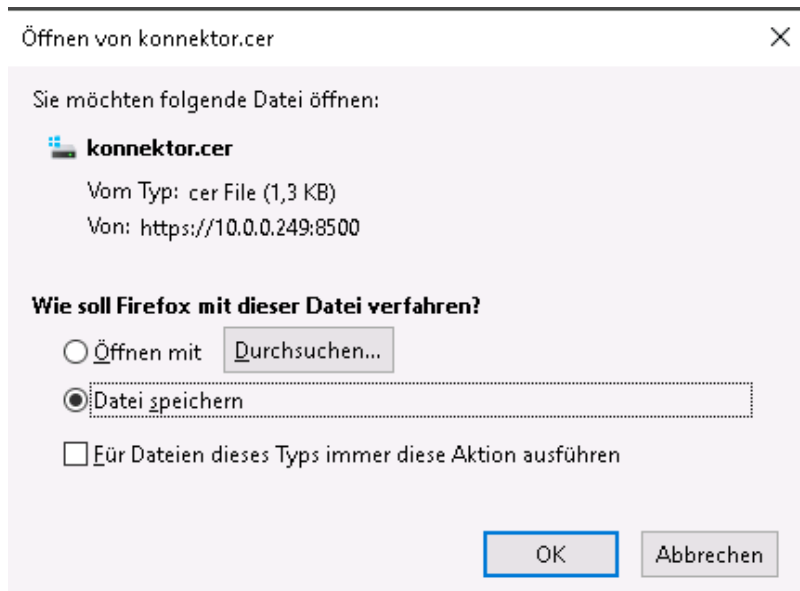


Wie in der Abbildung geschehen, ist die Option **TLS-Pflicht** zu **aktivieren**. In der Auswahlbox **Authentifizierung** wählen Sie **Zertifikat**. Die Option **Ungesicherter Zugriff auf Dienstverzeichnisdienst** ist zu **deaktivieren**.

Um ein Zertifikat zu generieren, wechseln Sie zurück zum Menüpunkt **Praxis, Client-Systeme**. Ein Server Zertifikat erzeugen Sie per Klick auf:

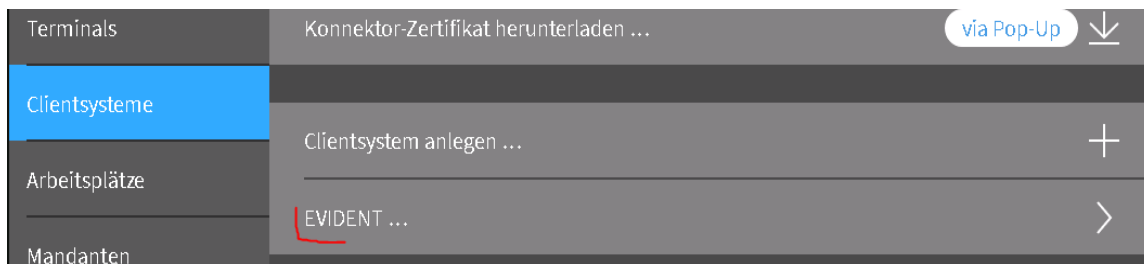


Es öffnet sich folgendes Fenster:

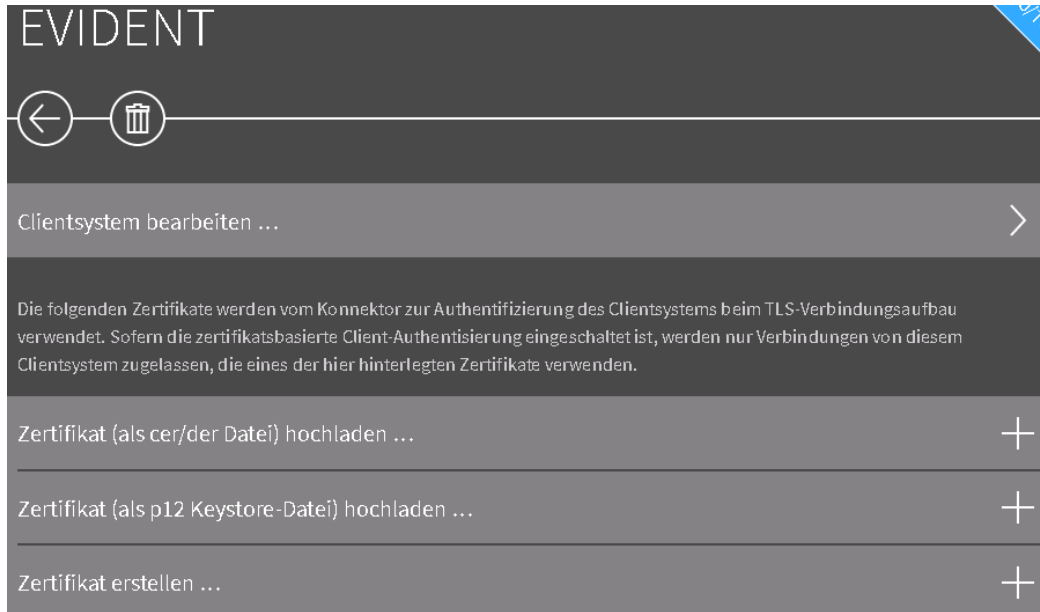


Hier wird das **Server Zertifikat** mit der Dateibezeichnung **konnektor.cer** über **Datei speichern** heruntergeladen und damit gesichert.

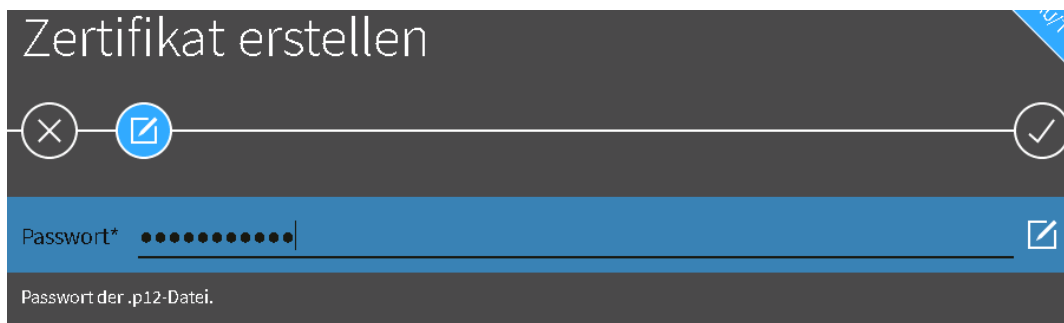
Möchten Sie das **Client Zertifikat** generieren, beginnen Sie ebenfalls im Menü **Praxis, Clientsysteme** und klicken dort auf **EVIDENT**.



Es erscheint das Fenster:



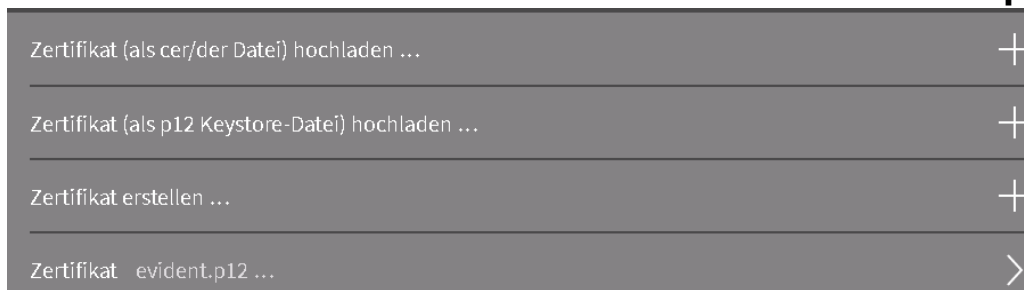
Hier wählen Sie die unterste Option, also **Zertifikat erstellen**. Damit gelangen Sie zu folgender Ansicht:



Unter Beachtung der Vorgaben geben Sie das gewünschte **Passwort** ein und **notieren** bzw. **sichern** Ihre Eingabe. Gespeichert wird die Eingabe per

Klick auf .

In der Übersicht erscheint nun die Zeile **Zertifikat evident.p12...**



Diese Zeile klicken Sie an und laden das Zertifikat per Klick auf die Schaltfläche **Zertifikat herunterladen ...** herunter.

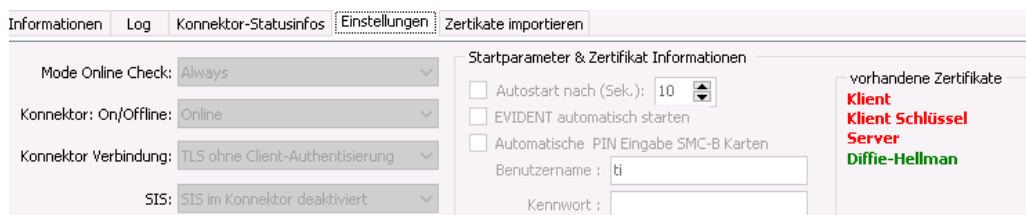
Empfehlung: Die beiden Zertifikate am besten in einem Ordner sichern nebst der Textdatei mit dem Passwort.

Hinweis: Der secunet Konnektor muss nach Änderung von *ohne TLS* auf *mit TLS* neu gestartet werden.

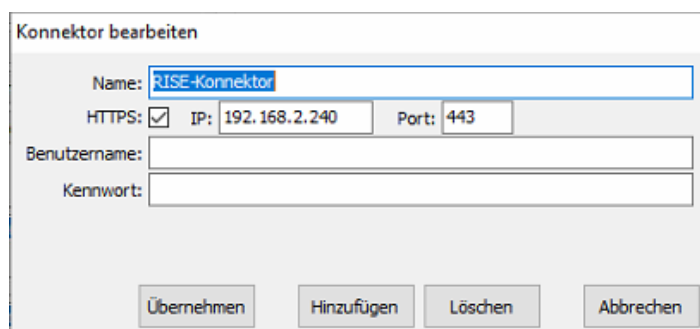
4. Zertifikate in den Konnektor Manager (KM) importieren

Nach der Beschreibung wie die Zertifikate erzeugt werden folgt noch deren Einbindung in den EVIDENT Konnektor Manager.

Der KM sichert alle Zertifikate im Verzeichnis **ProgData\KM**. Dort sollte sich die **Diffie-Hellman-Cryptodatei DHGRP12.PEM** befinden. Falls nicht, kann nicht fortgefahren werden. Erkennbar ist das Vorhandensein der Datei an der grünen Schrift rechts in den Einstellungen des KM im Bereich vorhandene Zertifikate:



Um das Verzeichnisdienstverzeichnis (VDV) per **HTTPS** statt http vom Konnektor zu beziehen, ist es erforderlich den Konnektor zu bearbeiten. Hier nochmal die Stelle im KM.

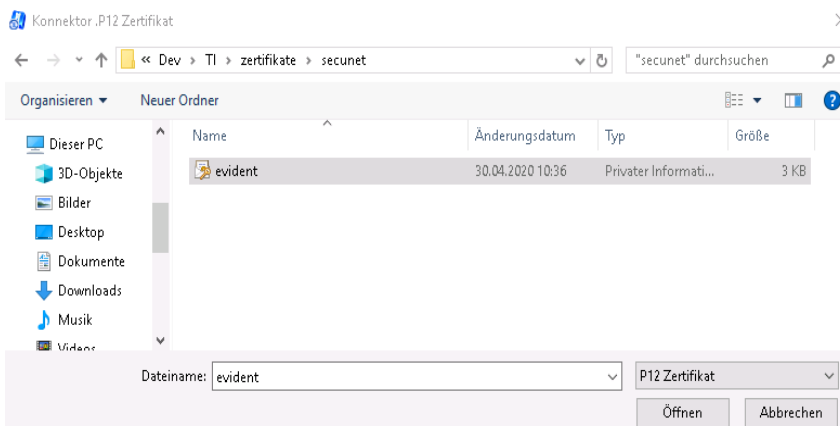


Zum Import der Zertifikate wechseln Sie auf die eigene **Registerseite Zertifikate importieren**.



4.1 Secunet Zertifikate importieren

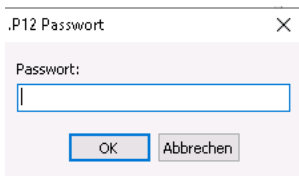
Per Klick auf die **Schaltfläche Server Zertifikat importieren** verzweigen Sie in die für Windows übliche Dateiauswahl.



Hier ist die **.CER** Datei zu selektieren und wiederum per Öffnen zu bestätigen.

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

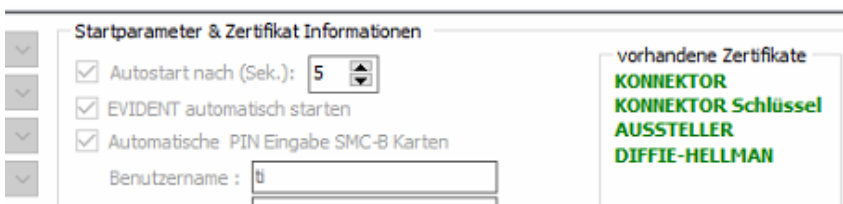
Nach Öffnen der P12 Datei erscheint die Passwortabfrage:



Es ist das gesicherte und gemerkte Passwort (siehe oben) einzugeben.

Per **Bestätigung** mit **OK** wird das Zertifikat importiert.

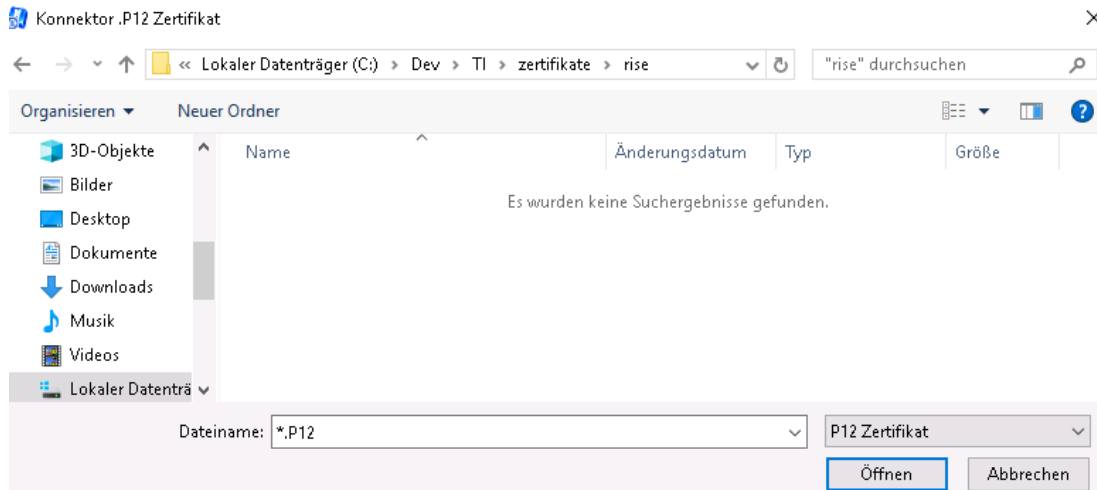
Als Ergebnis sollten im Register Einstellungen, wie nachfolgend abgebildet, sämtliche Zertifikate **grün** sein.



4.2 RISE Zertifikat importieren

Grundsätzlich ist der Ablauf identisch wie zuvor für secunet beschrieben. Daher hier nur noch die Unterschiede.

RISE erstellt **keine .P12 Datei**. Das bedeutet im Detailauswahlfenster erscheint zunächst kein Zertifikat.



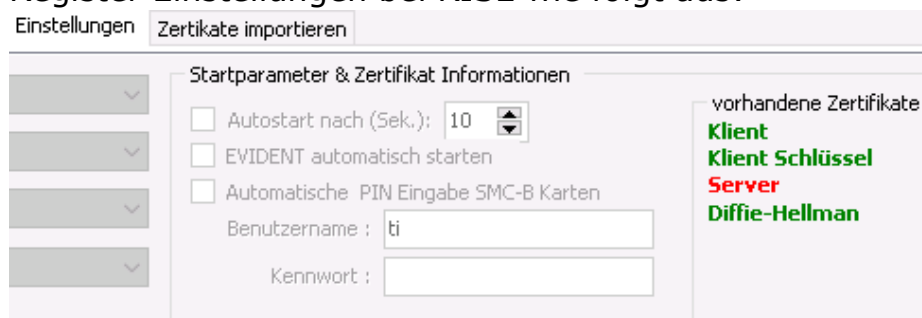
An der Stelle P12 Zertifikat rechts unten wechseln Sie daher bitte auf **Sämtliche Dateien**:



Es erscheint das Zertifikat sowie, sofern wie oben beschrieben das Passwort im gleichen Verzeichnis gespeichert wurde, zusätzlich die Passwortdatei.

Es ist das Zertifikat zu selektieren, zu öffnen und per Passwort zu bestätigen.

Die danach folgende Dateiauswahl ist abzubrechen, da RISE kein Serverzertifikat zum Herunterladen anbietet. Folglich sieht das Ergebnis im Register Einstellungen bei RISE wie folgt aus:



Abschließend zu diesem Thema die Anzeige dazu wie im Register Einstellungen die Verbindungsart zu definieren ist:

Mode Online Check:	Always	▼
Konnektor: On/Offline:	Online	▼
Konnektor Verbindung:	TLS mit Client-Zertifikat	▼
SIS:	SIS im Konnektor aktiviert	▼

Die Option TLS mit Client Authentisierung ist sowohl für RISE als auch für secunet **VERPFLICHTEND** zu verwenden.

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