



Beschreibung zur Weitergabe an den DVO, Stand 08.09.2022 Generieren und Exportieren von Zertifikaten für Praxen mit KoCoBox

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 !

Hinweis: In nachfolgender Beschreibung wird **ausschließlich** thematisiert, wie Sie in einer Praxis, die als Konnektor die **KoCoBox** betreibt, das erforderliche **Client-Zertifikat erzeugen** und **exportieren** sowie anschließend **in den Konnektor Manager importieren**.

Wünschen Sie ausführliche Informationen zur Einrichtung eines KIM-Arbeitsplatzes inklusive Einbindung des LDAP-Abgleichs in EVIDENT orientieren Sie sich bitte an der an o. a. Stelle auf der EVIDENT Homepage hinterlegten **Anleitung seit EVIDENT Version 5.68**. In den Schritten 1 bis 5 dieser Anleitung erfahren Sie alles Wissenswerte dazu.



1. Client Zertifikat für die KoCoBox erzeugen

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-Managementsschnittstelle** erzeugt. Nachfolgende Abbildung zeigt die Stelle:

KoCo Connector
KoCoBox-Managementsschnittstelle

TI ■ SIS ■ WAN ■ LAN ■

Benutzer [Rolle]: koko-root [Admin] Referenz- / Testumgebung

Menü

- Status
- Kartendienst
- Kartenterminaldienst
- Systeminformationsdienst
- Zertifikatsdienst
- Protokollierungsdienst
- LAN / WAN
- DHCP
- VPN
- Zeitdienst
- DNS
- Verwaltung**
 - Clientssysteme**
 - Ex-/Import
- Fachmodul VSDM
- Fachmodul AMTS
- Fachmodul NFDM
- Fachmodul ePA
- Benutzerverwaltung
- Infomodell
- Aktualisierung
- Signaturdienst

Anbindung Clientsysteme

Zugriff auf Dienstverzeichnisdienst auch via HTTP ermöglichen: ja nein

Verbindung nur via TLS: ein aus

Authentisierung verpflichtend: aktiviert nicht aktiviert

Authentisierungsmodus: Zertifikat Benutzername / Passwort

Zugangsdaten für Clientsysteme:

| Clientssystem | Benutzer |
|---------------|----------|
| | |

Zugangszertifikate für Clientsysteme

| Clientssystem | Distinguished Name | Aussteller | Kryptographisches Verf |
|---------------|--------------------|------------|------------------------|
| caEVIDENT | CN=KoCoBox | CN=KoCoBox | RSA-2048 |
| EVIDENT | CN=EVIDENT | CN=KoCoBox | RSA-2048 |

Im Bereich **Verwaltung Clientssysteme** wählen Sie die Option **Zugangszertifikat hinzufügen....** Damit werden Sie aufgefordert die im Infomodell hinterlegte Clientssystem-ID anzugeben. Danach wird für diese Clientssystem-ID ein TLS-Zertifikat generiert und steht zum Download bereit. Für den **Download** verwenden Sie bitte **unbedingt** den **Firefox Browser**.

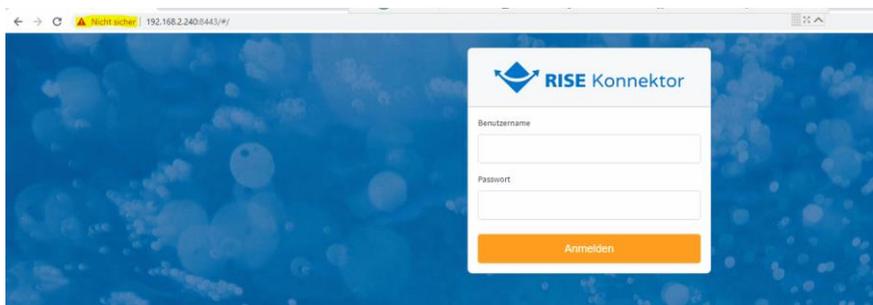


2. Konnektor Zertifikat für die KoCoBox exportieren

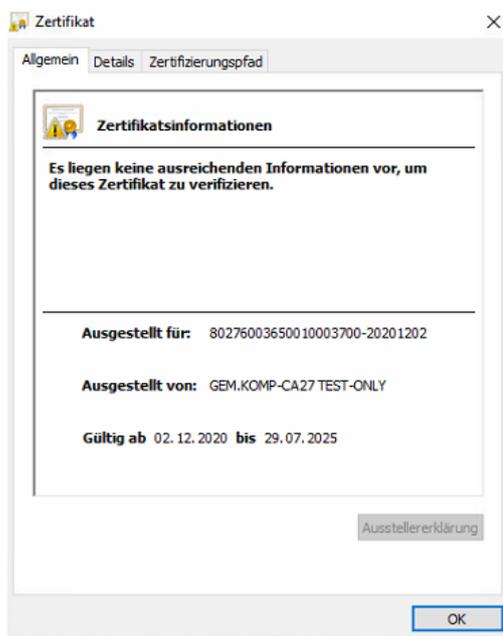
Nachfolgende Abbildung gilt sowohl für Rise als auch für die KoCoBox. Das Bild zeigt das Beispiel für Rise. Das Vorgehen ist bei der KoCoBox aber identisch.

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, bestätigen mit **Weiter**, und dann mit **Fertigstellen**.

3. 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:

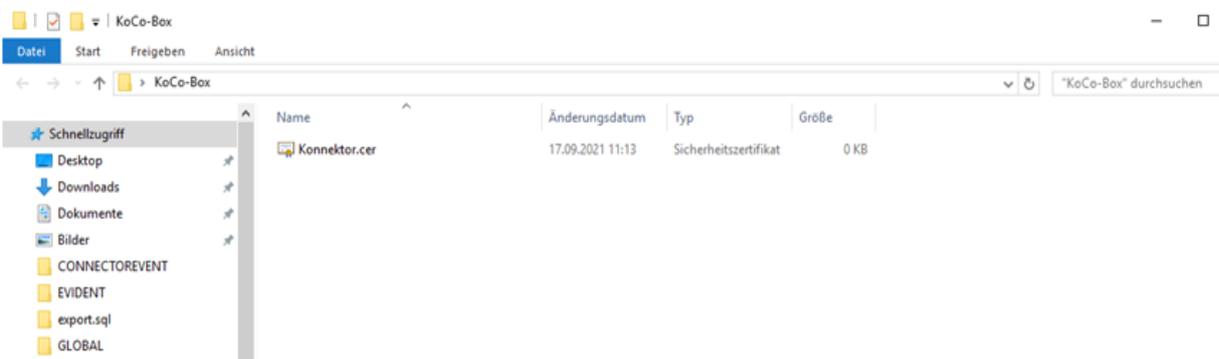
Um das Verzeichnisdienstverzeichnis (VDV) per **HTTPS** statt http vom Konnektor zu beziehen, ist es erforderlich den Konnektor zu bearbeiten. Hier nochmal die Stelle im KM.

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



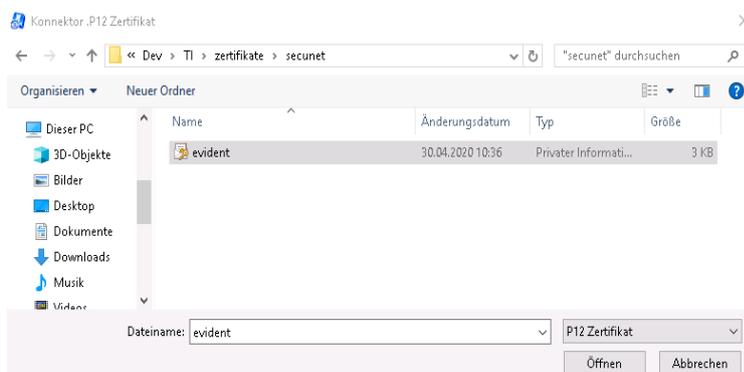
4. KoCoBox Zertifikat importieren

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



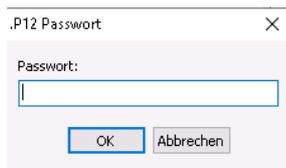
Hier ist die **.CER** Datei zu selektieren und wiederum per Öffnen zu bestätigen.

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





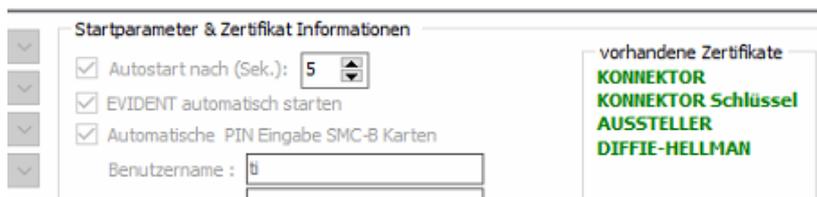
Nach Öffnen der P12 Datei erscheint die Passwortabfrage:



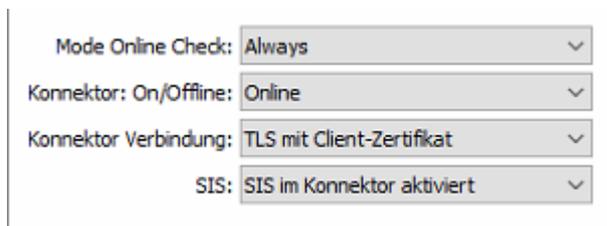
Es ist das gesicherte und gemerkte Passwort einzugeben.

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

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



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



Die Option TLS mit Client Authentisierung ist für alle Konnektoren **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.